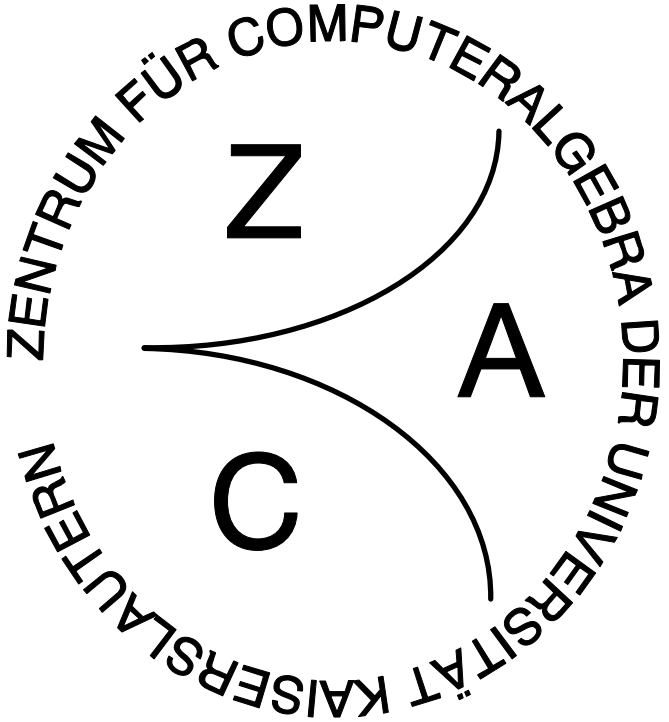
UNIVERSITÄT KAISERSLAUTERN
Zentrum für Computeralgebra

REPORTS ON COMPUTER ALGEBRA
NO. 16



String Rewriting and Gröbner Bases – A General Approach to Monoid and Group Rings

by

K. Madlener and B. Reinert

October 1997

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/`

String Rewriting and Gröbner Bases – A General Approach to Monoid and Group Rings

Klaus Madlener, Birgit Reinert
Universität Kaiserslautern
67663 Kaiserslautern
{madlener,reinert}@informatik.uni-kl.de

presented at the
Workshop on Symbolic Rewriting Systems
Monte Verita, May 1995

October, 1997

Abstract

The concept of algebraic simplification is of great importance for the field of symbolic computation in computer algebra. In this paper we review some fundamental concepts concerning reduction rings in the spirit of Buchberger. The most important properties of reduction rings are presented. 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. Several results on the connection of the word problem and the congruence problem are proven. The concepts of saturation and completion are introduced for monoid rings having a finite convergent presentation by a semi-Thue system. For certain presentations, including free groups and context-free groups, the existence of finite Gröbner bases for finitely generated right ideals is shown and a procedure to compute them is given.

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[1] for polynomial ideals in commutative polynomial rings over fields [Bu65]. It established a rewriting approach to the theory of polynomial ideals. Polynomials can be used as rules by giving an admissible[2] ordering on the terms and using the largest monomial according to this ordering as a left hand side of a rule. "Reduction" as defined by Buchberger 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.

The method of Gröbner bases allows to solve many problems related to polynomial ideals in a computational fashion. It was shown by Hilbert (compare Hilbert's basis theorem) that every ideal in a polynomial ring has a finite generating set. However, an arbitrary finite generating set need not provide much insight into the nature of the ideal. Let $f_1 = X_1^2 + X_2$ and $f_2 = X_1^2 + X_3$ be two polynomials in the polynomial ring[3] $\mathbf{Q}[X_1, X_2, X_3]$. Then $\imath = \{f_1 * g_1 + f_2 * g_2 \mid g_1, g_2 \in \mathbf{Q}[X_1, X_2, X_3]\}$ is the ideal they generate and it is not hard to see that the polynomial $X_2 - X_3$ belongs to $\imath$ since $X_2 - X_3 = f_1 - f_2$. But what can be said about the polynomial $f = X_3^3 + X_1 + X_3$? Does it belong to $\imath$ or not?

The problem to decide whether a given polynomial lies in a given ideal is called the membership problem for ideals. In case the generating set is a Gröbner basis this problem becomes immediately solvable, as the membership problem then reduces to checking whether the polynomial reduces to zero.

In our example the set $\{X_1^2 + X_3, X_2 - X_3\}$ is a generating set of $\imath$ which is in fact a Gröbner basis. Now returning to the polynomial $f = X_3^3 + X_1 + X_3$ we find that it cannot belong to $\imath$ since neither X_1^2 nor X_2 is a divisor of a term in f and hence f cannot be reduced to zero by the polynomials in the Gröbner basis.

Further applications of Gröbner bases to algebraic questions can be found e.g. in the work of Buchberger [Bu87], Becker and Weispfenning [BeWe92] and in the book of Cox, Little and O'Shea [CoLiOS92].

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 non-commutative algebras

[1] Note that similar concepts appear in a paper of Hironaka where the notion of a complete set of polynomials is called a standard basis [Hi64].

[2] A term ordering $\succeq$ is called admissible if for every term s, t, u, $s \succeq 1$ holds, and $s \succeq t$ implies $s \circ u \succeq t \circ u$. An ordering fulfilling the latter condition is also said to be compatible with the respective multiplication $\circ$.

[3] $\mathbf{Q}$ denotes the rational numbers.

over fields and other rings. In general for such rings arbitrary finitely generated ideals will not have finite Gröbner bases. Nevertheless, there are interesting classes for which every finitely generated (left or right) ideal has a finite Gröbner basis which can be computed by appropriate variants of Buchberger's algorithm.

First successful generalizations were extensions to commutative polynomial rings over coefficient domains other than fields. It was shown by several authors including Buchberger, Kandri-Rody, Kapur, Narendran, Lauer, Stifter and Weispfenning that Buchberger's approach remains valid for polynomial rings over the integers, or even Euclidean rings, and over regular rings (see e.g. [Bu83, Bu85, KaKa84, KaKa88, KaNa85a, La76, St85, We87]). For regular rings Weispfenning has to deal with the situation that zero-divisors in the coefficient domain have to be considered.

Since the development of computer algebra systems for commutative algebras enabled to perform tedious calculations using computers, attempts to generalize such systems and especially Buchberger's ideas to non-commutative algebras followed. Originating from special problems in physics, Lassner in [La85] suggested how to extend existing computer algebra systems in order to handle special classes of non-commutative algebras, e.g. Weyl algebras. He studied structures where the elements could be represented using the usual representation of polynomials in commutative variables and the non-commutative multiplication could be performed by a so-called "twisted product" which required only procedures involving commutative algebra operations and differentiation. Later on together with Apel he extended Buchberger's algorithm to enveloping fields of Lie algebras [ApLa88]. Because these ideas use representations by commutative polynomials, Dickson's lemma can be carried over. The existence and construction of finite Gröbner bases for finitely generated left ideals is ensured. In [Ga88] Galligo also studied algorithmic questions on ideals of differential operators.

On the other hand, Mora gave a concept of Gröbner bases for a class of non-commutative algebras by saving an other property of the polynomial ring while losing the validity of Dickson's lemma. The usual polynomial ring can be viewed as a monoid ring where the monoid is a finitely generated free commutative monoid. Mora studied the class where the free commutative monoid is substituted by a free monoid – the class of finitely generated free monoid rings (compare e.g. [Mo85, Mo94]). The ring operations are mainly performed in the coefficient domain while the terms are treated like words, i.e., the variables no longer commute with each other. The definitions of (one- and two-sided) ideals, reduction and Gröbner bases are carried over from the commutative case to establish a similar theory of Gröbner bases in "free non-commutative polynomial rings over fields". But these rings are no longer Noetherian if they are generated by more than one variable. Mora presented a terminating completion procedure for finitely generated one-sided ideals and an enumeration procedure for finitely generated two-sided ideals with respect to some term ordering in free monoid rings.

Gröbner bases and Mora's Algorithm have been generalized to path algebras (see [FaFeGr93, Ke97]); free non-commutative polynomial rings are in fact a particular instance of path algebras.

Another class of non-commutative rings where the elements can be represented by the usual polynomials and which allow the construction of finite Gröbner bases for arbitrary ideals are the so-called solvable rings, a class intermediate between commutative and general

non-commutative polynomial rings. They were studied by Kandri-Rody, Weispfenning and Kredel [KaWe90, Kr93]. Solvable polynomial rings can be described by ordinary polynomial rings $\mathbf{K}[X_1, \ldots, X_n]$ provided with a "new" definition of multiplication which coincides with the ordinary multiplication except for the case that a variable X_j is multiplied with a variable X_i with lower index, i.e., $i < j$. In the latter case multiplication can be defined by equations of the form $X_j \star X_i = c_{ij} X_i X_j + p_{ij}$ where $c_{ij} \in \mathbf{K}^* = \mathbf{K} \backslash \{0\}$ and p_{ij} is a polynomial "smaller" than $X_i X_j$ with respect to a fixed admissible term ordering on the polynomial ring.

The more special case of twisted semi-group rings, where $c_{ij} = 0$ is possible, has been studied in [Ap88, Mo88].

In [We92] Weispfenning showed the existence of finite Gröbner bases for arbitrary finitely generated ideals in non-Noetherian skew polynomial rings over two variables X, Y where a "new" multiplication $\star$ is introduced such that $X \star Y = XY$ and $Y \star X = X^e Y$ for some fixed $e \in \mathbf{N}^+$.

Ore extensions have been successfully studied by Pesch in his PhD Thesis and his results on two-sided Gröbner bases are presented in this volume [Pe97].

Most of the results cited so far assume admissible well-founded orderings on the set of terms so that in fact reduction can be defined by considering the head monomials only. This is essential to characterize Gröbner bases in the respective ring with respect to the corresponding reduction in a finitary manner and to enable to decide whether a finite set is a Gröbner basis by checking whether the s-polynomials are reducible to zero[4].

There are rings combined with reduction where admissible well-founded orderings cannot be accomplished and, therefore, other concepts to characterize Gröbner bases have been developed. For example in case the ring contains zero-divisors a well-founded ordering on the ring is no longer compatible with the ring multiplication[5]. This phenomenon has been studied for the case of zero-divisors in the coefficient domain by Kapur and Madlener [KaMa86] and by Weispfenning for the special case of regular rings [We87]. In his PhD thesis [Kr93], Kredel described problems occurring when dropping the axioms guaranteeing the existence of admissible orderings in the theory of solvable polynomial rings by allowing $c_{ij} = 0$ in the defining equations above. He sketched the idea of using saturation to repair some of them. Saturation enlarges the generating sets in order to ensure that enough head terms exist to do all necessary reductions and this process can often be related to additional special critical pairs. Similar ideas can be found in the PhD thesis of Apel [Ap88]. For special cases, e.g. for the Grassmann (exterior) algebras, positive results can be achieved (compare the paper of Stokes [St90]).

Before we move on to give a more abstract generalization of structures allowing Gröbner basis algorithms, let us first summarize some important notations and definitions of reduction relations and basic properties related to them, as can be found more explicitly for example in the work of Huet or Book and Otto ([Hu80, Hu81, BoOt93]).

Let $\mathcal{E}$ be a set of elements and $\longrightarrow$ a binary relation on $\mathcal{E}$ called **reduction**. For $a, b \in \mathcal{E}$ we will write $a \longrightarrow b$ in case $(a, b) \in \ \longrightarrow$. A pair $(\mathcal{E}, \longrightarrow)$ will be called a **reduction system**.

[4]Note that we always assume that the reduction in the ring is effective.

[5]When studying monoid rings over reduction rings it is possible that the ordering on the ring is not compatible with scalar multiplication as well as with multiplication with monomials or polynomials.

Obviously the reflexive symmetric transitive closure $\overset{*}{\longleftrightarrow}$ is an equivalence relation on $\mathcal{E}$ and the reflexive transitive closure $\overset{*}{\longrightarrow}$ can be viewed as a reduction relation on $\mathcal{E}$.

Well-known decision problems related to a reduction system are the word problem and the generalized word problem.

Definition 1.1 *The* **word problem** *for* $(\mathcal{E}, \longrightarrow)$ *is to decide for* $a, b \in \mathcal{E}$*, whether* $a \overset{*}{\longleftrightarrow} b$ *holds.*

Definition 1.2 *The* **generalized word problem** *for* $(\mathcal{E}, \longrightarrow)$ *and* $\mathcal{E}_1 \subseteq \mathcal{E}$ *is to decide for* $a \in \mathcal{E}$*, whether there exists* $b \in \mathcal{E}_1$ *such that* $a \overset{*}{\longleftrightarrow} b$ *holds..*

Instances of these problems are well-known in the literature and undecidable in general, but we will outline sufficient conditions such that $(\mathcal{E}, \longrightarrow)$ has solvable word problem.

An element $a \in \mathcal{E}$ is said to be **reducible** (with respect to $\longrightarrow$) if there exists an element $b \in \mathcal{E}$ such that $a \longrightarrow b$. All elements $b \in \mathcal{E}$ such that $a \overset{*}{\longrightarrow} b$ are called **successors** of a and in case $a \overset{+}{\longrightarrow} b$ they are called **proper successors**. An element which has no proper successor is called **irreducible**. In case $a \overset{*}{\longrightarrow} b$ and b is irreducible, b is called a **normal form** of a. Notice that for an element a in $\mathcal{E}$ there can be no, one or many normal forms.

Definition 1.3 *A reduction system* $(\mathcal{E}, \longrightarrow)$ *is said to be* **Noetherian** *(or* **terminating***) in case there are no infinitely descending reduction chains* $a_0 \longrightarrow a_1 \longrightarrow \ldots$ *with* $a_i \in \mathcal{E}$*,* $i \in \mathbf{N}$*.*

In case $(\mathcal{E}, \longrightarrow)$ is Noetherian every element in $\mathcal{E}$ has at least one normal form.

Definition 1.4 *A reduction system* $(\mathcal{E}, \longrightarrow)$ *is called* **confluent***, if for all* $a, a_1, a_2 \in \mathcal{E}$*,* $a \overset{*}{\longrightarrow} a_1$ *and* $a \overset{*}{\longrightarrow} a_2$ *implies the existence of* $a_3 \in \mathcal{E}$ *such that* $a_1 \overset{*}{\longrightarrow} a_3$ *and* $a_2 \overset{*}{\longrightarrow} a_3$*.*

In case $(\mathcal{E}, \longrightarrow)$ is confluent every element has at most one normal form. We can combine these two properties to give sufficient conditions for the solvability of the word problem.

Definition 1.5 *A reduction system* $(\mathcal{E}, \longrightarrow)$ *is said to be* **complete** *or* **convergent** *in case it is both, Noetherian and confluent.*

Convergent reduction systems with effective[6] reduction relations have solvable word problem, as every element has a unique normal form and two elements are equal if and only if their normal forms are equal. Of course we cannot always expect $(\mathcal{E}, \longrightarrow)$ to be convergent. Even worse, both properties are undecidable in general. Nevertheless, there are weaker conditions which guarantee convergence.

Definition 1.6 *A reduction system* $(\mathcal{E}, \longrightarrow)$ *is said to be* **locally confluent***, if for all* $a, a_1, a_2 \in \mathcal{E}$*,* $a \longrightarrow a_1$ *and* $a \longrightarrow a_2$ *implies the existence of an element* $a_3 \in \mathcal{E}$ *such that* $a_1 \overset{*}{\longrightarrow} a_3$ *and* $a_2 \overset{*}{\longrightarrow} a_3$*.*

[6]By "effective" we mean that given an element we can decide whether a successor exists and then construct it.

Now Newman's lemma gives an important connection between confluence and local confluence.

Lemma 1.7 (Newman) *Let $(\mathcal{E}, \longrightarrow)$ be a Noetherian reduction system. Then $(\mathcal{E}, \longrightarrow)$ is confluent if and only if $(\mathcal{E}, \longrightarrow)$ is locally confluent.*

Therefore, if the reduction system is terminating, a check for confluence can be reduced to a check for local confluence. It is often the case that the test for local confluence is a finitary one, hence leading to "critical-pair" based completion procedures. In case the test for local confluence fails for a pair, the reduction relation is refined without changing the generated equivalence relation but preserving termination. This is e.g. done for the critical pairs in the Knuth-Bendix completion procedure and for the s-polynomials in Buchberger's algorithm.

Besides the extensions of Buchberger's ideas using knowledge on the algebra mentioned before there are also considerations of finding essential properties of reduction for a ring to allow finite Gröbner bases – the idea of defining so-called reduction rings. A first generalization of this kind was given by Buchberger himself and his student Stifter in characterizing reduction rings by adding additional axioms to the ring axioms [St85, St87]. Another approach was given by Kapur and Narendran for polynomials over reduction rings in [KaNa85a].

We will here use the axiomatization given by Madlener in 1986: Let $\mathbf{R}$ be a ring with a reduction $\Longrightarrow_B$ associated with subsets $B \subseteq \mathbf{R}$ satisfying the following axioms

(A1) $\Longrightarrow_B = \bigcup_{b \in B} \Longrightarrow_b$, $\Longrightarrow_B$ is terminating for all subsets $B \subseteq \mathbf{R}$.

(A2) $a \Longrightarrow_b c$ implies $a - c \in \mathsf{ideal}(b)$.

(A3) $a \Longrightarrow_a 0$ for all $a \in \mathbf{R} \backslash \{0\}$.

Notice that in case R is commutative (A2) implies $c = a - b \cdot r$ for some $r \in \mathbf{R}$. In the non-commutative case in general we get $c = a - \sum_{i=1}^{k} r_{i1} \cdot b \cdot r_{i2}$ for some $r_{i1}, r_{i2} \in \mathbf{R}$, $1 \leq i \leq k$ or we can define a more restricted form of reduction by demanding $c = a - r_1 \cdot b \cdot r_2$ for some $r_1, r_2 \in \mathbf{R}$.

Further let $\imath = \mathsf{ideal}(B)$ be the ideal generated by the set B in $\mathbf{R}$. If $\equiv_\imath$ denotes the congruence generated by $\imath$, from (A1) and (A2) $\overset{*}{\Longleftrightarrow}_B \subseteq \equiv_\imath$ follows. One method for solving the membership problem for $\imath$ by reduction methods is to transform B into a finite set B' such that $\Longrightarrow_{B'}$ is confluent on $\imath$. Notice that 0 has to be irreducible for all $\Longrightarrow_a$, $a \in \mathbf{R}$. Therefore, 0 will be chosen as the normal form of the ideal elements. Hence the goal is to achieve $a \in \imath$ if and only if $a \overset{*}{\Longrightarrow}_{B'} 0$. In particular B' also generates $\imath$ and $\imath$ is one equivalence class of $\overset{*}{\Longleftrightarrow}_{B'}$. The different definitions of reductions in rings existing in literature show that for solving the membership problem it is not necessary to enforce $\overset{*}{\Longleftrightarrow}_{B'} = \equiv_\imath$. E.g. the D-reduction notion given by Pan in [Pa85] does not have this property but it suffices to decide $\equiv_\imath$-equivalence of two elements because $a \equiv_\imath b$ if and only if $a - b \in \imath$. It may happen that D-reduction is not only confluent on $\imath$ but confluent everywhere and still $a \equiv_\imath b$ does not imply that the normal forms with respect to D-reduction are the same.

With this in mind there are several possible definitions of G-bases (Gröbner bases) when relating them to the solvability of the membership problem. We want to restrict ourselves to the original intention of Buchberger in which $\overset{*}{\Longleftrightarrow}_B = \equiv_{\mathsf{ideal}(B)}$ holds.

Definition 1.8 *A subset B of $\mathbf{R}$ is called a* **G-basis** *of an ideal $\imath$, if $\overset{*}{\Longleftrightarrow}_B = \equiv_\imath$ and $\Longrightarrow_B$ is confluent.*

$\mathbf{R}$ is called a **reduction ring** if every finitely generated ideal has a finite G-basis.
The notion of one-sided reduction rings can be defined similarly.
Also effective or computable reduction rings can be defined (e.g. Buchberger's reduction rings) namely those for which reduction is effective and there exists an algorithm for computing a finite G-basis from a finite set of generators of the ideal.

It is often useful, if $\mathbf{R}$ satisfies an additional axiom strongly related to interreduction.

(A4) $a \Longrightarrow_b$ and $b \Longrightarrow_c d$ imply $a \Longrightarrow_c$ or $a \Longrightarrow_d$.

Now the question arises which ring constructions, as e.g. extensions, products or quotients, preserve the property of being a reduction ring.

Theorem 1.9 *Let $\mathbf{R}$ be a Noetherian reduction ring. Then $\mathbf{R}[X_1, \ldots, X_n]$ is a Noetherian reduction ring.*

Theorem 1.10 *Let $\mathbf{R}$ be a reduction ring satisfying (A4) and $\imath$ a finitely generated ideal in $\mathbf{R}$. Then $\mathbf{R}/\imath$ is a reduction ring satisfying (A4).*

Theorem 1.11 *Let $\mathbf{R}_1, \mathbf{R}_2$ be reduction rings. Then the sum $\mathbf{R}_1 \times \mathbf{R}_2 = \{(r_1, r_2) \mid r_1 \in \mathbf{R}_1, r_2 \in \mathbf{R}_2\}$ is a reduction ring.*

Of course for every such construction an appropriate notion of reduction has to be found which arises naturally in these cases. Another interesting question is, when and how a given algorithm for computing G-bases for a reduction ring can be lifted when constructing new reduction rings. This is possible in all three cases given above and was also studied by Buchberger and Stifter who gave an axiomatic description of the properties necessary to enable such a lifting.
In general we have to compute G-bases and syzygy bases for sets of elements in the original reduction ring in order to lift the G-bases computations to the new reduction ring. In case the original reduction ring is a principal ideal ring, only special sets, namely of size two for the G-bases and of size one for the syzygy bases, have to be considered.

That different choices of reduction are possible shall be illustrated in a short example. Let us consider the reduction ring $\mathbf{Z}_m$ for some $m \in \mathbf{N}^+$. Then the polynomial ring $\mathbf{Z}_m[X_1, \ldots, X_n]$ again is a reduction ring. Reduction in $\mathbf{Z}_m[X_1, \ldots, X_n]$ on one hand can be defined by lifting the reduction given in $\mathbf{Z}_m$ (compare theorem 1.9). But we can also view $\mathbf{Z}_m[X_1, \ldots, X_n]$ as a quotient, namely $\mathbf{Z}[X_1, \ldots, X_n]/(m)$, and lift a reduction defined for the polynomial ring $\mathbf{Z}[X_1, \ldots, X_n]$ to our structure (compare theorem 1.10). This shows that there are various ways to treat a given ring as a reduction ring by specifying different reductions.

Several fields where reduction systems are studied and used can be found in computer science. The theory of term rewriting systems plays an important role e.g. in algebraic specifications of abstract data structures, equational programming, program transformation or automated theorem proving. The concept of completion based on the Knuth-Bendix completion procedure given in [KnBe70] has become very influential in this field. In [LeCh86] Le Chenadec describes how with many equational classes of algebras one can associate a completion procedure of a finitely presented algebra A in the class which translates a presentation of A into a (not necessarily finite) complete set of syntactic replacement rules. He incorporates the ideas of rewriting modulo theories (class rewriting) which can be generalized to normalized rewriting [Mar93]. He also includes algorithms encoding knowledge about the input which linearly solve the word problem for some classes of groups (e.g. small cancellation groups introduced by Dehn [De12] where he presented a string-rewriting based solution to the word problem for these groups).

Several authors have studied the relations between Buchberger's algorithm and the Knuth-Bendix completion procedure. The main difficulty is to capture fields, since they are not equationally definable. Hence by using conditional or more generally constraint rewriting this problem can be surpassed. In fact Bachmair and Ganzinger have shown that Buchberger's algorithm can be viewed as a constraint-based variant of completion [BaGa94b] where the operations in the coefficient field are expressed via constraints and separated from the computations in the polynomial ring structure done by rewriting. Earlier attempts using class rewriting can be found in [KaKaWi89]. Madlener and Reinert have shown that certain undecidability results for string rewriting systems carry over to monoid and group rings since the specialization of the Knuth-Bendix completion procedure for string rewriting systems is an instance of Mora's generalization of Buchberger's algorithm for free monoid rings [Re95]. These results can be found in the next section of this paper.

As we have seen there are two main approaches to use rewriting techniques for symbolic computation. One is to give a formal definition of the objects by means of axiomatization in a term rewriting system. The other is to solve problems in special structures by incorporating knowledge on the structure into the procedure. In this paper we want to show how this can be done for monoid and group rings by giving different notions of reduction and showing how specializing the reduction according to the given group presentation leads to algorithmic solutions for some classes of groups. Since our approach combines rewriting for the presentation of the monoid or group and polynomial rewriting in the field of monoid and group rings, let us first introduce a special kind of term rewriting systems, the so called string rewriting systems or semi-Thue systems. These systems are strongly related to the idea of presenting monoids or groups in terms of generators and defining relations [Gi79, LySch77, MaKaSo76].

A semi-Thue system consists of an alphabet Σ and a set of rules $T \subseteq \Sigma^* \times \Sigma^*$[7]. 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 semi-Thue 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. There have been numerous studies investigating special kinds of semi-Thue

[7] Σ^* is the set of all words on the alphabet Σ where λ presents the **empty word**, i.e., the word of length zero, and $\equiv$ the identity on words.

presentations and the influence of certain properties on the decidability of certain questions related to the monoid or group they present. Of special interest is the question which monoids have presentations by finite convergent semi-Thue systems and how to compute them. Kapur and Narendran in [KaNa85b] and Jantzen in [Ja81, Ja85] give examples of monoid presentations for which completion does not terminate (i.e. there is no equivalent finite convergent system with respect to any completion ordering) although a finite convergent semi-Thue system over a different alphabet presenting the same monoid exists. Squier proved the existence of finitely presented monoids with decidable word problem which cannot be presented by a finite convergent semi-Thue system [Sq87]. In [De92] Deiß introduces conditional semi-Thue systems and gives finite convergent conditional presentations for the monoids given by Narendran and Squier.

Besides demanding overall confluence, to decide the word problem for a group confluence on the congruence class of λ is sufficient. The property of being confluent on specific congruence classes only and specialized completion procedures for such presentations have been studied by Otto and others [Ot87, OtZh91, MNOZ93].

The subgroup problem is also an important decision problem for groups. Kuhn and Madlener have shown how the notion of prefix rewriting – a specialization of ordinary string rewriting – can be applied to solve the subgroup problem for certain classes of groups [KuMa89]. Prefix rewriting and its completion is a direct generalization of Nielsen's method to solve the subgroup problem in the class of free groups [Ni21]. In case of confluence it can be used to compute Schreier-representatives of the subgroup cosets. A related question is when subgroups of groups allowing certain presentations again have a presentation of the same type. For some groups such a presentation for the subgroup can be computed from a confluent prefix rewriting system for the subgroup [KuMaOt94].

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[8] on Σ^* such that for all $(l, r) \in T$, $l \succ r$ holds. This ordering is called a completion ordering of (Σ, T). The monoid $\mathcal{M}$ is isomorphic to the set $\mathrm{IRR}(T)$ of words irreducible with respect to T. The empty word $\lambda \in \Sigma^*$ presents the identity of $\mathcal{M}$. The word problem is solvable, which is essential for computation in $\mathbf{K}[\mathcal{M}]$. Multiplication of two terms $u, v \in \mathcal{M}$ is defined by $u \circ v = (uv)\downarrow_T$. The completion ordering of the presentation 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 $\mathbf{K}[\mathcal{M}]$ over a field $\mathbf{K}$ 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 $\mathbf{K}[\mathcal{M}]$ we call the set $\mathsf{ideal}_r(F) = \{\sum_{i=1}^{n} \alpha_i \cdot f_i * w_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, f_i \in F, w_i \in \mathcal{M}\}$ the **right ideal** and $\mathsf{ideal}(F) = \{\sum_{i=1}^{n} \alpha_i \cdot u_i * f_i * w_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, f_i \in F, u_i, w_i \in \mathcal{M}\}$ the **two-sided ideal** generated by F. We will henceforth always assume that the field $\mathbf{K}$ is computable.

The contents of the remaining sections of the paper is an extension of our work on Gröbner bases in arbitrary monoid rings as it was presented at the ISSAC meeting in Kiew in 1993

[8] An ordering on Σ^* is called admissible, if for all $u, v, w, x, y \in \Sigma^*$, $w \succeq \lambda$ holds and $u \succ v$ implies $xuy \succ xvy$.

[MaRe93b] combined with some results of the PhD thesis [Re95]. It organizes as follows: In section 2 some undecidability results on the existence of finite Gröbner bases are presented. Section 3 outlines our approach of introducing reduction to a monoid ring $\mathbf{K}[\mathcal{M}]$. Two possible definitions of reduction – strong and prefix reduction – are studied and characterizations of Gröbner bases for finitely generated right ideals in the respective settings are given. A procedure which enumerates prefix Gröbner bases for finitely generated right ideals is given. We close the section by extending the characterization of prefix Gröbner bases to two-sided ideals. Finally, in section 4 we prove termination of the procedure to compute prefix Gröbner bases given in section 3 for some classes of groups, namely finite, free and plain groups, and show how this procedure can be extended to compute finite prefix Gröbner bases in the class of context-free groups. Section 5 gives some perspectives for further work in this field.

Addendum
We want to point out that the approach given here has also been specialized for the class of polycyclic groups [Re96, MaRe97a]. These results are outlined in the concluding remarks. There we also present a table which illustrates how the existence of finite Gröbner bases with respect to special reductions is related to groups having a subgroup problem solvable by rewriting methods.

Acknowledgments
The first author wants to thank several colleagues for fruitful discussions. In particular Bruno Buchberger who introduced him to the study of reduction rings and Deepak Kapur for sharing with him ideas all the years after the workshop held in Otzenhausen. We both thank Andrea Sattler-Klein, Teo Mora, Paliath Narendran and Friedrich Otto for valuable discussions on parts of this paper. Volker Weispfenning has taken influence on parts of this work as the second advisor of Reinert's PhD thesis [Re95].

2 Fundamental Relations Between Semi-Thue Systems and Monoid Rings

Kandri-Rody and Weispfenning have shown in [KaWe90] that the ideal membership problem for finitely generated two-sided ideals is algorithmically unsolvable for the free monoid ring $\mathbf{Q}[\{X_1, X_2\}^*]$ by reducing the halting problem for Turing machines to this problem. Here we state a similar result by showing that the word problem for semi-Thue systems is equivalent to a restricted version of the ideal membership problem in free monoid rings $\mathbf{K}[\Sigma^*]$ where Σ is a finite alphabet.

Theorem 2.1 *Let (Σ, T) be a finite semi-Thue system and $P_T = \{l - r \mid (l, r) \in T\}$ a set of polynomials associated with T. Then for $u, v \in \Sigma^*$ the following statements are equivalent:*

(1) $u \overset{*}{\longleftrightarrow}_T v$.

(2) $u - v \in \mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T)$.

The existence of a finite semi-Thue system over an alphabet with two elements having undecidable word problem yields that the ideal membership problem for free monoid rings

with more than one generator is undecidable. In case the free monoid is generated by one element, we have decidable ideal membership problem. In fact this is the ordinary polynomial ring in one variable and, e.g., the Euclidean algorithm can be applied to solve the ideal membership problem.

Perhaps less obvious is that the word problem for finitely presented groups is similarly equivalent to a restricted version of the membership problem for ideals in a free group ring. Let the group be presented by a semi-Thue system (Σ, T) such that there exists an involution $\imath : \Sigma \longrightarrow \Sigma$ such that for all $a \in \Sigma$ we have $\imath(a) \neq a$, $\imath(\imath(a)) = a$, and the rules $(\imath(a)a, \lambda)$ and $(a\imath(a), \lambda)$ are included in T. Such systems are called group systems.

Theorem 2.2 *Let $(\Sigma, T \cup T_I)$ be a finite group system and $T_I = \{(\imath(a)a, \lambda), (a\imath(a), \lambda) \mid a \in \Sigma\}$, i.e., (Σ, T_I) is a presentation of a free group $\mathcal{F}$. Further we can associate a system of polynomials $P_T = \{l - r \mid (l, r) \in T\}$ with T and without loss of generality we can assume that l and r are in normal form with respect to T_I. Then for $u, v \in \Sigma^*$ the following statements are equivalent:*

(1) $u \overset{*}{\longleftrightarrow}_{T \cup T_I} v$.

(2) $u{\downarrow_{T_I}} - v{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$.

As before, the existence of a finite group presentation over four letters (resulting from two generators) with unsolvable word problem implies that the ideal membership problem for free group rings with more than one generator is undecidable. Groups with one generator are known to have decidable word problem. The ideal membership problem for free group rings with one generator is solvable as this ring corresponds to the ring of Laurent polynomials for the (commutative) free group with one generator.

Definition 2.3 (Mora) *Let $\succ$ be a total admissible well-founded ordering on Σ^* used to sort the terms in the polynomials in decreasing order. Further let $p = \sum_{i=1}^{n} \alpha_i \cdot w_i, g = \sum_{j=1}^{m} \beta_j \cdot v_j \in \mathbf{K}[\Sigma^*]$.*
We say g reduces *p to q at a monomial $\alpha_k \cdot w_k$ of p in one step, denoted by $p \longrightarrow_g q$, if*

(a) $xv_1y \equiv w_k$ *for some $x, y \in \Sigma^*$, where $v_1 \succ v_j$, $2 \leq j \leq n$, and*

(b) $q = p - (\alpha_k \cdot \beta_1^{-1}) \cdot x * g * y$.

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

Notice that for a set of polynomials F, $\overset{*}{\longleftrightarrow}_F = \equiv_{\mathsf{ideal}(F)}$ holds and if additionally $\longrightarrow_F$ is confluent we call F a Gröbner basis of $\mathsf{ideal}(F)$.

While theorem 2.1 reduces the word problem for semi-Thue systems to the ideal membership problem in free monoid rings, reviewing the proof of this theorem (compare page 35) we see that in fact the existence of finite convergent semi-Thue systems corresponds to the existence of finite Gröbner bases and vice versa. Hence solvable word problem does not imply the existence of finite Gröbner bases as the example of a finitely presented monoid $\Sigma = \{a, b\}$,

$T = \{aba \longrightarrow bab\}$ with solvable word problem but no finite convergent presentation with respect to any admissible ordering shows (see [KaNa85b]). The ideal generated by the polynomial $aba - bab$ in $\mathbf{K}[\{a,b\}^*]$ has no finite Gröbner basis with respect to any admissible ordering on $\{a,b\}^*$. Notice that in this example we can apply a so called Tietze transformation to the semi-Thue system, i.e. we can change the presentation without changing the monoid, giving us the equivalent presentation $\Sigma' = \{a,b,c\}$, $T' = \{aba \longrightarrow bab, ba \longrightarrow c\}$ which can be successfully completed, e.g. with respect to the length-lexicographical ordering with precedence $a \succ b \succ c$ resulting in $T'' = \{ac \longrightarrow cb, ba \longrightarrow c, bcb \longrightarrow c^2, bc^2 \longrightarrow c^2a\}$. Similarly the ideal generated by $\{aba - bab, ba - c\}$ has a finite Gröbner basis with respect to the same ordering. Due to the result of Squire in [Sq87] there are finitely presented monoids with solvable word problem which have no finite convergent presentations and his examples give rise to finitely generated ideals in free monoid rings with solvable ideal membership problem which have no finite Gröbner bases.

So now we have seen that since finitely generated ideals in free monoid rings can have unsolvable membership problem, in general they cannot admit finite Gröbner bases. It even is possible for a finitely generated ideal to admit a finite Gröbner basis with respect to one admissible ordering and none with respect to another admissible ordering. On the other hand, in [Mo85] Mora provided a procedure which given an admissible ordering enumerates a Gröbner basis with respect to this ordering. This procedure terminates in case a finite Gröbner basis with respect to the given ordering exists. Hence the question might arise, whether it is possible to decide for a finite set of polynomials and an admissible ordering whether a finite Gröbner basis with respect to this ordering exists. This turns out to be undecidable.

Theorem 2.4 *It is undecidable, whether a finitely generated ideal has a finite Gröbner basis in the free monoid ring* $\mathbf{K}[\{s,t\}^*]$ *with respect to two-sided reduction as defined in definition 2.3.*

This result holds even assuming solvable membership problem for the ideal [Sa96].

Corollary 2.5 *It is undecidable, whether for a finitely generated ideal in* $\mathbf{K}[\{s,t\}^*]$ *there exists a total, well-founded, admissible ordering on* $\{s,t\}^*$ *such that the ideal has a finite Gröbner basis with respect to reduction as defined in 2.3.*

Hence, for two-sided ideals the case of free monoids is already hard although free monoids allow simple presentations by semi-Thue systems, namely empty sets of defining relations. In theorem 2.2 we have shown that the word problem for group presentations is reducible to a restricted version of the ideal membership problem for a free group ring. We will show now that a similar result holds for the right ideal membership problem in group rings.

Definition 2.6 *Given a subset* S *of a group* $\mathcal{G}$*, let* $\langle S \rangle$ *denote the subgroup generated by* S*. The* **generalized word problem** *or* **subgroup problem** *is then to determine, given* $w \in \mathcal{G}$*, whether* $w \in \langle S \rangle$*.*

The word problem for a group $\mathcal{G}$ is just the generalized word problem for the trivial subgroup in $\mathcal{G}$. Thus the existence of a group with undecidable word problem yields undecidability

for the subgroup problem. On the other hand, decidable word problem for a group does not imply decidable generalized word problem.

The next theorem states that the subgroup problem for a group is equivalent to a special instance of the right ideal membership problem in the corresponding group ring.

Theorem 2.7 *Let S be a finite subset of $\mathcal{G}$ and $\mathbf{K}[\mathcal{G}]$ the group ring corresponding to $\mathcal{G}$. Further let $P_S = \{s-1 \mid s \in S\}$ be a set of polynomials[9] associated to S. Then the following statements are equivalent:*

(1) $w \in \langle S \rangle$.

(2) $w - 1 \in \mathsf{ideal}_r(P_S)$.

This theorem implies that when studying group rings we can only expect those over groups with solvable generalized word problem to allow solvable membership problem for right ideals. Moreover, reviewing the proof (compare page 38) we find that again reduction relations in semi-Thue systems are related to right ideal congruences and vice versa. In section 4 and 5 we will see how this leads to strong connections to known solutions of the subgroup problem by rewriting methods. So appropriate candidates are e.g. free, Abelian, nilpotent and polycyclic groups. On the other hand, solvable subgroup problem only implies the solvability of a restricted version of the right ideal membership problem.

3 Defining Reduction in $\mathbf{K}[\mathcal{M}]$

Throughout this paper let $\mathcal{M}$ be a monoid presented by a finite convergent semi-Thue system (Σ, T) and $\succeq$ the well-founded ordering on $\mathcal{M}$ induced by the completion ordering of its presentation. Notice that although the completion ordering is compatible on Σ^* with concatenation, this in general no longer holds for the ordering $\succeq$ on $\mathcal{M}$ with respect to the multiplication $\circ$ on $\mathcal{M}$. For example groups do not allow compatible well-founded orderings due to the existence of inverse elements. Given a non-zero polynomial p in $\mathbf{K}[\mathcal{M}]$, 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**. $\mathsf{T}(p)$ is the set of terms occurring in p. The ordering on $\mathcal{M}$ can be extended to a partial ordering on $\mathbf{K}[\mathcal{M}]$ 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 3.1 *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[10] of the head term to allow reduction. Then we could reduce the polynomial $b^2 + 1 \in \mathbf{Q}[\mathcal{G}]$ at the monomial b^2 by the polynomial $a + b$ as $b^2 = a \circ b^3$. This would give us:*

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

[9] Note that we use $1 = 1 \cdot \lambda = \lambda$.

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

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

Hence we will need additional restrictions in order to prevent that a monomial is replaced by a larger polynomial. Since our monoid $\mathcal{M}$ in general is not commutative, we will restrict ourselves to right ideals – hence to right multiples – and inspect two variations of defining right reduction. For further variants see e.g. [MaRe95, Re95].

Definition 3.2 *Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{M}]$. We say f* **strongly right reduces** *p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow_f^{\mathrm{s}} q$, if*

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

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

We write $p \longrightarrow_f^{\mathrm{s}}$ if there is a polynomial q as defined above and p is then called strongly right reducible by f. Strong right reduction by a set $F \subseteq \mathbf{K}[\mathcal{M}]$ is denoted by $p \longrightarrow_F^{\mathrm{s}} q$ and abbreviates $p \longrightarrow_f^{\mathrm{s}} q$ for some $f \in F$.

Note that in order to strongly right reduce p, the polynomial f need not be smaller than p. The condition $\mathsf{HT}(f * w) = t$ prevents reduction with a polynomial in case $f * w = 0$, i.e., if the monomials of f eliminate each other by multiplying f with w. This might happen in case the monoid ring contains zero-divisors. Further, in case we have $p \longrightarrow_f^{\mathrm{s}} q$ at the monomial $\alpha \cdot t$, then $t \notin \mathsf{T}(q)$. In order to decide, whether a polynomial f strongly right reduces a polynomial p at a monomial $\alpha \cdot t$ one has to decide whether there exist elements $s \in \mathsf{T}(p)$ and $w \in \mathcal{M}$ such that $s \circ w = \mathsf{HT}(f * w) = t$. Since this problem is connected to solving equations $s \circ \mathrm{x} = t$ in one variable x in the monoid $\mathcal{M}$ presented by (Σ, T), this problem is undecidable in general, even if $\mathcal{M}$ is presented by a convergent semi-Thue system. Note that there can be no, one or even (infinitely) many solutions depending on $\mathcal{M}$. In case $\mathcal{M}$ is a group the equation only has one unique solution.

Example 3.3 *Let $\Sigma = \{a, b\}$ and $T = \{ab \longrightarrow a\}$ be a presentation of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b$. Then the equation $b \circ \mathrm{x} = a$ has no solution in $\mathcal{M}$, the equation $b \circ \mathrm{x} = b$ has one solution in $\mathcal{M}$, namely $\mathrm{x} = \lambda$, and the equation $a \circ \mathrm{x} = a$ has infinitely many solutions in $\mathcal{M}$, namely the set $\{b^n | n \in \mathbf{N}\}$.*

The following example illustrates how different monomials can become equal when modifying a polynomial in order to use it for strong right reduction.

Remark 3.4 *Let $\Sigma = \{a, b\}$ and $T = \{ab \longrightarrow b\}$ be a presentation of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b$. Furthermore, let f_1, f_2, p be polynomials in $\mathbf{Q}[\mathcal{M}]$ such that $f_1 = a^2 + a$, $f_2 = a^2 - a$ and $p = b + \lambda$. Then p is strongly right reducible by f_1 at b, as $\mathsf{HT}(f_1 * b) = \mathsf{HT}(2 \cdot b) = b$ and $p \longrightarrow_{f_1}^{\mathrm{s}} p - \frac{1}{2} \cdot f_1 * b = b + \lambda - \frac{1}{2} \cdot 2 \cdot b = \lambda$. On the other hand, although both equations $a^2 \circ \mathrm{x} = b$ and $a \circ \mathrm{x} = b$ have b as a solution, we get that p is not strongly right reducible by f_2, as $f_2 * b = b - b = 0$.*

In case $\mathcal{M}$ is a right cancellative monoid or a group, the phenomenon described in this remark can no longer occur, since then $u \circ w = v \circ w$ implies $u = v$ for all $u, w, w \in \mathcal{M}$. Let us continue to state some of the properties strong right reduction satisfies.

Lemma 3.5 *Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$ and $p, q, q_1, q_2 \in \mathbf{K}[\mathcal{M}]$ some polynomials. Then the following statements hold:*

(1) $p \longrightarrow^{\mathrm{s}}_F q$ implies $p > q$, in particular $\mathsf{HT}(p) \succeq \mathsf{HT}(q)$.

(2) $\longrightarrow^{\mathrm{s}}_F$ is Noetherian.

(3) If $p \longrightarrow^{\mathrm{s}}_{q_1} 0$ and $q_1 \longrightarrow^{\mathrm{s}}_{q_2} 0$ hold, so does $p \longrightarrow^{\mathrm{s}}_{q_2} 0$.

(4) $\alpha \cdot p * w \xrightarrow{\leq 1}{}^{\mathrm{s}}_p 0$ for all $\alpha \in \mathbf{K}$, $w \in \mathcal{M}$.

Unfortunately, for strong right reduction $p \longrightarrow^{\mathrm{s}}_q$, $q \longrightarrow^{\mathrm{s}}_w q_1$ in general does not imply $p \longrightarrow^{\mathrm{s}}_{\{w,q_1\}}$, as the following example shows[11]. Therefore, our structure satisfies (A1), (A2) and (A3) but not (A4) of the axioms given in the introduction.

Example 3.6 *Let $\Sigma = \{a, b, c\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, c^2 \longrightarrow \lambda\}$ be a monoid presentation of a group $\mathcal{G}$ with a length-lexicographical ordering induced by $a \succ b \succ c$. Looking at $p = ba + b, q = bc + \lambda$ and $w = ac + b \in \mathbf{Q}[\mathcal{G}]$ we get $p \longrightarrow^{\mathrm{s}}_q p - q * ca = -ca + b$ and $q \longrightarrow^{\mathrm{s}}_w q - w * c = -a + \lambda = q_1$, but $p \not\longrightarrow^{\mathrm{s}}_{\{w,q_1\}}$. Trying to reduce ba by w or q_1 we get $w * a = \underline{aca} + ba, w * caba = ba + \underline{bcaba}$ and $q_1 * aba = -ba + \underline{aba}, q_1 * ba = -\underline{aba} + ba$ all violating condition (a) of definition 3.2. Trying to reduce b we get the same problem with $w * cab = b + \underline{bcab}, q_1 * ab = -b + \underline{a}$ and $q_1 * b = -\underline{ab} + b$.*

Nevertheless, strong right reduction has the essential properties which allow us to characterize a right ideal by reduction with respect to a set of generators, e.g. the translation lemma holds and the right ideal congruence can be described by reduction.

Lemma 3.7 *Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$ and $p, q, h \in \mathbf{K}[\mathcal{M}]$ some polynomials. Then the following statements hold:*

(1) Let $p - q \longrightarrow^{\mathrm{s}}_F h$. Then there are polynomials $p', q' \in \mathbf{K}[\mathcal{M}]$ such that we have $p \xrightarrow{*}{}^{\mathrm{s}}_F p', q \xrightarrow{*}{}^{\mathrm{s}}_F q'$ and $h = p' - q'$.

(2) Let 0 be a normal form of $p - q$ with respect to $\longrightarrow^{\mathrm{s}}_F$. Then there exists a polynomial $g \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}{}^{\mathrm{s}}_F g$ and $q \xrightarrow{*}{}^{\mathrm{s}}_F g$.

(3) $p \xleftrightarrow{*}{}^{\mathrm{s}}_F q$ if and only if $p - q \in \mathsf{ideal}_r(F)$.

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

Definition 3.8 *A set $G \subseteq \mathbf{K}[\mathcal{M}]$ is called a* **Gröbner basis** *with respect to the reduction $\longrightarrow^{\mathrm{s}}$ or a* **strong Gröbner basis** *of $\mathsf{ideal}_r(G)$, if $\xleftrightarrow{*}{}^{\mathrm{s}}_G = \equiv_{\mathsf{ideal}_r(G)}$, and $\longrightarrow^{\mathrm{s}}_G$ is confluent.*

Notice that by lemma 3.7 we have

[11] This property is important for introducing interreduction to a completion procedure.

Lemma 3.9 *For a set of polynomials G in $\mathbf{K}[\mathcal{M}]$, G is a strong Gröbner basis of $\mathsf{ideal}_r(G)$ if and only if for all $g \in \mathsf{ideal}_r(G)$ we have $g \xrightarrow{*}{}^{\mathrm{s}}_{G} 0$.*

Unlike in Buchberger's case a polynomial itself need not be a Gröbner basis of the right ideal it generates.

Example 3.10 *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 monoid presentation of a group $\mathcal{G}$ with with a length-lexicographical ordering induced by $a \succ b \succ c$. Further, let us consider the polynomial $p = a + b + c \in \mathbf{Q}[\mathcal{G}]$. Then $\longrightarrow^{\mathrm{s}}_{p}$ is not confluent on $\mathsf{ideal}_r(p)$, as we can strongly right reduce $a + b + c \longrightarrow^{\mathrm{s}}_{p} b - \lambda$ using $p * b = c + \lambda + \underline{a}$ and $a + b + c \longrightarrow^{\mathrm{s}}_{p} 0$, but although $b - \lambda \in \mathsf{ideal}_r(p)$, $b - \lambda \not\xrightarrow{*}{}^{\mathrm{s}}_{p} 0$, as for all $w \in \mathcal{G}$, $\mathsf{HT}(p * w) \neq b$.*

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 strong right reduction as situations were both polynomials can be applied for strong reduction.

Definition 3.11 *Given two non-zero polynomials*[12] *$p_1, p_2 \in \mathbf{K}[\mathcal{M}]$, every pair of elements $w_1, w_2 \in \mathcal{M}$ such that $\mathsf{HT}(p_1 * w_1) = \mathsf{HT}(p_2 * w_2)$, defines a* **strong s-polynomial**

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

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 strong s-polynomial will be called non-trivial in case it is non-zero and notice that we always have $\mathsf{HT}(\mathsf{spol}_s(p_1, p_2, w_1, w_2)) \prec \mathsf{HT}(p_1 * w_1) = \mathsf{HT}(p_2 * w_2)$.

Example 3.12 *Reviewing example 3.10 we find that a polynomial can have a non-trivial strong s-polynomial with itself. In fact since $\mathsf{HT}(a + b + c) = a = \mathsf{HT}((a + b + c) * b)$ we get that $(\lambda, b) \in U_{a+b+c,a+b+c}$ gives rise to a strong s-polynomial*

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

This phenomenon, which differs from the one for free monoid rings, is due to the fact that the definition of critical situations no longer only involves the head terms of the respective polynomials but the whole polynomials. The set U_{p_1,p_2} is contained in the set of all solutions in $\mathcal{M}$ to the equations in two variables of the form $u \circ \mathrm{x} = v \circ \mathrm{y}$ where $u \in \mathsf{T}(p_1)$ and $v \in \mathsf{T}(p_2)$. It can be empty, finite or even infinite. We can now give a criterion that implies confluence for strong right reduction in terms of strong s-polynomials.

Theorem 3.13 *For a set F of polynomials in $\mathbf{K}[\mathcal{M}]$, the following statements are equivalent:*

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

(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 $\mathsf{spol}_s(f_k, f_l, w_k, w_l) \xrightarrow{*}{}^{\mathrm{s}}_{F} 0$.

[12] Notice that $p_1 = p_2$ is possible.

Notice that this theorem, although characterizing a strong Gröbner basis by strong s-polynomials, in general does not give a finite test to check whether a set is a strong Gröbner basis, since in general infinitely many strong s-polynomials have to be considered. Later on we will see that the right ideal generated by $a+b+c$ in example 3.10 has finite strong Gröbner bases and we will show how to compute such a basis.

The following example shows how already two polynomials can cause infinitely many critical situations.

Example 3.14 *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 $a \succ b \succ c \succ d \succ e \succ f$. Further consider two polynomials $p_1 = a + f, p_2 = bf + a \in \mathbf{Q}[\mathcal{M}]$. Then we get infinitely many critical situations*

$$\mathsf{HT}(p_1 * (bc)^i dw) = f \circ (bc)^i dw = bf \circ (bc)^{i-1} dw = \mathsf{HT}(p_2 * (bc)^{i-1} dw),$$

where $i \in \mathbf{N}^+, w \in \mathcal{M}$, giving rise to infinitely many strong s-polynomials

$$\mathsf{spol}_s(p_1, p_2, (bc)^i dw, (bc)^{i-1} dw) = (a+f) * (bc)^i dw - (bf+a) * (bc)^{i-1} dw$$

and $U_{p_1,p_2} = \{((bc)^i dw, (bc)^{i-1} dw) \mid i \in \mathbf{N}^+, w \in \mathcal{M}\}$.

Notice that in contrary to the definition of s-polynomials in commutative polynomial rings in this example there are infinitely many strong s-polynomials originating from p_1 and p_2 which *cannot* be expressed by monomial multiples of one or even a finite set of these s-polynomials. Therefore, localization of critical situations in general is very hard. As example 3.14 shows, the set U_{p_1,p_2} need not have a "suitable finite basis", e.g. there need not exist a finite set $B \subseteq U_{p_1,p_2}$ such that for every pair $(w_1, w_2) \in U_{p_1,p_2}$ there exists a pair $(u_1, u_2) \in B$ and an element $w \in \mathcal{M}$ with $u_1 \circ w = w_1$ and $u_2 \circ w = w_2$. The subset $\{((bc)^i d, (bc)^{i-1} d) \mid i \in \mathbf{N}^+\} \subset U_{p_1,p_2}$ is such a basis, but it is not finite and there is in fact no finite one.

It turns out that the following uniform problem is undecidable, even in monoids where the solvability of equations of the form $u \circ \mathrm{x} = v \circ \mathrm{y}$ is decidable.

Given: Two polynomials $p, q \in \mathbf{K}[\mathcal{M}]$, and
(Σ, T) a convergent semi-Thue system presenting $\mathcal{M}$.
Question: Does there exist a strong s-polynomial for p and q?

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 strong right reduction we studied is called 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. Hence, reduction defined in this way can be called "stable" and resembles Buchberger's definition of reduction. The results can be found in [MaRe93b, Re95].

In the following we will introduce a further weakening of strong reduction using prefixes in Σ^*. Notice that such prefixes are divisors with respect to word concatenation and hence easy to determine.

Definition 3.15 *Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{M}]$. 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) $q = p - \alpha \cdot \mathsf{HC}(f)^{-1} \cdot f * w$.

We write $p \longrightarrow^{\mathrm{p}}_f$ if there is a polynomial q as defined above and p is then called prefix reducible by f. Prefix reduction by a set $F \subseteq \mathbf{K}[\mathcal{M}]$ is denoted by $p \longrightarrow^{\mathrm{p}}_F q$ and abbreviates $p \longrightarrow^{\mathrm{p}}_f q$ for some $f \in F$.

Notice that in the above definition the equation in (a) has at most one solution and we then always have $\mathsf{HC}(f * w) = \mathsf{HC}(f)$. This is due to the fact that $t \equiv \mathsf{HT}(f)w$ implies $\mathsf{HT}(f)w = \mathsf{HT}(f * w)$ and $\mathsf{HT}(f)w \succ s \circ w$ for all $s \in \mathsf{T}(f - \mathsf{HM}(f))$. Further, in case f prefix reduces p to q at the monomial $\alpha \cdot t$, we have $t \notin \mathsf{T}(q)$ and $p > q$. In case $\mathcal{M}$ is the free monoid strong and prefix reduction coincide and are in fact Mora's reduction for treating right ideals in the free monoid ring. The statements (1) to (3) of lemma 3.5 can be carried over to prefix reduction. But it is no longer true that $p * w \longrightarrow^{\mathrm{p}}_p 0$ in case $p * w \neq 0$.

Example 3.16 *Let $\Sigma = \{a, b\}$ and $T = \{ab \longrightarrow \lambda, ba \longrightarrow \lambda\}$ be a monoid presentation of a group $\mathcal{G}$ with a length-lexicographical ordering induced by $a \succ b$. Further let $p = a^2 + 1 \in \mathbf{Q}[\mathcal{G}]$. Then $p * b = a + b$ is not prefix reducible to zero by p.*

As before, we can show that the translation lemma holds for prefix reduction.

Lemma 3.17 *Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$ and $p, q, h \in \mathbf{K}[\mathcal{M}]$ some polynomials. Then the following statements hold:*

(1) Let $p - q \longrightarrow^{\mathrm{p}}_F h$. Then there are $p', q' \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}{}^{\mathrm{p}}_F p', q \xrightarrow{*}{}^{\mathrm{p}}_F q'$ and $h = p' - q'$.

(2) Let 0 be a normal form of $p - q$ with respect to $\longrightarrow^{\mathrm{p}}_F$. Then there exists a polynomial $g \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}{}^{\mathrm{p}}_F g$ and $q \xrightarrow{*}{}^{\mathrm{p}}_F g$.

Furthermore, $p \longrightarrow^{\mathrm{p}}_q$ and $q \longrightarrow^{\mathrm{p}}_w q$ imply $p \longrightarrow^{\mathrm{p}}_{\{w,q\}}$, i.e. the axioms (A1), (A2), (A3) and (A4) hold. Unfortunately, prefix reduction need not capture the right ideal congruence.

Lemma 3.18 *Let $p, q \in \mathbf{K}[\mathcal{M}]$ and $F \subseteq \mathbf{K}[\mathcal{M}]$. Then $p \xleftrightarrow{*}{}^{\mathrm{p}}_F q$ implies $p - q \in \mathsf{ideal}_r(F)$ but not vice versa.*

Example 3.19 *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 $p = a+b+c, q = b-\lambda \in \mathbf{Q}[\mathcal{G}]$ and the set $F = \{a+b+c\} \subseteq \mathbf{Q}[\mathcal{G}]$ we get $p - q = a + c + \lambda = (a + b + c) * b \in \mathsf{ideal}_r(F)$, but $a + b + c \xleftrightarrow{*}{\not\longrightarrow}{}^{\mathrm{p}}_F b - \lambda$. To prove this claim, let us assume $a + b + c \xleftrightarrow{*}{}^{\mathrm{p}}_F b - \lambda$. Then, since $a + b + c \longrightarrow^{\mathrm{p}}_F 0$, we get $b - \lambda \xleftrightarrow{*}{}^{\mathrm{p}}_F 0$. Let $n \in \mathbf{N}^+$ be minimal such that $b - \lambda \xleftrightarrow{n}{}^{\mathrm{p}}_F 0$. As $b - \lambda \not\longrightarrow^{\mathrm{p}}_F 0$ we know $n > 1$. Thus, let us look at the sequence*

$$b - \lambda =: p_0 \longleftrightarrow^{\mathrm{p}}_F p_1 \longleftrightarrow^{\mathrm{p}}_F \ldots \longleftrightarrow^{\mathrm{p}}_F p_{n-1} \longleftrightarrow^{\mathrm{p}}_F 0,$$

where for all $1 \leq i \leq n-1$, $p_i = p_{i-1} + \alpha_i \cdot (a+b+c) * w_i$, $\alpha_i \in \mathbf{K}^*, w_i \in \mathcal{G}$ *and* $\mathsf{HT}((a+b+c) * w_i) \equiv aw_i$. *Further let* $t = \max\{\mathsf{HT}(p_i) \mid 1 \leq i \leq n-1\}$. *Then* $t \succ b$, *as* $aw \succ b$ *for all* $w \in \mathcal{G}$ *such that* $a \circ w \equiv aw$. *Let* p_l *be the first polynomial with* $\mathsf{HT}(p_l) = t$, *i.e.,* $\mathsf{HT}(p_j) \prec t$ *for all* $j < l$, *and let* p_{l+k} *be the next polynomial, where the occurrence of* t *is changed. Since* $\mathsf{HT}((a+b+c) * w_{l+k}) \equiv aw_{l+k} \equiv t \equiv aw_l \equiv \mathsf{HT}((a+b+c) * w_l)$ *we can conclude* $w_{l+k} \equiv w_l$. *Further our transformation sequence is supposed to be of minimal length, i.e.,* t *is not changed by the reductions taking place in the sequence* $p_l \overset{k-1}{\longleftrightarrow}{}^{\mathrm{p}}_F p_{l+k-1}$. *But then, eliminating* p_l *and substituting* p_{l+j} *by* $p'_{l+j} = p_{l+j} - \alpha_l \cdot (a+b+c) * w_l$ *for all* $1 \leq j < k$ *gives us a shorter sequence* $b - \lambda \overset{n-1}{\longleftrightarrow}{}^{\mathrm{p}}_F 0$ *contradicting our assumption.*

Obviously for a set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$ we have $\longrightarrow^{\mathrm{p}}_F \subseteq \longrightarrow^{\mathrm{s}}_F$, but as seen in example 3.19 in general we cannot expect $\overset{*}{\longleftrightarrow}{}^{\mathrm{p}}_F = \overset{*}{\longleftrightarrow}{}^{\mathrm{s}}_F$. This can be gained by enriching the set F to a set F' such that $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(F')$ and $\overset{*}{\longleftrightarrow}{}^{\mathrm{p}}_{F'} = \overset{*}{\longleftrightarrow}{}^{\mathrm{s}}_F$. This will be achieved by a process called prefix saturation.

Definition 3.20 *A set of polynomials* $F \subseteq \{\alpha \cdot p * w \mid \alpha \in \mathbf{K}^*, w \in \mathcal{M}\}$ *is called a* **prefix saturating set** *for a non-zero polynomial* $p \in \mathbf{K}[\mathcal{M}]$, *if for all* $w \in \mathcal{M}$, *in case* $p * w \neq 0$ *then* $p * w \longrightarrow^{\mathrm{p}}_F 0$ *holds.* $\mathcal{SAT}_p(p)$ *denotes the family of all prefix saturating sets for* p.

Definition 3.21 *We call a set* $F \subseteq \mathbf{K}[\mathcal{M}]$ **prefix saturated**, *if for all* $f \in F$ *and all* $w \in \mathcal{M}$, $f * w \longrightarrow^{\mathrm{p}}_F 0$ *holds in case* $f * w \neq 0$.

Note that in defining prefix saturating sets we demand prefix reducibility to 0 in *one* step. This is done to have some equivalent for $p * w \longrightarrow_p 0$ in Buchberger's approach and the fact that for strong right reduction we have $p * w \longrightarrow_p 0$ in case $p * w \neq 0$. Other definitions of similar properties are possible and can be found in [Ap88, Kr93, Re95].

Of course there are procedures to enumerate prefix saturating sets of a polynomial p, since the set $\{p * w \mid w \in \mathcal{M}\}$ is recursively enumerable, and it is decidable whether $q \longrightarrow^{\mathrm{p}}_F 0$ for some $q \in \mathbf{K}[\mathcal{M}]$ and $F \subset \mathbf{K}[\mathcal{M}]$ finite. But in general the set $\{p * w \mid w \in \mathcal{M}\}$ is infinite and, hence, we have to look for "suitable" subsets and to find and compute finite ones in case they exist. Note that prefix saturating sets for a polynomial p are prefix saturated. A nice property of prefix saturated sets is that they allow special representations of the elements belonging to the right ideal they generate.

Lemma 3.22 *Let* $F \subseteq \mathbf{K}[\mathcal{M}]$ *be a prefix saturated set. Then every non-zero polynomial* $g \in \mathsf{ideal}_r(F)$ *has a representation of the form* $g = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$ *with* $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$, *and* $\mathsf{HT}(f_i * w_i) \equiv \mathsf{HT}(f_i) w_i$.

In fact using prefix reduction combined with prefix saturation we can simulate strong right reduction and therefore we can then capture the right ideal congruence.

Lemma 3.23 *For* $f, g, p \in \mathbf{K}[\mathcal{M}]$ *and* $S \in \mathcal{SAT}_p(p)$, $f \longrightarrow^{\mathrm{s}}_p g$ *if and only if* $f \longrightarrow^{\mathrm{p}}_S g$.

Lemma 3.24 *For a prefix saturated set* F *of polynomials in* $\mathbf{K}[\mathcal{M}]$ *and* $p, q \in \mathbf{K}[\mathcal{M}]$ *we have* $p \overset{*}{\longleftrightarrow}{}^{\mathrm{p}}_F q$ *if and only if* $p - q \in \mathsf{ideal}_r(F)$.

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 semi-Thue 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 $p \in \mathbf{K}[\mathcal{M}]$ and
(Σ, T) a convergent semi-Thue system presenting $\mathcal{M}$.
Find: $S \in \mathcal{SAT}_p(p)$.

$S := \{p\}$;
$H := \{p\}$;
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 $q' \not\rightarrow_S^{\mathrm{p}} 0$ and $q' \neq 0$
      then $S := S \cup \{q'\}$;
        $H := H \cup \{q'\}$;
    endif
  endfor
endwhile

Theorem 3.25 *For a given polynomial $p \in \mathbf{K}[\mathcal{M}]$, let S be the set generated by procedure* PREFIX SATURATION. *Then for all $w \in \mathcal{M}$ every non-zero polynomial $p * w$ is prefix reducible to zero in one step using S.*

Hence, procedure PREFIX SATURATION enumerates a prefix saturating set for a polynomial and we find:

Lemma 3.26 *In case a polynomial has a finite prefix saturating set, then procedure* PREFIX SATURATION *terminates.*

This is the case e.g. for monoids with a finite convergent monadic presentation. Similar to definition 3.8 we can define Gröbner bases with respect to prefix reduction.

Definition 3.27 *A set $G \subseteq \mathbf{K}[\mathcal{M}]$ is said to be a* **prefix Gröbner basis** *of $\mathsf{ideal}_r(G)$, if $\overset{*}{\longleftrightarrow}{}_G^{\mathrm{p}} = \equiv_{\mathsf{ideal}_r(G)}$, and $\longrightarrow_G^{\mathrm{p}}$ 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 3.28 *Reviewing example 3.19, let* $p = a + b + c$. *Then* $S = \{a + b + c, a + c + \lambda, bc + c^2 + b, ba + ca + \lambda, ca + a + \lambda, c^2 + b + c\} \in \mathcal{SAT}_p(p)$, *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* $b-\lambda \not\xrightarrow{*}{}^{\mathrm{p}}_S 0$.

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. Remember that prefix saturation enriches a polynomial p to a set $S \in \mathcal{SAT}_p(p)$ such that we can substitute $q \longrightarrow^{\mathrm{s}}_p q'$ by $q \longrightarrow^{\mathrm{p}}_{p' \in S} q'$. We use this additional information to give a confluence criterion that will use a refined definition of s-polynomials.

Definition 3.29 *Given two non-zero polynomials* $p_1, p_2 \in \mathbf{K}[\mathcal{M}]$, *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*

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

As before non-zero prefix s-polynomials are called non-trivial. In case an s-polynomial exists we always have $\mathsf{HT}(\mathsf{spol}_p(p_1, p_2)) \prec \mathsf{HT}(p_1) \equiv \mathsf{HT}(p_2)w$. Notice that a finite set $F \subseteq \mathbf{K}[\mathcal{M}]$ defines finitely many prefix s-polynomials and the following lemma enables us to localize our confluence test to these s-polynomials.

Lemma 3.30 *Let* F *be a set of polynomials in* $\mathbf{K}[\mathcal{M}]$ *and* $p \in \mathbf{K}[\mathcal{M}]$. *Further let* $p \xrightarrow{*}{}^{\mathrm{p}}_F 0$ *and let us assume this reduction sequence results in a representation* $p = \sum_{i=1}^{k} \alpha_i \cdot g_i * w_i$, *where* $\alpha_i \in \mathbf{K}^*$, $g_i \in F$, *and* $w_i \in \mathcal{M}$. *Then for every term* $t \in \mathcal{M}$ *such that* $t \succ \mathsf{HT}(p)$ *and every term* $w \in \mathcal{M}$ *we get that if* $s \in \bigcup_{i=1}^{k} \mathsf{T}(g_i * w_i * w)$ *then* $tw \succ s$ *holds.*

Prefix s-polynomials alone are not sufficient to characterize prefix Gröbner bases, but in case we demand our set of polynomials to be prefix saturated we can give a characterization similar to theorem 3.13.

Theorem 3.31 *For a prefix saturated set* F *of polynomials in* $\mathbf{K}[\mathcal{M}]$, *the following statements are equivalent:*

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

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

Corollary 3.32 *A prefix saturated set* $F \subseteq \mathbf{K}[\mathcal{M}]$ *is a prefix Gröbner basis of* $\mathsf{ideal}_r(F)$ *if and only if for all* $g \in \mathsf{ideal}_r(F)$ *we have* $g \xrightarrow{*}{}^{\mathrm{p}}_F 0$.

Now theorem 3.31 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. Termination will be shown for some special cases where finite prefix saturated Gröbner bases exist in the next section.

Procedure: Prefix Gröbner Bases

Given: A finite set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$, and
(Σ, T) a convergent semi-Thue system presenting $\mathcal{M}$.
Find: $\mathrm{GB}(F)$ a prefix Gröbner basis of F.
Using: SAT_p a prefix saturating procedure for polynomials.

$G := \bigcup_{f \in F} \text{SAT}_p(f)$;
% 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 3.31 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$(\mathsf{spol}_p(q_1, q_2), \longrightarrow_G^{\text{p}})$;
                % Compute a normal form using prefix reduction
                if $h \neq 0$
                    then $G := G \cup \text{SAT}_p(h)$;
                            % G is prefix saturated
                            $B := B \cup \{(f, \tilde{h}), (\tilde{h}, f) \mid f \in G, \tilde{h} \in \text{SAT}_p(h)\}$;
                endif
    endif
endwhile
$\text{GB}(F) := G$

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. In the next section certain groups with very simple finite prefix saturating sets are presented. 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. This results in a more technical procedure.

Termination of procedure PREFIX GRÖBNER BASES can be shown e.g. for finite convergent special monoid or monadic group presentations. More details on this subject are provided in the next section.

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 3.10.

Example 3.33 *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* $G = \{a+b+c, a+c+\lambda, bc+c^2+b, ba+ca+\lambda, ca+a+\lambda, c^2+b+c\}$ *(compare example 3.28).*
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

$$\mathsf{spol}_p(bc + c^2 + b, b - \lambda) = c^2 + b + c \longrightarrow_G^{\text{p}} 0$$

respectively

$$\mathsf{spol}_p(ba + ca + \lambda, b - \lambda) = ca + a + \lambda \longrightarrow_G^{\text{p}} 0$$

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* $\mathsf{ideal}_r(a+b+c)$.

Furthermore, theorem 3.31 characterizes prefix saturated prefix Gröbner bases. But prefix Gröbner bases need not be prefix saturated. In [Re95] we have hence given other characterizations of prefix Gröbner bases and introduced the concept of interreduction to the theory. Using those results we can even state that for $\mathsf{ideal}_r(a+b+c)$ in example 3.33 the set $\{a+c+\lambda, ca-c, c^2+c+\lambda, b-\lambda\}$ is a reduced prefix Gröbner basis. We close this section by showing how similar to the case of solvable polynomial rings ([Kr93, KaWe90]), Gröbner bases of two-sided ideals can be characterized by prefix reduction and prefix Gröbner bases which have additional properties. We will call a set of polynomials a **Gröbner basis** of the two-sided ideal it generates, if it fulfills one of the equivalent statements in the next theorem.

Theorem 3.34 *For a set of polynomials* $G \subseteq \mathbf{K}[\mathcal{M}]$, *assuming that* $\mathcal{M}$ *is presented by* (Σ, T) *as described above, the following properties are equivalent:*

(1) G *is a prefix Gröbner basis of* $\mathsf{ideal}_r(G)$ *and* $\mathsf{ideal}_r(G) = \mathsf{ideal}(G)$.

(2) For all $g \in \mathsf{ideal}(G)$ *we have* $g \xrightarrow{*}{}^{\mathrm{p}}_{G} 0$.

(3) G *is a prefix Gröbner basis of* $\mathsf{ideal}_r(G)$ *and for all* $w \in \mathcal{M}$, $g \in G$ *we have* $w * g \in \mathsf{ideal}_r(G)$.

(4) G *is a prefix Gröbner basis of* $\mathsf{ideal}_r(G)$ *and for all* $a \in \Sigma$, $g \in G$ *we have* $a * g \in \mathsf{ideal}_r(G)$.

Statement 4 enables a constructive approach to extend procedure Prefix Gröbner Bases in order to enumerate prefix Gröbner bases of two-sided ideals (and in fact in case prefix saturation always terminates this procedure will compute finite prefix saturated Gröbner bases in case they exist). Item 2 states how prefix Gröbner bases are related to the membership problem for two-sided ideals. In this case if $\mathbf{K}[\mathcal{M}]$ is a right reduction ring and G is a finite prefix Gröbner basis of $\mathsf{ideal}(G)$, then $\mathbf{K}[\mathcal{M}]/\mathsf{ideal}(G)$ is a right reduction ring.

4 Group Rings

In this section we show how structural information on certain classes of groups can be used to prove termination of procedure Prefix Gröbner Bases and to improve it. Let us start with the classes of finite, free respectively plain groups. These groups have in common that they can be presented using convergent 2-monadic group presentations, i.e., Σ contains inverses of length one for all generators and for all rules $(l,r) \in T$, $|l| \leq 2$ and $|r| \leq 1$ hold. In fact finite or free groups are also plain groups, but sometimes it is useful to take advantage of the additional information we have concerning them. For example we can improve the process of saturation. Given a non-trivial group element w we let $\ell(w)$ denote the last letter and $\mathsf{inv}(w)$ the inverse of w.

Definition 4.1 *For a polynomial $p \in \mathbf{K}[\mathcal{G}]$ which has more than one monomial, we define*

$$\sigma(p) \;=\; \max\{u \in \mathcal{G} \mid \mathsf{HT}(p * u) = \mathsf{HT}(p) \circ u \text{ is a prefix of } \mathsf{HT}(p)\}.$$

Then we can set $\mathsf{can}(p) = p * \sigma(p)$ *and* $\mathsf{acan}(p) = \mathsf{can}(p) * \mathsf{inv}(\ell(\mathsf{HT}(\mathsf{can}(p))))$. *For a non-zero polynomial* $\alpha \cdot t \in \mathbf{K}[\mathcal{G}]$ *we set* $\sigma(p) = \mathsf{inv}(t)$ *and* $\mathsf{can}(p) = \mathsf{acan}(p) = \alpha$.

Notice that $\mathsf{HT}(\mathsf{can}(p)) = \mathsf{HT}(p) \circ \sigma(p)$, but in case p has more than one monomial $\mathsf{HT}(\mathsf{acan}(p)) \neq \mathsf{HT}(p) \circ \sigma(p) \circ \mathsf{inv}(\ell(\mathsf{HT}(\mathsf{can}(p))))$.

Example 4.2 *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* $a \succ b$. *Then for the polynomial* $p = b^4 + b^2 + \lambda \in \mathbf{Q}[\mathcal{G}]$ *we get* $\sigma(p) = a$, $\mathsf{can}(p) = p * \sigma(p) = \underline{b^3} + b + a$, *and* $\mathsf{acan}(p) = p * a^2 = b^2 + \lambda + \underline{a^2}$.

These polynomials can be used to define prefix saturating sets.

Lemma 4.3 *Let* $p \in \mathbf{K}[\mathcal{G}]$ *contain more than one monomial. Then the following statements hold:*

(1) In case $\mathcal{G}$ *is a free group presented by* (Σ, T_I), *then* $\textsc{Sat}_p(p) = \{\mathsf{can}(p), \mathsf{acan}(p)\}$ *is a prefix saturating set for* p.

(2) In case $\mathcal{G}$ *is a plain group presented by a reduced convergent 2-monadic group system* (Σ, T), $a = \ell(\mathsf{HT}(\mathsf{can}(p)))$ *and* $a' = \ell(\mathsf{HT}(\mathsf{acan}(p)))$, *then* $\textsc{Sat}_p(p) = \{\mathsf{can}(p), \mathsf{can}(p) * b \mid (ab, c) \in T\} \cup \{\mathsf{acan}(p), \mathsf{acan}(p) * b \mid (a'b, c) \in T\}$ *is a prefix saturating set for* p.

Then we can compute finite prefix Gröbner bases of finitely generated right ideals for plain group rings using procedure Prefix Gröbner Bases and specifying saturating sets as described in lemma 4.3.

Theorem 4.4 *Given a 2-monadic confluent group presentation for a group* $\mathcal{G}$ *and a finite set of polynomials* $F \subseteq \mathbf{K}[\mathcal{G}]$, *procedure* Prefix Gröbner Bases *terminates.*

We continue to show how we can gain a similar result for context-free group rings. A finitely generated context-free group $\mathcal{G}$ is a group with a free normal subgroup of finite index. Hence, let the group $\mathcal{G}$ be given by X a finite set of generators for a free subgroup $\mathcal{F}$ and $\mathcal{E}$ a finite group such that $(\mathcal{E}\backslash\{\lambda\}) \cap X = \emptyset$ and $\mathcal{G}/\mathcal{F} \cong \mathcal{E}$. For all $e \in \mathcal{E}$ let $\phi_e : X \cup X^{-1} \longrightarrow \mathcal{F}$ be a function such that ϕ_λ is the inclusion and for all $x \in X \cup X^{-1}$, $\phi_e(x) = \mathsf{inv}(e) \circ_{\mathcal{G}} x \circ_{\mathcal{G}} e$. For all $e_1, e_2 \in \mathcal{E}$ let $z_{e_1,e_2} \in \mathcal{F}$ such that $z_{e_1,\lambda} \equiv z_{\lambda,e_1} \equiv \lambda$ and for all $e_1, e_2, e_3 \in \mathcal{E}$ with $e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3$, $e_1 \circ_{\mathcal{G}} e_2 \equiv e_3 z_{e_1,e_2}$. Let $\Sigma = (\mathcal{E}\backslash\{\lambda\}) \cup X \cup X^{-1}$ and let T contain the following rules:

xx^{-1}	$\longrightarrow$	λ	and
$x^{-1}x$	$\longrightarrow$	λ	for all $x \in X$,
e_1e_2	$\longrightarrow$	$e_3 z_{e_1,e_2}$	for all $e_1, e_2 \in \mathcal{E}\backslash\{\lambda\}, e_3 \in \mathcal{E}$ such that $e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3$,
xe	$\longrightarrow$	$e\phi_e(x)$	and
$x^{-1}e$	$\longrightarrow$	$e\phi_e(x^{-1})$	for all $e \in \mathcal{E}\backslash\{\lambda\}, x \in X$.

(Σ, T) then is convergent and is called a virtually free presentation (compare [CrOt94]). Presenting $\mathcal{G}$ in this way we find that the elements of the group are of the form eu where $e \in \mathcal{E}$ and $u \in \mathcal{F}$. We can specify a total well-founded ordering on the group by combining a total well-founded ordering $\succeq_{\mathcal{E}}$ on $\mathcal{E}$ and a length-lexicographical ordering $\geq_{\text{lex}}$ on $\mathcal{F}$: Let $w_1, w_2 \in \mathcal{G}$ such that $w_i \equiv e_i u_i$ where $e_i \in \mathcal{E}$, $u_i \in \mathcal{F}$. Then we define $w_1 \succ w_2$ if and only if $|w_1| > |w_2|$ or ($|w_1| = |w_2|$ and $e_1 \succ_{\mathcal{E}} e_2$) or ($|w_1| = |w_2|$, $e_1 =_{\mathcal{E}} e_2$ and $u_1 >_{\text{lex}} u_2$). This ordering is compatible with right concatenation using elements in $\mathcal{F}$ in the following sense: Given $w_1, w_2 \in \mathcal{G}$ presented as described above, $w_1 \succ w_2$ implies $w_1 u \succ w_2 u$ for all $u \in \mathcal{F}$ in case $w_1 u, w_2 u \in \mathcal{G}$.

Example 4.5 *Let $\mathcal{E}$ be the finite group presented by $\Sigma' = \{a\}$ and $T' = \{a^2 \longrightarrow \lambda\}$ and $\mathcal{F}$ the free group generated by $X = \{x\}$. Further let $\phi_a(x) = x$ and $\phi_a(x^{-1}) = x^{-1}$ be a conjugation homomorphism. Then $\Sigma = \{a, x, x^{-1}\}$ and $T = \{xx^{-1} \longrightarrow \lambda, x^{-1}x \longrightarrow \lambda\} \cup \{a^2 \longrightarrow \lambda\} \cup \{xa \longrightarrow ax, x^{-1}a \longrightarrow ax^{-1}\}$ is a virtually free presentation of $\mathcal{G}$, the direct product of $\mathcal{E}$ and $\mathcal{F}$.*

Let us take a closer look at prefix reduction in $\mathbf{K}[\mathcal{G}]$.

Example 4.6 *Let $\mathcal{G}$ be the group specified in example 4.5. Further let $p = ax^2 + x + \lambda$, $q_1 = a + x$ and $q_2 = x^2 + \lambda$ be polynomials in $\mathbf{Q}[\mathcal{G}]$.*
Then the polynomial p is prefix reducible at its head term ax^2 by q_1 giving us

$$p \longrightarrow^{\text{p}}_{q_1} p - q_1 * x^2 = \underline{ax^2} + x + \lambda - \underline{ax^2} - x^3 = x + \lambda + \underline{x^3}.$$

On the other hand, as x^2 is no prefix of ax^2, this is not true for q_2.

Since prefix reduction using a non-constant[13] polynomial involves right multiples of the polynomial with elements in $\mathcal{F}$ only, we can restrict ourselves to special prefix-saturating sets.

Definition 4.7 *A set $F \subseteq \{\alpha \cdot p * w \mid \alpha \in \mathbf{K}^*, w \in \mathcal{F}\}$ is called a* **$\mathcal{F}$-prefix saturating set** *for a non-zero polynomial p in $\mathbf{K}[\mathcal{G}]$, if for all $w \in \mathcal{F}$ the polynomial $p * w$ is prefix reducible to zero using F in one step. A set of polynomials $F \subseteq \mathbf{K}[\mathcal{G}]$ is called a* **$\mathcal{F}$-prefix saturated set**, *if for all $f \in F$ and for all $w \in \mathcal{F}$ the polynomial $f * w$ is prefix reducible to zero using F in one step.*

Reviewing the results on free groups, for a polynomial p in $\mathbf{K}[\mathcal{G}]$ we can specify $\mathsf{can}(p)$ and $\mathsf{acan}(p)$ and use them to define $\mathcal{F}$-prefix saturating sets.

Definition 4.8 *For a non-zero polynomial $p \in \mathbf{K}[\mathcal{G}]$ containing more than one monomial we define*

$$\sigma(p) = \max\{u \in \mathcal{F} \mid \mathsf{HT}(p * u) = \mathsf{HT}(p) \circ u \text{ is a prefix of } \mathsf{HT}(p)\}$$

and set $\mathsf{can}(p) = p * \sigma(p)$. In case $\mathsf{HT}(p) \neq e\mathsf{inv}(\sigma(p))$ for $e \in \mathcal{E}$ we define $\mathsf{acan}(p) = \mathsf{can}(p) * \mathsf{inv}(\ell(\mathsf{can}(p)))$ and else $\mathsf{acan}(p) = \mathsf{can}(p)$. For a polynomial $p = \alpha \cdot t \in \mathbf{K}[\mathcal{G}]$ we set $\mathsf{can}(p) = \mathsf{acan}(p) = \alpha$.

[13] A constant polynomial is an element in $\mathbf{K}$.

Lemma 4.9 *For a non-zero polynomial p in $\mathbf{K}[\mathcal{G}]$ the set $\{\mathsf{can}(p), \mathsf{acan}(p)\}$ is a $\mathcal{F}$-prefix saturating set.*

Example 4.10 *Let $\mathcal{G}$ be the group specified in example 4.5 and $p = ax^2 + x + \lambda$ a polynomial in $\mathbf{Q}[\mathcal{G}]$. Then the polynomials $p * x^{-1} = \underline{ax} + \lambda + x^{-1} = \mathsf{can}(p)$ and $p * x^{-2} = a + x^{-1} + \underline{x^{-2}} = \mathsf{acan}(p)$ give us a $\mathcal{F}$-prefix-saturating set for p.*

The following lemma will be used as an analogon to lemma 3.30 when we characterize prefix Gröbner bases by using prefix reduction, prefix s-polynomials and now $\mathcal{F}$-prefix saturated sets.

Lemma 4.11 *Let p be a non-zero polynomial and F a set of polynomials in $\mathbf{K}[\mathcal{G}]$. Then $p \xrightarrow{*}{}^{\mathrm{p}}_{F} 0$ gives us a representation of $p = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{G}$ such that for all $w \in \mathcal{F}$ with $\mathsf{HT}(p * w) \equiv \mathsf{HT}(p)w$, we get $\mathsf{HT}(p)w \succeq \mathsf{HT}(f_i * w_i * w)$. In particular for all $t \in \mathcal{M}$ with $t \succeq \mathsf{HT}(p)$, if $t \circ w \equiv tw$ for some $w \in \mathcal{M}$, then $tw \succeq \mathsf{HT}(f_i * w_i * w)$ holds.*

For every $e \in \mathcal{E}$ let the mapping $\psi_e : \mathbf{K}[\mathcal{G}] \longrightarrow \mathbf{K}[\mathcal{G}]$ be defined by $\psi_e(f) := f * e$ for $f \in \mathbf{K}[\mathcal{G}]$. We now can give a characterization of prefix Gröbner bases by transforming a generating set for a right ideal using these finitely many mappings. This will enable us to restrict ourselves to $\mathcal{F}$-prefix saturated sets when characterizing prefix Gröbner bases.

Theorem 4.12 *Let $F \subseteq \mathbf{K}[\mathcal{G}]$ and $G \subseteq \mathbf{K}[\mathcal{G}]$ such that*

(a) $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$,

(b) $F \cup \{\psi_e(f) | f \in F, e \in \mathcal{E}\} \subseteq G$, *and*

(c) G *is $\mathcal{F}$-prefix saturated.*

Then the following statements are equivalent:

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

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

On first sight the characterization given in theorem 4.12 above might seem artificial. The crucial point is that in losing the property "admissible" for our ordering, an essential lemma in Buchberger's context, namely that $p \xrightarrow{*}_{F} 0$ implies $p * w \xrightarrow{*}_{F} 0$ for any term w, no longer holds. Defining reduction by restricting ourselves to prefixes we gain enough structural information to weaken this lemma, but we have to do additional work to still describe the right ideal congruence. One step is to close the set of polynomials generating the right ideal with respect to the finite group $\mathcal{E}$: For a set of polynomials F using the $\mathcal{E}$-closure $F_{\mathcal{E}} = \{\psi_e(f) \mid f \in F, e \in \mathcal{E}\}$ we can characterize the right ideal generated by F in terms of $F_{\mathcal{E}}$ since $\mathsf{ideal}_r(F) = \{\sum_{i=1}^{k} \alpha_i \cdot f_i * u_i \mid \alpha_i \in \mathbf{K}, f_i \in F_{\mathcal{E}}, u_i \in \mathcal{F}\}$. If we additionally incorporate the concept of saturation, prefix reduction can be used to express the right ideal congruence and then a prefix Gröbner basis can be characterized as usual by prefix s-polynomials. Now, using the characterization given in theorem 4.12 we can modify procedure PREFIX GRÖBNER BASES as follows:

Procedure: PREFIX GRÖBNER BASES IN CONTEXT-FREE GROUP RINGS

Given: A finite set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$, and
(Σ, T) a virtually free presentation of $\mathcal{G}$.
Find: $\text{GB}(F)$ a prefix Gröbner basis of F.

$G := \{\mathsf{can}(\psi_e(f)), \mathsf{acan}(\psi_e(f)) \mid e \in \mathcal{E}, f \in F\}$;
% G fulfills (a), (b) and (c) of theorem 4.12
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ **do**
    % Test if statement (2) of theorem 4.12 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$(\mathsf{spol}_p(q_1, q_2), \longrightarrow_G^{\mathrm{p}})$;
            % Compute a normal form using prefix reduction
            if $h \neq 0$
                then $G := G \cup \{\mathsf{can}(h), \mathsf{acan}(h)\}$;
                    % G fulfills (a), (b) and (c) of theorem 4.12
                    $B := B \cup \{(f, \tilde{h}), (\tilde{h}, f) \mid f \in G, \tilde{h} \in \{\mathsf{can}(h), \mathsf{acan}(h)\}\}$;
            endif
    endif
endwhile
$\text{GB}(F) := G$

Termination can be shown as in theorem 4.4.

Notice that the classes of groups studied in this section are known to have solvable subgroup problem. For free groups there is Nielsen's approach known as Nielsen reduction (compare [LySch77, AvMa84]). Kuhn and Madlener have developed prefix reduction methods and applied them successfully to the class of plain groups (see [KuMa89]). Cremanns and Otto successfully treated the class of context-free groups (see [CrOt94]).

5 Conclusions

We have shown how reduction can be introduced to monoid and group rings and how Gröbner bases can be characterized. Our approach involves techniques as saturation, since the general absence of a well-founded compatible ordering causes severe problems. The technique of saturating a set of rules or relations is frequently used by completion based approaches in computer algebra and theorem proving. E.g. symmetrization of a group as described by Le Chenadec [LeCh86], symmetrized sets for free Abelian group rings as defined by Sims [Si94], right orbits for free group rings as defined by Rosenmann [Ro93], or multiplication by non-Pommaret-multiplicatives as described by Zharkov and Blinkov [ZhBl93] all have the same idea in common and can be subsumed under the concept of saturation. In fact the methods of Sims and Rosenmann correspond to special cases of our approach. The method of Zharkov and Blinkov and their definition of involutive bases which

Apel has compared to Gröbner bases in [Ap95], corresponds directly to the computation of interreduced suffix Gröbner bases in the commutative polynomial ring viewed as a free commutative monoid ring.

The weakening of strong right reduction presented here is prefix reduction. This reduction has a finitary local confluence test and terminating procedures to compute finite prefix Gröbner bases for finitely generated right ideals in the classes of finite, free, plain respectively context-free groups, were given. So all these rings are examples of effective one-sided reduction rings. An implementation is on the way. Furthermore, in [Re95] we have shown that prefix reduction satisfies axiom (A4) and hence successfully introduced the concept of interreduction to prefix Gröbner bases. Interreduction and critical-pair criteria are closely related to notions of redundancy as considered in general theorem proving [BaGa94a].

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 general 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 [ZhBl93]. In [Re95] other ways of weakening strong right reduction for special structures are developed and studied, e.g., for commutative monoids and nilpotent groups. Terminating algorithms for computing Gröbner bases of both, right and two-sided ideals, in commutative monoid rings and nilpotent group rings are provided. 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 $p, g \in \mathbf{K}[\mathcal{M}]$ and a set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$ 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 $\mathcal{M}$.
Variations of this lemma are e.g. the lemmata 3.22 and 3.30.

(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 $F \subseteq \mathbf{K}[\mathcal{M}]$ 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.

Similar to theorem 3.34 w-Gröbner bases of two-sided ideals can be characterized and enumerating procedures can be given.

This approach has been successfully applied to special groups. The class of finitely presented groups contains subclasses which – using appropriate presentations – allow to solve the

subgroup problem using string-rewriting techniques. In [MaRe97b] we have pointed out how these results are related to the existence (and in fact even the construction) of Gröbner bases in the respective group rings. This shall now be summarized in the following table, which lists 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 (for more information on the reductions and the computation of Gröbner bases related to them see [MaRe93b, Re95, MaRe96a, MaRe97a, Re96]).

Group	*left ideals*	*right ideals*	*two-sided ideals*
free	$\longrightarrow^{\mathrm{su}}$	$\longrightarrow^{\mathrm{p}}$	none[14]
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. Free groups need free presentations with length-lexicographical completion ordering for prefix and suffix reduction. Plain groups require canonical 2-monadic presentations with inverses of length 1 and again length-lexicographical completion ordering for prefix as well as suffix reduction. Context-free groups demand virtually free presentations (see [CrOt94]) for prefix and a modified version of these presentations for suffix reduction. All these special forms of the presentations are similarly required when solving the subgroup problem using prefix-rewriting techniques. For nilpotent groups we need convergent so called PCNI-presentations for quasi-commutative and left-polycyclic reduction. In the case of polycyclic groups we need PCP-presentations for left-polycyclic and reversed PCP-presentations for right-polycyclic reduction.

Alternatives to restricting reduction by incorporating more and more structural knowledge in order to get finite bases were developed in the field of term rewriting. One problem related to the Knuth-Bendix procedure is that it diverges for many cases and it is in general undecidable if it will diverge on a given input. Resulting from this many people have studied what patterns of rules might cause such a divergence. Several methods to solve divergence problems have been offered in order to detect infinite sets of rules which share certain structural regularities e.g. by using constraints, recurrence schemes or auxiliary operators and/or sorts. In the context of string rewriting convergent regular presentations for monoids and groups are considered and inductive inference methods have been proposed to detect the patterns. Another possibility is to follow the approach given by Deiß in [De92] of

[14] By theorem 2.2 the existence of such finite bases would solve the subgroup problem for groups presented by convergent semi-Thue systems.

defining conditional semi-Thue systems and to develop a concept of "conditional polynomial rewriting". Nevertheless, Sattler-Klein in [Sa96] has shown that such approaches are limited. This is due to her result that any recursively enumerable subset of $\mathbf{N}^n$, where $n \in \mathbf{N}^+$, can be encoded into a canonical system generated by completion.

As mentioned in the introduction, when one is solely interested in solving the membership problem a Gröbner basis with its confluence property is not necessary. Alternatives known from term rewriting are unfailing completion or confluence on special equivalence classes only. Our definitions of reduction in monoid rings so far always guarantee overall confluence since the translation lemma holds. In order to approach other group rings or to develop other techniques, "weaker" forms of reduction should be considered, especially for those cases where the subgroup problem for the group is solvable by partial confluence but not by confluence.

Furthermore, in [Re95] we have shown how the theory of Gröbner bases in monoid and group rings over fields can be lifted to monoid and group rings over reduction rings fulfilling the axioms given in the introduction and some computability conditions, e.g., allowing to compute finite Gröbner bases for ideals in the coefficient domain. Hence the results of this paper also hold for monoid and group rings over reduction rings, e.g., the case of the integers $\mathbf{Z}$ is studied in [MaRe93a].

References

[Ap88] J.Apel, *Gröbnerbasen in nichtkommutativen Algebren und ihre Anwendung* PhD Thesis. Leipzig. 1988.

[ApLa88] J. Apel and W. Lassner. *An Extension of Buchberger's Algorithm and Calculations in Enveloping Fields of Lie Algebras.* Journal of Symbolic Computation(1988) 6. pp 361-370.

[Ap95] J. Apel. *A Gröbner Approach to Involutive Bases.* Journal of Symbolic Computation(1995) Vol. 19 No. 5. pp 441-457.

[AvMa84] J. Avenhaus and K. Madlener. *The Nielsen Reduction and P-Complete Problems in Free Groups.* Theoretical Computer Science 32(1984). pp 61-76.

[AvMaOt86] J. Avenhaus, K. Madlener, F. Otto. *Groups Presented by Finite Two-Monadic Church-Rosser Thue Systems.* Transactions of the American Mathematical Society. Vol. 297(1986). pp 427-443.

[BaGa94a] L. Bachmair and H. Ganzinger. *Rewrite-Based Equational Theorem Proving With Selection Simplification.* Journal of Symbolic Computation(1994) Vol. 4 No. 3. pp 1-31.

[BaGa94b] L. Bachmair and H. Ganzinger. *Buchberger's algorithm: A constraint-based completion procedure.* Proc. CCL'94. pp 285-301.

[Ba81] G. Bauer. *Zur Darstellung von Monoiden durch konfluente Reduktionssysteme.* PhD Thesis. Universität Kaiserslautern. 1981.

[BaCaMi81] G. Baumslag, F. Cannonito and C. Miller III. *Computable Algebra and Group Embeddings.* Journal of Algebra 69(1981). pp 186-212.

[BeWe92] T. Becker and V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra.* Springer Verlag(1992).

[Bu65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal.* PhD Thesis. Universität Innsbruck. 1965.

[Bu83] B. Buchberger. *A Critical-Pair Completion Algorithm for Finitely Generated Ideals in Rings.* Proc. Logic and Machines: Decision Problems and Complexity. Springer LNCS 171. pp 137-161.

[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.

[Bu87] B. Buchberger. *Applications of Gröbner Bases in Non-Linear Computational Geometry.* In: R. Janßen (ed.). Trends in Computer Algebra. Springer LNCS 296(1987). pp 52-80.

[Bu91] R. Bündgen. *Simulating Buchberger's Algorithm by a Knuth-Bendix Completion Procedure.* Proc. RTA'91. pp 386-397.

[BoOt93] R. Book and F. Otto. *String-Rewriting Systems.* Springer Verlag(1993).

[CoLiOS92] D. Cox, J. Little and D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer Verlag(1992).

[CrOt94] R. Cremanns and F. Otto. *Constructing Canonical Presentations for Subgroups of Context-Free Groups in Polynomial Time.* Proc. ISSAC'94.

[De12] M. Dehn. *Über unendliche diskontinuierliche Gruppen.* Mathematische Annalen 71(1912). pp 116-144.

[De92] T. Deiß. *Conditional Semi-Thue Systems for Presenting Monoids.* Proc. STACS'92. pp 557-565.

[FaFeGr93] D. Farkas, C. Feustel, E. Green. *Synergy in the theories of Gröbner bases and path algebras.* Canadian Journal of Mathematics. Vol. 45 Nr. 4(1993). pp 727-739.

[Ga88] A. Galligo. *Some algorithmic questions on ideals of differential operators.* Proc. EUROCAL '85 II. LNCS **204** (1985). pp 413-421.

[GeCzLa92] K. O. Geddes, S. R. Czapor and G. Labahn. *Algorithms for Computer Algebra.* Kluwer Academic Publishers. Massachusettes(1992).

[Gi79] R. Gilman. *Presentations of Groups and Monoids.* Journal of Algebra 57(1979). pp 544-554.

[Hi64] H. Hironaka. *Resolution of singularities of an Algebraic Variety over a Field of Characteristic Zero.* Annals of Mathematics 79(1964). pp 109-326.

[Hu80] G. Huet. *Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems.* Journal of the ACM 27(4)(1980). pp 797-821.

[Hu81] G. Huet. *A Complete Proof of Correctness of the Knuth-Bendix Completion Algorithm.* Journal of Computer and System Science 23(1)(1981). pp 11-21.

[Ja81] M. Jantzen. *On a Special Monoid with Single Defining Relation.* Theoretical Computer Science 16(1981). pp 61-73.

[Ja85] M. Jantzen. *A Note on a Special One-rule Semi-Thue System.* Information Processing Letters 21(1985). pp 135-140.

[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.

[KaKaWi89] A. Kandri-Rody, D. Kapur and F. Winkler. *Knuth-Bendix Procedure and Buchberger Algorithm – a Synthesis.* Proc. ISSAC'89. pp 55-67.

[KaMe79] M. I. Kargapolov and Ju. I. Merzljakov. *Fundamentals of the Theory of Groups.* Springer Verlag(1979).

[KaMa86] D. Kapur and K. Madlener. Private communication.

[KaNa85a] D. Kapur and P. Narendran. *Constructing a Gröbner Basis for a Polynomial Ring.* Proc. Combinatorial Algorithms in Algebraic Structures. Otzenhausen(1985). Eds J. Avenhaus, K. Madlener. Universität Kaiserslautern.

[KaNa85b] D. Kapur and P. Narendran. *A Finite Thue System with Decidable Word Problem and Without Equivalent Finite Canonical System.* Theoretical Computer Science 35(1985). pp 337-344.

[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.

[Ke97] B. J. Keller. *Alternatives in Implementing Noncommutative Gröbner Basis Systems.* See this volume.

[KnBe70] D. Knuth and P. Bendix. *Simple Word Problems in Universal Algebras.* J. Leech (editor). Computaional Problems in Abstract Algebra. Pergamon Press. Oxford. 1970. pp 263-297

[Kr93] H. Kredel. *Solvable Polynomial Rings.* Verlag Shaker. Aachen. 1993.

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

[KuMaOt94] N. Kuhn, K. Madlener and F. Otto. *Computing Presentations for Subgroups of Polycyclic Groups and of Context-Free Groups.* Applicable Algebra in Engineering, Communication and Computing 5(1994). pp 287-316.

[La85] W. Lassner. *Symbol Representations of Noncommutative Algebras.* Proc. EUROCAL'85. Springer LNCS 204. pp 99-115.

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

[LeCh86] P. Le Chenadec. *Canoniacl Forms in Finitely Presented Algebras.* Pitman/Wiley. London. 1986.

[LySch77] R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory.* Springer Verlag(1977).

[Ma86] K. Madlener. *Existence and Construction of Gröbner Bases for Ideals in Reduction Rings.* Working paper. 1986.

[MNOZ93] K. Madlener, P. Narendran, F. Otto and L. Zhang. *On Weakly Confluent Monadic String-Rewriting Systems.* Theoretical Computer Science 113(1993). pp 119-165.

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

[MaOt94] K. Madlener and F. Otto. *Some Undecidability Results for Finitely Generated Thue Congruences on a Two-Letter Alphabet.* E. Schock (ed.). Beiträge zur Angewandten Analysis und Informatik, Helmut Brakhage zu Ehren. Verlag Shaker. Aachen. 1994. pp 248-261.

[MaRe93a] K. Madlener and B. Reinert. *On Gröbner Bases in Monoid and Group Rings.* SEKI Report SR-93-08. Universität Kaiserslautern.

[MaRe93b] K. Madlener and B. Reinert. *Computing Gröbner Bases in Monoid and Group Rings.* Proc. ISSAC'93. pp 254-263.

[MaRe95] K. Madlener and B. Reinert. *On Gröbner Bases for Two-Sided Ideals in Nilpotent Group Rings.* SEKI Report SR-95-01. Universität Kaiserslautern.

[MaRe96a] K. Madlener and B. Reinert. *A Generalization of Gröbner Bases Algorithms to Nilpotent Group Rings.* Applicable Algebra in Engineering, Communication and Computing Vol. 8 No. 2(1997). pp 103-123.

[MaRe97a] K. Madlener and B. Reinert. *A Generalization of Gröbner Basis Algorithms to Polycyclic Group Rings.* Journal of Symbolic Computation. To appear.

[MaRe97b] K. Madlener and B. Reinert. *Congruemces in Monoids and Ideals in Monoid Rings.* Technical Report. Universität Kaiserslautern. 1997.

[MaKaSo76] W. Magnus, A. Karrass and D. Solitar. *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations.* Dover Publications. New York. 1976.

[Mar93] C. Marché. *Normalized Rewriting – Application to Ground Completion and Standard Bases.* In: H. Comon, J.-P. Jouannaud (Eds.). Term Rewriting. Springer. 1993. pp 154-169.

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

[Mo88] T. Mora. *Gröbner bases for non-commutative algebras.* Proc. ISSAC'88. LNCS 358(1989). pp 150-161.

[Mo94] T. Mora. *An Introduction to Commutative and Non-Commutative Gröbner Bases.* Theoretical Computer Science 134(1994). pp 131-173.

[Ni21] J. Nielsen. *Om Regning med ikke kommutative Faktoren og dens Anvendelse i Gruppeteorien.* Mat. Tidsskr. B.(1921). pp 77-94.

[OD83] C. Ó'Dúnlaing. *Undecidable Questions Related to Church-Rosser Thue Systems.* Theoretical Computer Science 23(1983). pp 339-345.

[Ot87] F. Otto. *On Deciding the Confluence of a Finite String-Rewriting System on a Given Congruence Class.* Journal of Computer and System Science 35(1987). pp 285-310.

[OtZh91] F. Otto and L. Zhang. *Decision Problems for Finite Special String-Rewiting Systems that are Confluent on some Congruence Class.* Acta Informatica 28(1991). pp 477-510.

[Pa85] L. Pan. *On the Gröbner Bases of Ideals in Polynomial Rings over a Prinicipal Ideal Domain.* University of California. Santa Barbara. Department of Mathematics. Internal Manuscript. 1985.

[Pe97] M. Pesch. *Two-sided Gröbner Bases in Iterated Ore Extensions.* See this volume.

[Re95] B. Reinert. *Gröbner Bases in Monoid and Group Rings.* PhD Thesis. Universität Kaiserslautern. 1995.

[Re96] B. Reinert. *Introducing Reduction to Polycyclic Group Rings - A Comparison of Methods.* Reports on Computer Algebra No 9. Centre of Computer Algebra. Universität Kaiserslautern. 1996.

[Ro93] A. Rosenmann. *An Algorithm for Constructing Gröbner and Free Schreier Bases in Free Group Algebras.* Journal of Symbolic Computation 16(1993). pp 523-549.

[Sa91] A. Sattler-Klein. *Divergence Phenomena During Completion.* Proc. RTA'91. pp 374-385.

[Sa96] A. Sattler-Klein. *A Systematic Study of Infinite Canonial Systems generated by Knuthe-Bendix Completion and Related Problems.* PhD Thesis. Universität Kaiserslautern. 1996.

[Si87] C. Sims. *Verifying Nilpotence.* Journal of Symbolic Computation 3(1987). pp 231-247.

[Si90] C. Sims. *Implementing the Baumslag-Cannonito-Miller Polycyclic Quotient Algorithm.* Journal of Symbolic Computation 9(1990). pp 707-723.

[Si94] C. Sims. *Computation with finitely presented groups.* Cambridge University Press 1994.

[Sq87] C. Squier. *Word Problems and a Homological Finiteness Condition for Monoids.* Journal of Pure Applied Algebra 49(1987). pp 201-217.

[St85] S. Stifter. *Computation of Gröbner Bases over the Integers and in General Reduction Rings.* Diplomarbeit. Johannes Kepler Universität Linz. 1985.

[St87] S. Stifter. *A generalization of Reduction Rings.* Journal of Symbolic Computation 4(1987). pp 351-364.

[St90] T. Stokes. *Gröbner Bases in Exterior Algebras.* Journal of Automated Reasoning 6(1990). pp 233-250.

[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.

[Wi88] D. Wißmann. *Applying Rewriting Techniques to Groups with Power-Commutation-Presentations.* Proc. ISSAC'88. pp 378-389.

[Wi89] D. Wißmann. *Anwendung von Rewriting-Techniken in polyzyklischen Gruppen.* PhD Thesis. Universität Kaiserslautern. 1989.

[ZhBl93] A. Zharkov and Yu. Blinkov. *Involution Approach to Solving Systems of Algebraic Equations.* Proc. IMACS'93. pp 11-16.

6 Appendix

This section contains the proofs of the lemmata and theorems given in the paper.

Proof of Theorem 2.1:
$1 \Longrightarrow 2:$ Using induction on k we show that $u \overset{k}{\longleftrightarrow}_T v$ implies $u - v \in \mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T)$. In the base case $k = 0$ there is nothing to show, since $u - u = 0 \in \mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T)$. Thus let us assume that $\tilde{u} \overset{k}{\longleftrightarrow}_T \tilde{v}$ implies $\tilde{u} - \tilde{v} \in \mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T)$. Then looking at $u \overset{k}{\longleftrightarrow}_T u_k \longleftrightarrow_T v$ we find $u_k \longleftrightarrow_T v$ with $(l_j, r_j) \in T$. Without loss of generality we can assume $u_k \equiv x l_j y$ for some $x, y \in \Sigma^*$ thus giving us $v \equiv x r_j y$, and since multiplication in the free monoid is concatenation, v can be expressed in terms of polynomials by $v = u_k - x * (l_j - r_j) * y$. As $u - v = u - u_k + x * (l_j - r_j) * y$ and $u - u_k \in \mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T)$ our induction hypothesis yields $u - v \in \mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T)$.

$2 \Longrightarrow 1:$ It remains to show that $u - v \in \mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T)$ implies $u \overset{*}{\longleftrightarrow}_T v$. We know $u - v = \sum_{j=1}^{n} \beta_j \cdot x_j * (l_{i_j} - r_{i_j}) * y_j$, where $\beta_j \in \mathbf{K}^*, x_j, y_j \in \Sigma^*$. Therefore, by showing the following stronger result we are done: A representation $u - v = \sum_{j=1}^{m} p_j$ where $p_j = \alpha_j \cdot (w_j - w'_j)$, $\alpha_j \in \mathbf{K}^*$ and $w_j \overset{+}{\longleftrightarrow}_T w'_j$ implies that $u \overset{*}{\longleftrightarrow}_T v$. Thus let $u - v = \sum_{j=1}^{m} p_j$ be such a representation. Depending on this representation $\sum_{j=1}^{m} p_j$ and the ordering $\succeq$ on Σ^* we can define $t = \max\{w_j, w'_j \mid j = 1, \ldots m\}$ and K is the number of polynomials p_j containing t as a term. We will show our claim by induction on (m, K), where $(m', K') < (m, K)$ if and only if $m' < m$ or ($m' = m$ and $K' < K$). In case $m = 0$, then $u - v = 0$ implies $u \equiv v$ and hence $u \overset{0}{\longleftrightarrow}_T v$. Now suppose $m > 0$.
In case $K = 1$, let p_k be the polynomial containing t. Since we either have $p_k = \alpha_k \cdot (t - w'_k)$ or $p_k = \alpha_k \cdot (w_k - t)$, where $\alpha_k \in \{1, -1\}$, without loss of generality we can assume $u \equiv t$ and $p_k = t - w'_k$. Using p_k we can decrease m by subtracting p_k from $u - v$ giving us $w'_k - v = \sum_{j=1, j \neq k}^{m} p_j$. Since $u \equiv t \overset{*}{\longleftrightarrow}_T w'_k$ and our induction hypothesis yields $w'_k \overset{*}{\longleftrightarrow}_T v$ we can conclude $u \overset{*}{\longleftrightarrow}_T v$.
In case $K > 1$ there are two polynomials p_k, p_l in the corresponding representation containing the term t and without loss of generality we can assume $p_k = \alpha_k \cdot (t - w'_k)$ and $p_l = \alpha_l \cdot (t - w'_l)$, as the cases where $p_k = \alpha_k \cdot (w'_k - t)$ or $p_l = \alpha_l \cdot (w'_l - t)$ occur can be treated similarly by modifying the respective coefficient. If $w'_k \equiv w'_l$ we can immediately decrease m by substituting the occurrence of $p_k + p_l$ by $(\alpha_k + \alpha_l) \cdot p_l$. Otherwise we can proceed as follows:

$$\begin{aligned} p_k + p_l &= p_k \underbrace{-\alpha_k \cdot \alpha_l^{-1} \cdot p_l + \alpha_k \cdot \alpha_l^{-1} \cdot p_l}_{=0} + p_l \\ &= (\alpha_k \cdot (w'_k - t) - \alpha_k \cdot \alpha_l^{-1} \cdot \alpha_l \cdot (w'_l - t)) + (\alpha_k \cdot \alpha_l^{-1} + 1) \cdot p_l \\ &= \underbrace{(-\alpha_k \cdot w'_k + \alpha_k \cdot w'_l)}_{=p'_k} + (\alpha_k \cdot \alpha_l^{-1} + 1) \cdot p_l \end{aligned}$$

where $p'_k = \alpha_k \cdot (w'_l - w'_k)$, $w'_k \overset{*}{\longleftrightarrow}_T t \overset{*}{\longleftrightarrow}_T w'_l$ and $w'_l \neq w'_k$. Therefore, in case $\alpha_k \cdot \alpha_l^{-1} + 1 = 0$, i.e., $\alpha_k = -\alpha_l$, m is decreased. On the other hand p'_k does not contain t, i.e., K will be decreased in any case.

□

Proof of Theorem 2.2:
$1 \Longrightarrow 2:$ Using induction on k we show that $u \overset{k}{\longleftrightarrow}_{T \cup T_I} v$ implies $u{\downarrow_{T_I}} - v{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$. In the base case $k = 0$ we have $u \equiv v$ and, therefore, $u{\downarrow_{T_I}} - u{\downarrow_{T_I}} = 0 \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$. Hence, let us assume that $\tilde{u} \overset{k}{\longleftrightarrow}_{T \cup T_I} \tilde{v}$ implies $\tilde{u}{\downarrow_{T_I}} - \tilde{v}{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$. Thus, looking at $u \overset{k}{\longleftrightarrow}_{T \cup T_I} u_k \longleftrightarrow_{T \cup T_I} v$ we can distinguish the following cases:

1. $u_k \longleftrightarrow_T v$ with $(l, r) \in T$.
   Without loss of generality we can assume $u_k \equiv xly$ and $v \equiv xry$ for some words $x, y \in \Sigma^*$. Now this gives us

$$u{\downarrow_{T_I}} - v{\downarrow_{T_I}} = u{\downarrow_{T_I}} - \underbrace{u_k{\downarrow_{T_I}} + xly{\downarrow_{T_I}}}_{=0} - xry{\downarrow_{T_I}}$$

   and $xly{\downarrow_{T_I}} - xry{\downarrow_{T_I}} = x * (l - r) * y$, where $*$ denotes multiplication in $\mathbf{K}[\mathcal{F}]$. By our induction hypothesis we know $u{\downarrow_{T_I}} - u_k{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$ and, hence, we get $u{\downarrow_{T_I}} - v{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$.

2. $u_k \longleftrightarrow_{T_I} v$ with $(a\imath(a), \lambda) \in T_I$[15].
   Without loss of generality we can assume $u_k \equiv xa\imath(a)y$ for some $x, y \in \Sigma^*$ and $v \equiv xy$, i.e., $u_k{\downarrow_{T_I}} = v{\downarrow_{T_I}}$ and therefore $u{\downarrow_{T_I}} - v{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$.

$2 \Longrightarrow 1:$ It remains to show that $u{\downarrow_{T_I}} - v{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$ implies $u \overset{*}{\longleftrightarrow}_{T \cup T_I} v$. We know $u{\downarrow_{T_I}} - v{\downarrow_{T_I}} = \sum_{j=1}^{n} \beta_j \cdot x_j * (l_{i_j} - r_{i_j}) * y_j$, where $\beta_j \in \mathbf{K}^*, x_j, y_j \in \mathcal{F}$. Therefore, by showing the following stronger result we are done: A representation $u - v = \sum_{j=1}^{m} p_j$ where $p_j = \alpha_j \cdot (w_j - w_j')$, $\alpha_j \in \mathbf{K}^*$, $u, v, w_j, w_j' \in \mathcal{F}$ and $w_j \overset{+}{\longleftrightarrow}_T w_j'$ implies that $u \overset{*}{\longleftrightarrow}_T v$. Hence, let $u - v = \sum_{j=1}^{m} p_j$ be such a representation. Depending on this representation $\sum_{j=1}^{m} p_j$ and the ordering $\succeq$ on Σ^* we can define $t = \max\{w_j, w_j' \mid j = 1, \ldots m\}$ and K is the number of polynomials p_j containing t as a term. We will show our claim by induction on (m, K), where

$(m', K') < (m, K)$ if and only if $m' < m$ or ($m' = m$ and $K' < K$). In case $m = 0$, then $u - v = 0$ implies $u = v$ and hence $u \overset{0}{\longleftrightarrow}_T v$[16]. Now suppose $m > 0$.
In case $K = 1$, let p_k be the polynomial containing t. Since we either have $p_k = \alpha_k \cdot (t - w_k')$ or $p_k = \alpha_k \cdot (w_k - t)$, where $\alpha_k \in \{1, -1\}$, without loss of generality we can assume $u = t$ and $p_k = t - w_k'$. Using p_k we can decrease m by subtracting p_k from $u - v$ giving us $w_k' - v = \sum_{j=1, j \neq k}^{m} p_j$. Since $u = t \overset{*}{\longleftrightarrow}_T w_k'$ and our induction hypothesis yields $w_k' \overset{*}{\longleftrightarrow}_T v$ we get $u \overset{*}{\longleftrightarrow}_T v$.
In case $K > 1$ there are two polynomials p_k, p_l in the corresponding representation containing the term t and without loss of generality we can assume $p_k = \alpha_k \cdot (t - w_k')$ and $p_l = \alpha_l \cdot (t - w_l')$, as the cases where $p_k = \alpha_k \cdot (w_k' - t)$ or $p_l = \alpha_l \cdot (w_l' - t)$ occur can be treated similarly by modifying the respective coefficient. If $w_k' = w_l'$ we can immediately decrease m by substituting the occurrence of $p_k + p_l$ by $(\alpha_k + \alpha_l) \cdot p_l$. Otherwise we can proceed as follows:

$$p_k + p_l \;=\; p_k \underbrace{- \alpha_k \cdot \alpha_l^{-1} \cdot p_l + \alpha_k \cdot \alpha_l^{-1} \cdot p_l}_{=0} + p_l$$

[15] The case $(\imath(a)a, \lambda) \in T$ is similar.
[16] Remember that $u, v \in \mathcal{F}$, i.e., they are in normal form with respect to T_I.

$$= \underbrace{(-\alpha_k \cdot w'_k + \alpha_k \cdot w'_l)}_{=p'_k} + (\alpha_k \cdot \alpha_l^{-1} + 1) \cdot p_l$$

where $p'_k = \alpha_k \cdot (w'_l - w'_k)$, $w'_k \overset{*}{\longleftrightarrow}_T t \overset{*}{\longleftrightarrow}_T w'_l$ and $w'_l \neq w'_k$. Hence, in case $\alpha_k \cdot \alpha_l^{-1} + 1 = 0$, i.e., $\alpha_k = -\alpha_l$, m is decreased. On the other hand p'_k does not contain t, i.e., K will be decreased in any case.

□

Proof of Theorem 2.4:
Using the technique described by Ó'Dúnlaing in [OD83] Madlener and Otto have shown that the following question is undecidable ([MaOt94]):

Let $\succeq$ be a compatible well-founded partial ordering on $\{s,t\}^*$ such that $s \succ \lambda$ and $t \succ \lambda$ both hold.
Given a finite Thue system T on $\{s,t\}$. Is there a finite and confluent system T' on $\{s,t\}$ that is equivalent to T and based on $\succ$?

To prove our claim we show that the answer for T is "yes" if and only if the set of polynomials P_T associated to T has a finite Gröbner basis in $\mathbf{K}[\{s,t\}^*]$ with respect to $\succ$. If there is an equivalent, finite presentation $(\{s,t\}, T')$ convergent with respect to $\succ$, then the set $P_{T'}$ is a finite Gröbner basis of P_T in $\mathbf{K}[\{s,t\}^*]$. This follows as the Thue reduction $\longleftrightarrow_{T'}$ can be simulated by the symmetric closure of the reduction $\longrightarrow^{\mathrm{m}}_{P_T}$ in $\mathbf{K}[\{s,t\}^*]$ (compare definition 2.3). Thus it remains to show that in case P_T has a finite Gröbner basis in $\mathbf{K}[\{s,t\}^*]$, there exists a finite Gröbner basis G such that for all $g \in G$ we have $g = u - v$, where $u, v \in \{s,t\}^*$, and $u \overset{*}{\longleftrightarrow}_T v$. Then $(\{s,t\}, T)$ has an equivalent, convergent, finite presentation $(\{s,t\}, T')$, namely $T' = \{(u,v) \mid u - v \in G\}$, since the reduction $\longrightarrow^{\mathrm{m}}$

in $\mathbf{K}[\{s,t\}^*]$ can be compared to a transformation step in a Thue system when restricted to polynomials of the form $u - v$. First we show that in case a finite set F has a finite Gröbner basis in $\mathbf{K}[\{s,t\}^*]$ the procedure Gröbner Bases in Free Monoid Rings also computes a finite Gröbner basis of F. Let $\tilde{G}$ be a finite Gröbner basis of P_T with $\mathsf{HT}(\tilde{G}) = \{\mathsf{HT}(g) \mid g \in \tilde{G}\} = \{t_1, \ldots, t_k\}$. Let $H_{t_i} = \{x t_i y \mid x, y \in \Sigma^*\}$, then $\mathsf{HT}(\mathsf{ideal}(P_T)) = \bigcup_{i=1}^{k} H_{t_i}$, since all polynomials in $\mathsf{ideal}^{\mathbf{K}[\{s,t\}^*]}(P_T)$ reduce to zero by $\tilde{G}$. Further our procedure is correct and, therefore, for each t_i there has to be at least one g_i added to G such that $t_i \equiv x\mathsf{HT}(g_i)y$ for some $x, y \in \Sigma^*$, i.e., $\mathsf{HT}(g_i)$ "divides" t_i. Note that as soon as all such g_i are added to G, we have $\mathsf{HT}(\mathsf{ideal}^{\mathbf{K}[\{s,t\}^*]}(G)) \supseteq \bigcup_{i=1}^{k} H_{t_i}$ and all further computed s-polynomials must reduce to zero (we take the notion of s-polynomials as defined by Mora in [Mo94]). Since the procedure is correct, G then is also a Gröbner basis of $\mathsf{ideal}(P_T)$. It remains to show that in case P_T has a finite Gröbner basis, the finite output G of our procedure has the desired property that for all $g \in G$, $g = u - v$ where $u, v \in \{s,t\}^*$, and $u \overset{*}{\longleftrightarrow}_T v$. Since all polynomials in P_T have the desired property let us look at the polynomials added to G: Let us assume all polynomials in G have the desired structure and a new polynomial g is added. In case g is due to s–polynomial computation of two polynomials $u_1 - v_1$,$u_2 - v_2$ we do not lose our structure. The same is true for computing the normal form of a polynomial $u - v$ using a set of polynomials having the same structure. Further $u \overset{*}{\longleftrightarrow}_T v$ is inherited within these operations (compare also the proof of theorem 2.1).

□

In this proof we used a result of Madlener and Otto in [MaOt94] - a strengthening of

Ó'Dúnlaing's result in [OD83] to alphabets Σ_2 containing 2 letters. Let $\mathcal{P}$ be a property of semi-Thue systems over Σ_2 satisfying the following three conditions:

(P1) Whenever T_1 and T_2 are two finite semi-Thue systems on the same alphabet Σ_2 such that T_1 and T_2 are equivalent, then T_1 has property $\mathcal{P}$ if and only if T_2 has it.

(P2) Each semi-Thue system $T_{\Sigma_2} = \{a \longrightarrow \lambda \mid a \in \Sigma_2\}$ has property $\mathcal{P}$.

(P3) If a finite semi-Thue system T on Σ_2 has property $\mathcal{P}$, then T has decidable word problem, i.e., the Thue congruence $\overset{*}{\longleftrightarrow}_T$ is decidable.

Then the following problem for $\mathcal{P}$ is undecidable in general:

Given: A finite semi-Thue system T on Σ_2.
Question: Does the Thue congruence $\overset{*}{\longleftrightarrow}_T$ have $\mathcal{P}$?

This result is used in the following proof.

Proof of Corollary 2.5:
This follows using the correspondence between Thue systems and ideal bases shown in theorem 2.4. Let us define a property $\mathcal{P}(T)$ for semi-Thue systems T on $\Sigma_2 = \{s, t\}$ as follows: $\mathcal{P}(T)$ if and only if there exists a total, well-founded, admissible ordering $\succeq$ on Σ_2^* such that there exists an equivalent finite semi-Thue system T' which is convergent with respect to $\succ$. Then $\mathcal{P}$ fulfills the conditions (P1), (P2) and (P3) mentioned above:

(P1): If $\mathcal{P}(T_1)$ holds so must $\mathcal{P}(T_2)$ as the existence of a total, well-founded, admissible ordering $\succeq$ on Σ_2^* such that there exists an equivalent finite semi-Thue system T' which is convergent with respect to $\succ$ for T_1 at once carries over to the equivalent system T_2.

(P2): The trivial system $\{s \longrightarrow \lambda, t \longrightarrow \lambda\}$ has property $\mathcal{P}$.

(P3): Having property $\mathcal{P}$ implies decidability of the Thue congruence.

Hence this property is undecidable in general and this result carries over to Gröbner bases in $\mathbf{K}[\{s, t\}^*]$ as before.

□

Proof of Theorem 2.7:
$1 \Longrightarrow 2:$ Let $w = u_1 \circ \ldots \circ u_k \in \langle S \rangle$, i.e., $u_1, \ldots, u_k \in S \cup \{\mathsf{inv}(s) | s \in S\}$. We show $w - 1 \in \mathsf{ideal}_r(P_S)$ by induction on k. In the base case $k = 0$ there is nothing to show, as $w = \lambda \in \langle S \rangle$ and $0 \in \mathsf{ideal}_r(P_S)$. Hence, suppose $w = u_1 \circ \ldots \circ u_{k+1}$ and $u_1 \circ \ldots \circ u_k - 1 \in \mathsf{ideal}_r(P_S)$. Then $(u_1 \circ \ldots \circ u_k - 1) * u_{k+1} \in \mathsf{ideal}_r(P_S)$ and, since $u_{k+1} - 1 \in \mathsf{ideal}_r(P_S)$[17], we get $(u_1 \circ \ldots \circ u_k - 1) * u_{k+1} + (u_{k+1} - 1) = w - 1 \in \mathsf{ideal}_r(P_S)$.

$2 \Longrightarrow 1:$ We have to show that $w - 1 \in \mathsf{ideal}_r(P_T)$ implies $w \in \langle S \rangle$. We know $w - 1 = \sum_{j=1}^{n} \alpha_j \cdot (u_j - 1) * x_j$, where $\alpha_j \in \mathbf{K}^*$, $u_j \in S \cup \{\mathsf{inv}(s) | s \in S\}$, $x_j \in \mathcal{G}$. Therefore, by showing the following stronger result we are done: A representation $w - 1 = \sum_{j=1}^{m} p_j$ where

[17] We either have $u_{k+1} - 1 \in P_S$ or $\mathsf{inv}(u_{k+1}) \in S$, i.e., $(\mathsf{inv}(u_{k+1}) - 1) * u_{k+1} = u_{k+1} - 1 \in \mathsf{ideal}(P_S)$.

$p_j = \alpha_j \cdot (w_j - w'_j)$, $\alpha_j \in \mathbf{K}^*$,$w_j \neq w'_j$ and $w_j \circ \mathsf{inv}(w'_j) \in \langle S \rangle$ implies $w \in \langle S \rangle$. Now, let $w - 1 = \sum_{j=1}^{m} p_j$ be such a representation and $\succeq$ be an arbitrary total well-founded ordering on $\mathcal{G}$. Depending on this representation and $\succeq$ we define $t = \max\{w_j, w'_j \mid j = 1, \ldots m\}$ and K is the number of polynomials p_j containing t as a term. We will show our claim by induction on (m, K), where $(m', K') < (m, K)$ if and only if $m' < m$ or ($m' = m$ and $K' < K$). In case $m = 0$, $w - 1 = 0$ implies $w = 1$ and hence $w \in \langle S \rangle$. Thus let us assume $m > 0$.
In case $K = 1$, let p_k be the polynomial containing t. As we either have $p_k = \alpha_k \cdot (t - w'_k)$ or $p_k = \alpha_k \cdot (w_k - t)$, where $\alpha_k \in \{1, -1\}$, without loss of generality we can assume $p_k = t - w'_k$. Using p_k we can decrease m by subtracting p_k from $w - 1$ giving us $w'_k - 1 = \sum_{j=1, j\neq k}^{m} p_j$. Since $t \circ \mathsf{inv}(w'_k) \in \langle S \rangle$ and our induction hypothesis yields $w'_k \in \langle S \rangle$, we can conclude $w = t = (t \circ \mathsf{inv}(w'_k)) \circ w'_k \in \langle S \rangle$.
In case $K > 1$ there are two polynomials p_k, p_l in the corresponding representation and without loss of generality we can assume $p_k = \alpha_k \cdot (t - w'_k)$ and $p_l = \alpha_l \cdot (t - w'_l)$. If then $w'_k = w'_l$ we can immediately decrease m by substituting the occurrence of $p_k + p_l$ by $(\alpha_k + \alpha_l) \cdot p_l$. Otherwise we can proceed as follows:

$$\begin{aligned} p_k + p_l &= p_k \underbrace{-\alpha_k \cdot \alpha_l^{-1} \cdot p_l + \alpha_k \cdot \alpha_l^{-1} \cdot p_l}_{=0} + p_l \\ &= \underbrace{(-\alpha_k \cdot w'_k + \alpha_k \cdot w'_l)}_{p'_k} + (\alpha_k \cdot \alpha_l^{-1} + 1) \cdot p_l \end{aligned}$$

where $p'_k = \alpha_k \cdot (w'_l - w'_k)$, $w'_k \neq w'_l$ and $w'_k \circ \mathsf{inv}(w'_l) \in \langle S \rangle$, since $w'_k \circ \mathsf{inv}(t), t \circ \mathsf{inv}(w'_l) \in \langle S \rangle$ and $w'_k \circ \mathsf{inv}(w'_l) = w'_k \circ \mathsf{inv}(t) \circ t \circ \mathsf{inv}(w'_l)$. In case $\alpha_k \cdot \alpha_l^{-1} + 1 = 0$, i.e., $\alpha_k = -\alpha_l$, m is decreased. On the other hand p'_k does not contain t, i.e., if m is not decreased K is.

□

Proof of Lemma 3.5:
1. This follows from the fact that using a polynomial f together with $\alpha \in \mathbf{K}^*$ and $w \in \mathcal{M}$ for reduction we use $\alpha \cdot \mathsf{HM}(f * w) \longrightarrow -\alpha \cdot \mathsf{RED}(f * w)$ as a rule and we know $\mathsf{HM}(f * w) > -\mathsf{RED}(f * w)$.

2. This follows from (1), as the ordering $\geq$ on $\mathbf{K}[\mathcal{M}]$ is well-founded.

3. $p \longrightarrow^{\mathrm{s}}_{q_1} 0$ implies $p = \alpha_1 \cdot q_1 * w_1$ for some $\alpha_1 \in \mathbf{K}^*, w_1 \in \mathcal{M}$, and $q_1 \longrightarrow^{\mathrm{s}}_{q_2} 0$ implies $q_1 = \alpha_2 \cdot q_2 * w_2$ for some $\alpha_2 \in \mathbf{K}^*, w_2 \in \mathcal{M}$. Combining this information we immediately get $p \longrightarrow^{\mathrm{s}}_{q_2} 0$, as $p = \alpha_1 \cdot q_1 * w_1 = \alpha_1 \cdot (\alpha_2 \cdot q_2 * w_2) * w_1 = (\alpha_1 \cdot \alpha_2) \cdot q_2 * (w_2 \circ w_1)$ and thus $\mathsf{HT}(q_2 * (w_2 \circ w_1)) = \mathsf{HT}(p)$.

4. This follows immediately from definition 3.2.

□

Proof of Lemma 3.7:
1. Let $p - q \longrightarrow^{\mathrm{s}}_F h = p - q - \alpha \cdot f * w$ with $\alpha \in \mathbf{K}^*$, $f \in F, w \in \mathcal{M}$ and let $\mathsf{HT}(f * w) = t$, i.e., $\alpha \cdot \mathsf{HC}(f * w)$ is the coefficient of t in $p - q$. We have to distinguish three cases:

(a) $t \in \mathsf{T}(p)$ and $t \in \mathsf{T}(q)$:
Then we can eliminate the term t in the polynomials p respectively q by reduction and get $p \longrightarrow^{\mathrm{s}}_f p - \alpha_1 \cdot f * w = p'$, $q \longrightarrow^{\mathrm{s}}_f q - \alpha_2 \cdot f * w = q'$, with $\alpha_1 - \alpha_2 = \alpha$, where $\alpha_1 \cdot \mathsf{HC}(f * w)$ and $\alpha_2 \cdot \mathsf{HC}(f * w)$ are the coefficients of t in p respectively q.

(b) $t \in \mathsf{T}(p)$ and $t \notin \mathsf{T}(q)$:
Then we can eliminate the term t in the polynomial p by reduction and get $p \longrightarrow^{\mathrm{s}}_{f} p - \alpha \cdot f * w = p'$ and $q = q'$.

(c) $t \in \mathsf{T}(q)$ and $t \notin \mathsf{T}(p)$:
Then we can eliminate the term t in the polynomial q by reduction and get $q \longrightarrow^{\mathrm{s}}_{f} q + \alpha \cdot f * w = q'$ and $p = p'$.

In all three cases we have $p' - q' = p - q - \alpha \cdot f * w = h$.

2. We show our claim by induction on k, where $p - q \xrightarrow{k}{}^{\mathrm{s}}_{F} 0$. In the base case $k = 0$ there is nothing to show. Hence, let $p - q \longrightarrow^{\mathrm{s}}_{F} h \xrightarrow{k}{}^{\mathrm{s}}_{F} 0$. Then by (1) there are polynomials $p', q' \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}{}^{\mathrm{s}}_{F} p', q \xrightarrow{*}{}^{\mathrm{s}}_{F} q'$ and $h = p' - q'$. Now the induction hypothesis for $p' - q' \xrightarrow{k}{}^{\mathrm{s}}_{F} 0$ yields the existence of a polynomial $g \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}{}^{\mathrm{s}}_{F} p' \xrightarrow{*}{}^{\mathrm{s}}_{F} g$ and $q \xrightarrow{*}{}^{\mathrm{s}}_{F} q' \xrightarrow{*}{}^{\mathrm{s}}_{F} g$.

3. Using induction on k we show that $p \xleftrightarrow{k}{}^{\mathrm{s}}_{F} q$ implies $p - q \in \mathsf{ideal}_r(F)$. In the base case $k = 0$ there is nothing to show, since $p - p = 0 \in \mathsf{ideal}_r(F)$. Thus let us assume that $\tilde{p} \xleftrightarrow{k}{}^{\mathrm{s}}_{F} \tilde{q}$ implies $\tilde{p} - \tilde{q} \in \mathsf{ideal}_r(F)$. Then looking at $p \xleftrightarrow{k}{}^{\mathrm{s}}_{F} p_k \longleftrightarrow^{\mathrm{s}}_{F} q$ we can distinguish two cases:

(a) $p_k \longrightarrow^{\mathrm{s}}_{f} q$ using a polynomial $f \in F$.
This gives us $q = p_k - \alpha \cdot f * w$, where $\alpha \in \mathbf{K}^*$, $w \in \mathcal{M}$, and since $p - q = p - p_k + \alpha \cdot f * w$ and $p - p_k \in \mathsf{ideal}_r(F)$, we get $p - q \in \mathsf{ideal}_r(F)$.

(b) $q \longrightarrow^{\mathrm{s}}_{f} p_k$ using a polynomial $f \in F$ can be treated similarly.

It remains to show that $p - q \in \mathsf{ideal}_r(F)$ implies $p \xleftrightarrow{*}{}^{\mathrm{s}}_{F} q$. Remember that $p - q \in \mathsf{ideal}_r(F)$ gives us a representation $p = q + \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ such that $\alpha_j \in \mathbf{K}^*$, $f_j \in F$, and $w_j \in \mathcal{M}$. We will show $p \xleftrightarrow{*}{}^{\mathrm{s}}_{F} q$ by induction on m. In the base case $m = 0$ there is nothing to show. Hence, let $p = q + \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j + \alpha_{m+1} \cdot f_{m+1} * w_{m+1}$ and by our induction hypothesis $p \xleftrightarrow{*}{}^{\mathrm{s}}_{F} q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1}$. Further, let $t = \mathsf{HT}(f_{m+1} * w_{m+1})$. In case $t \notin \mathsf{T}(q)$ we get $q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1} \longrightarrow^{\mathrm{s}}_{f_{m+1}} q$ and are done. In case $t \notin \mathsf{T}(p)$ we get $p - \alpha_{m+1} \cdot f_{m+1} * w_{m+1} \longrightarrow^{\mathrm{s}}_{f_{m+1}} p$. Thus, as $p - \alpha_{m+1} \cdot f_{m+1} * w_{m+1} = q + \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ the induction hypothesis yields $p - \alpha_{m+1} \cdot f_{m+1} * w_{m+1} \xleftrightarrow{*}{}^{\mathrm{s}}_{F} q$ and hence we are done. Otherwise let $\beta_1 \neq 0$ be the coefficient of t in $q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1}$ and $\beta_2 \neq 0$ the coefficient of t in q. This gives us a reduction step

$$
\begin{aligned}
&q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1} \longrightarrow^{\mathrm{s}}_{f_{m+1}} \\
&q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1} - \beta_1 \cdot \mathsf{HC}(f_{m+1} * w_{m+1})^{-1} \cdot f_{m+1} * w_{m+1} = \\
&q - (\beta_1 \cdot \mathsf{HC}(f_{m+1} * w_{m+1})^{-1} - a_{m+1}) \cdot f_{m+1} * w_{m+1}
\end{aligned}
$$

eliminating the occurrence of the term t in $q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1}$. Then obviously $\beta_2 = (\beta_1 \cdot \mathsf{HC}(f_{m+1} * w_{m+1})^{-1} - \alpha_{m+1}) \cdot \mathsf{HC}(f_{m+1} * w_{m+1})$ and, therefore, $q \longrightarrow^{\mathrm{s}}_{f_{m+1}} q - (\beta_1 \cdot \mathsf{HC}(f_{m+1} * w_{m+1})^{-1} - \alpha_{m+1}) \cdot f_{m+1} * w_{m+1}$, i.e., q and $q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1}$ are joinable.

□

Proof of Theorem 3.13:
$1 \Longrightarrow 2:$ Let $(w_k, w_l) \in U_{f_k, f_l}$ give us a strong s-polynomial belonging to the polynomials

f_k, f_l. Then by definition 3.11 we get

$$\mathsf{spol}_s(f_k, f_l, w_k, w_l) = \mathsf{HC}(f_k * w_k)^{-1} \cdot f_k * w_k - \mathsf{HC}(f_l * w_l)^{-1} \cdot f_l * w_l \in \mathsf{ideal}_r(F)$$

and, thus, $\mathsf{spol}_s(f_k, f_l, w_k, w_l) \xrightarrow{*}{}^{\mathrm{s}}_F 0$.

$2 \Longrightarrow 1:$ We have to show that every non-zero polynomial $g \in \mathsf{ideal}_r(F)\backslash\{0\}$ is $\longrightarrow^{\mathrm{s}}_F$-reducible to zero. Remember that for $h \in \mathsf{ideal}_r(F)$, $h \longrightarrow^{\mathrm{s}}_F h'$ implies $h' \in \mathsf{ideal}_r(F)$. Hence, as $\longrightarrow^{\mathrm{s}}_F$ is Noetherian, it suffices to show that every $g \in \mathsf{ideal}_r(F)\backslash\{0\}$ is $\longrightarrow^{\mathrm{s}}_F$-reducible. Now, let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be a representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*, f_j \in F$, and $w_j \in \mathcal{M}$. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{M}$ we define $t = \max\{\mathsf{HT}(f_j * w_j) \mid j \in \{1, \ldots m\}\}$ and K is the number of polynomials $f_j * w_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\mathrm{s}}_F$-reducible. We will show that g has a special representation which implies that g is top-reducible using F. This will be done by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[18]. In case $t \succ \mathsf{HT}(g)$ there are two polynomials f_k, f_l in the corresponding representation[19] such that $\mathsf{HT}(f_k * w_k) = \mathsf{HT}(f_l * w_l)$. By definition 3.11 we have a strong s-polynomial $\mathsf{spol}_s(f_k, f_l, w_k, w_l) = \mathsf{HC}(f_k * w_k)^{-1} \cdot f_k * w_k - \mathsf{HC}(f_l * w_l)^{-1} \cdot f_l * w_l$ corresponding to this overlap. We will now change our representation of g by using the additional information on this s-polynomial in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume $\mathsf{spol}_s(f_k, f_l, w_k, w_l) \neq 0$[20]. Hence, the reduction sequence $\mathsf{spol}_s(f_k, f_l, w_k, w_l) \xrightarrow{*}{}^{\mathrm{s}}_F 0$ results in a standard representation $\mathsf{spol}_s(f_k, f_l, w_k, w_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v_i$, where $\delta_i \in \mathbf{K}^*, h_i \in F$, and $v_i \in \mathcal{M}$ and all terms occurring in the sum are bounded by $\mathsf{HT}(\mathsf{spol}_s(f_k, f_l, w_k, w_l)) \prec t$. This gives us:

$$\begin{aligned}
& \alpha_k \cdot f_k * w_k + \alpha_l \cdot f_l * w_l \\
= \;& \alpha_k \cdot f_k * w_k + \underbrace{\alpha'_l \cdot \beta_k \cdot f_k * w_k - \alpha'_l \cdot \beta_k \cdot f_k * w_k}_{=0} + \alpha'_l \cdot \beta_l \cdot f_l * w_l \\
= \;& (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot f_k * w_k - \beta_l \cdot f_l * w_l)}_{=\mathsf{spol}_s(f_k, f_l, w_k, w_l)} \\
= \;& (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * v_i) \qquad (1)
\end{aligned}$$

where $\beta_k = \mathsf{HC}(f_k * w_k)^{-1}$, $\beta_l = \mathsf{HC}(f_l * w_l)^{-1}$ and $\alpha'_l \cdot \beta_l = \alpha_l$. By substituting (1) in our representation of g either t disappears or in case t remains maximal among the terms occurring in the new representation of g, K is decreased.

□

Proof of Lemma 3.17:
1. Let $p - q \longrightarrow^{\mathrm{p}}_F h = p - q - \alpha \cdot f * w$, where $\alpha \in \mathbf{K}^*, f \in F, w \in \mathcal{M}$ and $\mathsf{HT}(f)w = t$, i.e., $\alpha \cdot \mathsf{HC}(f)$ is the coefficient of t in $p - q$. We have to distinguish three cases:

[18] Note that this ordering is well-founded since $\succ$ is well-founded on $\mathcal{T}$ and $K \in \mathbf{N}$.
[19] Not necessarily $f_l \neq f_k$.
[20] In case $\mathsf{spol}_s(f_k, f_l, w_k, w_l) = 0$, just substitute 0 for the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i$ in the equations below.

(a) $t \in \mathsf{T}(p)$ and $t \in \mathsf{T}(q)$:
Then we can eliminate the term t in the polynomials p respectively q by prefix reduction and get $p \longrightarrow_f^{\mathrm{p}} p - \alpha_1 \cdot f * w = p'$, $q \longrightarrow_f^{\mathrm{p}} q - \alpha_2 \cdot f * w = q'$, with $\alpha_1 - \alpha_2 = \alpha$, where $\alpha_1 \cdot \mathsf{HC}(f)$ and $\alpha_2 \cdot \mathsf{HC}(f)$ are the coefficients of t in p respectively q.

(b) $t \in \mathsf{T}(p)$ and $t \notin \mathsf{T}(q)$:
Then we can eliminate the term t in the polynomial p by prefix reduction and get $p \longrightarrow_f^{\mathrm{p}} p - \alpha \cdot f * w = p'$ and $q = q'$.

(c) $t \in \mathsf{T}(q)$ and $t \notin \mathsf{T}(p)$:
Then we can eliminate the term t in the polynomial q by prefix reduction and get $q \longrightarrow_f^{\mathrm{p}} q + \alpha \cdot f * w = q'$ and $p = p'$.

In all three cases we have $p' - q' = p - q - \alpha \cdot f * w = h$.

2. We show our claim by induction on k, where $p - q \xrightarrow{k}_F^{\mathrm{p}} 0$. In the base case $k = 0$ there is nothing to show. Hence, let $p - q \longrightarrow_F^{\mathrm{p}} h \xrightarrow{k}_F^{\mathrm{p}} 0$. Then by (1) there are polynomials $p', q' \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}_F^{\mathrm{p}} p', q \xrightarrow{*}_F^{\mathrm{p}} q'$ and $h = p' - q'$. Now the induction hypothesis for $p' - q' \xrightarrow{k}_F^{\mathrm{p}} 0$ yields the existence of a polynomial $g \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}_F^{\mathrm{p}} p' \xrightarrow{*}_F^{\mathrm{p}} g$ and $q \xrightarrow{*}_F^{\mathrm{p}} q' \xrightarrow{*}_F^{\mathrm{p}} g$.

□

Proof of Lemma 3.23:
1. Suppose $f \longrightarrow_p^{\mathrm{s}} g$ at a monomial $\alpha \cdot t$, i.e., $g = f - \gamma \cdot p * w$ for some $\gamma \in \mathbf{K}, w \in \mathcal{M}$ and $HT(p * w) = t$. Since $p * w \longrightarrow_S^{\mathrm{p}} 0$ we have $p_1 \in S$ such that $p * w = p_1 * w_1$ for some $w_1 \in \mathcal{M}$ and further $t = HT(p * w) = HT(p_1 * w_1) = HT(p_1)w_1$ which implies $f \longrightarrow_{p_1 \in S}^{\mathrm{p}} g$.

2. Suppose $f \longrightarrow_{p_1 \in S}^{\mathrm{p}} g$, i.e., $g = f - \gamma_1 \cdot p_1 * w_1$ for some $\gamma_1 \in \mathbf{K}, w_1 \in \mathcal{M}$. Since $p_1 \in S$ we have $v \in \mathcal{M}$ such that $p_1 = p * v$. Further $t = HT(p_1)w_1 = HT(p_1 * w_1) = HT(p * v * w_1) = HT(p * (v \circ w_1))$ implies $f \longrightarrow_p^{\mathrm{s}} g$.

□

Proof of Theorem 3.25:
We show that for all $q \in S_p$,$w \in \mathcal{M}$ we have $q * w \longrightarrow_{S_p}^{\mathrm{p}} 0$ in case $q * w \neq 0$. Suppose this is not true. Then we can choose a non-zero counter-example $q * w$, where $\mathsf{HT}(q)w$ is minimal (according to the ordering $\succeq_T$ on Σ^*) and $q * w \not\longrightarrow_{S_p}^{\mathrm{p}} 0$. Thus $\mathsf{HT}(q)w$ must be T-reducible, as otherwise $q * w \longrightarrow_{q \in S_p}^{\mathrm{p}} 0$. Let $\mathsf{HT}(q)w \equiv t_1 t_2 w_1 w_2$ such that $\mathsf{HT}(q) \equiv t_1 t_2, t_2 \neq \lambda, w \equiv w_1 w_2$ and $l \equiv t_2 w_1$ for some $(l, r) \in T$. Furthermore, $w_1 \in \mathcal{M}$ as it is a prefix of $w \in \mathcal{M}$. Since $q \in S_p$ the polynomial q must have been added to the set H at some step and as we use a fair strategy to remove elements from H, q and $C(\mathsf{HT}(q))$ are considered. Thus, we have $w_1 \in C(\mathsf{HT}(q))$ by the definition of this set and we can distinguish two cases. If we have $q * w_1 \in S_p$ then $q * w = (q * w_1) * w_2 \longrightarrow_{S_p}^{\mathrm{p}} 0$, since $w_1 \in \mathcal{M}$ and $\mathsf{HT}(q)w \equiv \mathsf{HT}(q)w_1 w_2 \succ \mathsf{HT}(q * w_1)w_2$, contradicting our assumption. On the other hand, $q * w_1 \notin S_p$ implies $q * w_1 \longrightarrow_{q' \in S_p}^{\mathrm{p}} 0$ and we know $\mathsf{HT}(q)w_1 \succ \mathsf{HT}(q * w_1) \equiv \mathsf{HT}(q')z$ for some $z \in \mathcal{M}$. Further $q * w = (q * w_1) * w_2 = (\alpha \cdot q' * z) * w_2$, and $\mathsf{HT}(q)w \succ \mathsf{HT}(q')zw_2 \succeq \mathsf{HT}(q')(z \circ w_2)$. Therefore, we have $q * w = (\alpha \cdot q' * z) * w_2 = \alpha \cdot q' * (z \circ w_2) \longrightarrow_{S_p}^{\mathrm{p}} 0$, contradicting our assumption.

□

Proof of Lemma 3.26:
Let $p \in \mathbf{K}[\mathcal{M}]$ be the polynomial which is being saturated and $S \in \mathcal{SAT}_p(p)$ finite. Further let S_p be the set generated by the procedure. Since we have a correct enumeration of a prefix saturating set for p, each polynomial $q \in S$ has to be prefix reducible to zero by a polynomial in S_p[21]. Therefore, there exists a finite set $S' \subseteq S_p$ such that for every polynomials $q \in S$ there exists a polynomial $q' \in S'$ such that $q \longrightarrow^{\mathrm{p}}_{q'} 0$. Thus as soon as all polynomials in S' have been enumerated every remaining polynomial in H is prefix reducible to zero in one step using S' and hence the **while** loop terminates, as no more elements are added to the set H.

□

Proof of Theorem 3.31:
$1 \Longrightarrow 2:$ Let $\mathsf{HT}(f_k) \equiv \mathsf{HT}(f_l)w$ for $w \in \mathcal{M}$. Then by definition 3.29 we get

$$\mathsf{spol}_p(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k - \mathsf{HC}(f_l)^{-1} \cdot f_l * w \ \in \mathsf{ideal}_r(F),$$

and hence $\mathsf{spol}_p(f_k, f_l) \xrightarrow{*}{}^{\mathrm{p}}_F 0$.

$2 \Longrightarrow 1:$ We have to show that every non-zero element $g \in \mathsf{ideal}_r(F)$ is $\longrightarrow^{\mathrm{p}}_F$-reducible to zero. Remember that for $h \in \mathsf{ideal}_r(F)$, $h \longrightarrow^{\mathrm{p}}_F h'$ implies $h' \in \mathsf{ideal}_r(F)$. Hence as $\longrightarrow^{\mathrm{p}}_F$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}_r(F)\backslash\{0\}$ is $\longrightarrow^{\mathrm{p}}_F$-reducible. Now, let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be a representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*, f_j \in F, w_j \in \mathcal{M}$. By lemma 3.22 we can assume $\mathsf{HT}(f_i * w_i) \equiv \mathsf{HT}(f_i)w_i$. This will enable a restriction to prefix s-polynomials in order to modify the representation of g. Depending on the above representation of g and a well-founded total ordering $\succeq$ on $\mathcal{M}$ we define $t = \max\{\mathsf{HT}(f_j) \circ w_j \mid j \in \{1, \ldots m\}\}$ and K is the number of polynomials $f_j * w_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\mathrm{p}}_F$-reducible. We will show that g has a special representation which implies that g is top-reducible using F. This will be done by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or $(t' = t$ and $K' < K)$[22]. In case $t \succ \mathsf{HT}(g)$ there are two polynomials f_k, f_l in the corresponding representation[23] such that $\mathsf{HT}(f_k)w_k \equiv \mathsf{HT}(f_l)w_l$. We have either $\mathsf{HT}(f_k)z \equiv \mathsf{HT}(f_l)$ or $\mathsf{HT}(f_k) \equiv \mathsf{HT}(f_l)z$ for some $z \in \mathcal{M}$. Without loss of generality let us assume $\mathsf{HT}(f_k) \equiv \mathsf{HT}(f_l)z$ and hence $w_l \equiv zw_k$. Then definition 3.29 provides us with a prefix s-polynomial $\mathsf{spol}_p(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k - \mathsf{HC}(f_l)^{-1} \cdot f_l * z$. Note that, while in the proof of theorem 3.13 the s-polynomials correspond directly to the overlap $\mathsf{HT}(f_k * w_k) = \mathsf{HT}(f_l * w_l)$, i.e., w_k and w_l are involved in the s-polynomial, now we have an s-polynomial corresponding directly to the two polynomials f_k and f_l. We will see later on that this localization is strong enough because this situation has a prefix of the term t as an upper border and lemma 3.30 can be applied. We will now change our representation of g by using the additional information on the above prefix s-polynomial in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of t are decreased by at least 1. Let us assume $\mathsf{spol}_p(f_k, f_l) \neq 0$[24]. Hence, the reduction sequence $\mathsf{spol}_p(f_k, f_l) \xrightarrow{*}{}^{\mathrm{p}}_F 0$ results in a prefix standard representation of the form $\mathsf{spol}_p(f_k, f_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v_i$, where $\delta_i \in \mathbf{K}^*$, $h_i \in F$, $v_i \in \mathcal{M}$ and all terms occurring in the

[21] Especially there is a polynomial $q' \in S_p$ such that $\mathsf{HT}(q) \equiv \mathsf{HT}(q')z$ for some $z \in \mathcal{M}$.
[22] Note that this ordering is well-founded since $\succ$ is and $K \in \mathbf{N}$.
[23] Not necessarily $f_l \neq f_k$.
[24] In case $\mathsf{spol}_p(f_k, f_l) = 0$, just substitute 0 for $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i$ in the equations below.

sum are bounded by $\mathsf{HT}(\mathsf{spol}_p(f_k, f_l))$. Now as $\mathsf{HT}(\mathsf{spol}_p(f_k, f_l)) \prec \mathsf{HT}(f_k) \preceq t \equiv \mathsf{HT}(f_k)w_k$, by lemma 3.30 we then can conclude that t is a proper bound for all terms occurring in the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i * w_k$. Without loss of generality we can assume that for all polynomials occurring in this representation we have $\mathsf{HT}(h_i * v_i * w_k) \equiv \mathsf{HT}(h_i)(v_i \circ w_k)$ as F is prefix saturated and in case $\mathsf{HT}(h_i * v_i * w_k) \neq \mathsf{HT}(h_i)(v_i \circ w_k)$ we can substitute the polynomial $h_i * v_i * w_k$ by a product $\tilde{\alpha_i} \cdot \tilde{h_i} * u_i$ such that $h_i * v_i * w_k = \tilde{\alpha_i} \cdot \tilde{h_i} * u_i$ and $\mathsf{HT}(h_i * v_i * w_k) \equiv \mathsf{HT}(\tilde{h_i})u_i$ without increasing neither t nor K. This gives us:

$$
\begin{aligned}
& \alpha_k \cdot f_k * w_k + \alpha_l \cdot f_l * w_l \\
= \;& \alpha_k \cdot f_k * w_k + \underbrace{\alpha'_l \cdot \beta_k \cdot f_k * w_k - \alpha'_l \cdot \beta_k \cdot f_k * w_k}_{=0} + \alpha'_l \cdot \beta_l \cdot f_l * w_l \\
= \;& (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot f_k * w_k - \beta_l \cdot f_l * w_l)}_{=\mathsf{spol}_p(f_k, f_l) * w_k} \\
= \;& (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * v_i * w_k) \qquad (2)
\end{aligned}
$$

where $\beta_k = \mathsf{HC}(f_k)^{-1}$, $\beta_l = \mathsf{HC}(f_l)^{-1}$ and $\alpha'_l \cdot \beta_l = \alpha_l$. By substituting (2) in our representation of g either t disappears or in case t remains maximal among the terms occurring in the new representation of g, K is decreased.

□

Proof of Lemma 3.30:
As $\sum_{i=1}^{k} \alpha_i \cdot g_i * w_i$ belongs to the reduction sequence $p \xrightarrow{*}{}^{\mathrm{p}}_{F} 0$, for all $u \in \bigcup_{i=1}^{k} \mathsf{T}(g_i * w_i)$ we have $\mathsf{HT}(p) \succeq u$ implying $tw \succ \mathsf{HT}(p)w \succeq uw \succeq u \circ w$. Note that this proof uses the fact that the ordering $\succ$ on $\mathcal{M}$ is induced by the completion ordering $\succeq_T$ of the presentation (Σ, T) of $\mathcal{M}$, as we need that the ordering is compatible with concatenation, i.e., $uv \succeq_T (uv)\downarrow_T = u \circ v$ for all $u, v \in \mathcal{M}$.

□

Proof of Theorem 3.34:
$1 \Longrightarrow 2:$ Since $g \in \mathsf{ideal}(G) = \mathsf{ideal}_r(G)$ and G is a right Gröbner basis, we are done.

$2 \Longrightarrow 3:$ To show that G is a prefix Gröbner basis we have to prove $\xleftrightarrow{*}{}^{\mathrm{p}}_{G} = \equiv_{\mathsf{ideal}_r(G)}$ and for all $g \in \mathsf{ideal}_r(G)$, $g \xrightarrow{*}{}^{\mathrm{p}}_{G} 0$. The latter follows immediately since $\mathsf{ideal}_r(G) \subseteq \mathsf{ideal}(G)$ and hence for all $g \in \mathsf{ideal}_r(G)$ we have $g \xrightarrow{*}{}^{\mathrm{p}}_{G} 0$. The inclusion $\xleftrightarrow{*}{}^{\mathrm{p}}_{G} \subseteq \equiv_{\mathsf{ideal}_r(G)}$ is obvious. Hence let $f \equiv_{\mathsf{ideal}_r(G)} g$, i.e., $f - g \in \mathsf{ideal}_r(G)$. But then we have $f - g \xrightarrow{*}{}^{\mathrm{p}}_{G} 0$ and hence by lemma 3.17 there exists a polynomial $h \in \mathbf{K}[\mathcal{M}]$ such that $f \xrightarrow{*}{}^{\mathrm{p}}_{G} h$ and $g \xrightarrow{*}{}^{\mathrm{p}}_{G} h$, yielding $f \xleftrightarrow{*}{}^{\mathrm{p}}_{G} g$. Furthermore, $w * f \in \mathsf{ideal}(G)$ and $w * f \xrightarrow{*}{}^{\mathrm{p}}_{G} 0$ implies $w * f \in \mathsf{ideal}_r(G)$.

$3 \Longrightarrow 4:$ This follows immediately.

$4 \Longrightarrow 1:$ Since it is obvious that $\mathsf{ideal}_r(G) \subseteq \mathsf{ideal}(G)$ it remains to show that $\mathsf{ideal}(G) \subseteq \mathsf{ideal}_r(G)$ holds. Let $g \in \mathsf{ideal}(G)$, i.e., $g = \sum_{i=1}^{n} \alpha_i \cdot u_i * g_i * w_i$ for some $\alpha_i \in \mathbf{K}$, $g_i \in G$ and $u_i, w_i \in \mathcal{M}$. We will show by induction on $|u_i|$ that for $u_i \in \mathcal{M}$, $g_i \in G$, $u_i * g_i \in \mathsf{ideal}_r(G)$ holds. Then g also has a representation in terms of right multiples and hence lies in the right ideal generated by G as well. In case $|u_i| = 0$ we are immediately done. Hence let us assume $u_i \equiv ua$ for some $a \in \Sigma$ and by our assumption we know $a * g_i \in \mathsf{ideal}_r(G)$. Let

$a * g_i = \sum_{j=1}^{m} \beta_j \cdot g'_j * v_j$. Then we get $u_i * g_i = ua * g_i = u * (a * g_i) = u * (\sum_{j=1}^{m} \beta_j \cdot g'_j * v_j) = \sum_{j=1}^{m} \beta_j \cdot (u * g'_i) * v_j$ and by our induction hypothesis $u * g'_j \in \mathsf{ideal}_r(G)$ holds for every $1 \leq j \leq m$. Therefore, we can conclude $u_i * g_i \in \mathsf{ideal}_r(G)$.

□

Proof of Lemma 4.3:
We have to show that the polynomials in the set $\{\alpha \cdot p * w \mid \alpha \in \mathbf{K}^*, w \in \mathcal{G}\}$ are prefix reducible to zero in one step by $\textsc{Sat}_p(p)$. In case $p = \alpha \cdot t$, $\alpha \in \mathbf{K}^*$, $t \in \mathcal{G}$, we are done as $\textsc{Sat}_p(p) = \{\alpha\} \in \mathcal{SAT}(p)$. In case the polynomial p contains more than one monomial, we show that for every polynomial $q \in \textsc{Sat}_p(p)$ and every $w \in C(\mathsf{HT}(q)) = \{w \in \Sigma^* \mid tw \equiv t_1 t_2 w \equiv t_1 l, t_2 \neq \lambda \text{ for some } (l, r) \in T\}$ the multiple $q * w$ is prefix reducible to zero in one step using $\textsc{Sat}_p(p)$.

1. For the polynomials $\mathsf{can}(p)$ and $\mathsf{acan}(p)$ we get the corresponding sets $C(\mathsf{HT}(\mathsf{can}(p))) = \{\mathsf{inv}(\ell(\mathsf{HT}(\mathsf{can}(p))))\}$ respectively $C(\mathsf{HT}(\mathsf{acan}(p))) = \{\mathsf{inv}(\ell(\mathsf{HT}(\mathsf{acan}(p))))\}$. It can be shown that $\mathsf{can}(p) * \mathsf{inv}(\ell(\mathsf{HT}(\mathsf{can}(p)))) = \mathsf{acan}(p)$ and $\mathsf{acan}(p) * \mathsf{inv}(\ell(\mathsf{HT}(\mathsf{acan}(p)))) = \mathsf{can}(p)$ and hence the set $\{\mathsf{can}(p), \mathsf{acan}(p)\}$ is prefix saturated. Furthermore, as it is a subset of $\{p * w \mid w \in \mathcal{F}\}$ it is also a prefix saturating set for p.

2. Let $\mathsf{HT}(\mathsf{can}(p)) \equiv ta$ and $\mathsf{HT}(\mathsf{acan}(p)) = t' \circ \mathsf{inv}(a)$ for some $t, t' \in \mathcal{G}$, $a \in \Sigma$. In case $q \in \{\mathsf{can}(p), \mathsf{acan}(p)\}$, the fact that $C(\mathsf{HT}(q)) = C_q \cup \{\mathsf{inv}(\ell(\mathsf{HT}(q)))\}$ and the definition of $\textsc{Sat}_p(p)$ imply that for all $b \in C(\mathsf{HT}(q))$ we have $q * b \longrightarrow^{\mathrm{p}}_{\textsc{Sat}_p(p)} 0$. Now, let us assume that $q = \mathsf{can}(p) * b$ for some $b \in C_{\mathsf{can}(p)}$ and $(ab, c) \in T$, $c \in \Sigma$, $b \neq \mathsf{inv}(a)$. We have to distinguish the following two cases. If $\mathsf{HT}(q) \equiv tc$, then $C(tc) = \{d \mid (cd, e) \in T, d \in \Sigma, e \in \Sigma \cup \{\lambda\}\}$ and in case this set is not empty let us look at such a rule $(cd, e) \in T$. Since our presentation is a reduced convergent group presentation, there exists a rule of the form $\mathsf{inv}(a)c \longrightarrow b \in T$ where $|\mathsf{inv}(a)| = 1$. Now this gives us

$$bd \longleftarrow \underline{\mathsf{inv}(a)cd} \equiv \mathsf{inv}(a)\underline{cd} \longrightarrow \mathsf{inv}(a)e$$

and as $d \neq e$ and $b \neq \mathsf{inv}(a)$, there exists an element $f \in \Sigma \cup \{\lambda\}$ such that $bd \longrightarrow f$, $\mathsf{inv}(a)e \longrightarrow f \in T$. Again this results in the situation

$$e \longleftarrow cd \longleftarrow \underline{ab}d \equiv a\underline{bd} \longrightarrow af$$

and we either have $b \circ d = \lambda$ in case $f = \lambda$ or there exists a rule $af \longrightarrow e \in T$. In case $b \circ d = \lambda$ this implies $q * d = (\mathsf{can}(p) * b) * d = \mathsf{can}(p) * (b \circ d) = \mathsf{can}(p)$ and hence $q * d \longrightarrow^{\mathrm{p}}_{\textsc{Sat}_p(p)} 0$. Otherwise, $q * d = (\mathsf{can}(p) * b) * d = \mathsf{can}(p) * (b \circ d) = \mathsf{can}(p) * f$ implies $q * d \longrightarrow^{\mathrm{p}}_{\textsc{Sat}_p(p)} 0$ as $f \in C_{\mathsf{can}(p)}$ and hence $\mathsf{can}(p) * f \in \textsc{Sat}_p(p)$.

On the other hand, if $\mathsf{HT}(q) \not\equiv tc$ there exists a term $s \in \mathsf{T}(\mathsf{can}(p))$ such that $\mathsf{HT}(q) = s \circ b$ and $s \circ b \succ tc$. We have to distinguish two cases: In case $|s| < |ta|$ we know $s \circ b \equiv sb$, as $|s \circ b| = |tc|$. If $C(sb)$ is not empty let $be \longrightarrow f \in T$ be a corresponding rule. We get

$$ce \longleftarrow \underline{ab}e \equiv a\underline{be} \longrightarrow af.$$

As $c \neq a$ we either get $b \circ e = \lambda$ in case $f = \lambda$ implying that $q * e = (\mathsf{can}(p) * b) * e = \mathsf{can}(p) * (b \circ e) = \mathsf{can}(p)$ and hence $q * e \longrightarrow^{\mathrm{p}}_{\textsc{Sat}_p(p)} 0$, or there exists an element $g \in \Sigma \cup \{\lambda\}$ such that $ce \longrightarrow g, af \longrightarrow g \in T$, giving us $q * e = (\mathsf{can}(p) * b) * e = \mathsf{can}(p) * (b \circ e) = \mathsf{can}(p) * f$ and thus $q * e \longrightarrow^{\mathrm{p}}_{\textsc{Sat}_p(p)} 0$ as $f \in C_{\mathsf{can}(p)}$. On the other hand, if $|s| = |ta|$ with $s \equiv s'd$ and

$db \longrightarrow f \in T$, then $s \prec ta$ and $s \circ b \equiv s'f \succ tc$ implies $s' \equiv t$ and $f \succ c$. Now suppose $C(s'f) \neq \emptyset$ and let $fg \longrightarrow h \in T$ be a corresponding rule. Since $db \longrightarrow f \in T$ we also have $\mathsf{inv}(d)f \longrightarrow b \in T$, resulting in

$$bg \longleftarrow \underline{\mathsf{inv}(d)f}g \equiv \mathsf{inv}(d)\underline{fg} \longrightarrow \mathsf{inv}(d)h.$$

Since $g \neq h$ in case $h = \lambda$ we have $bg \longrightarrow \mathsf{inv}(d) \in T$ giving us $cg \longleftarrow \underline{abg} = a\underline{bg} \longrightarrow a\,\mathsf{inv}(d)$. But then, as $a, c, g, \mathsf{inv}(d)$ all are not equal to λ, there exists $i \in \Sigma \cup \{\lambda\}$ such that $cg \longrightarrow i$, $a\,\mathsf{inv}(d) \longrightarrow i \in T$, and thus $\mathsf{inv}(d) \in C_{\mathsf{can}(p)}$. This implies $q * g = (\mathsf{can}(p) * b) * g = \mathsf{can}(p) * \mathsf{inv}(d) \in \textsc{Sat}_p(p)$. On the other hand, in case $h \neq \lambda$, there exists $i \in \Sigma \cup \{\lambda\}$ such that $bg \longrightarrow i$, $\mathsf{inv}(d)h \longrightarrow i \in T$. Hence, $cg \longleftarrow \underline{abg} \equiv a\underline{bg} \longrightarrow ai$. In case $i = \lambda$, $bg \longrightarrow \lambda \in T$ immediately implies $q * g = (\mathsf{can}(p) * b) * g = \mathsf{can}(p) * (b \circ g) = \mathsf{can}(p)$. Otherwise there exists $j \in \Sigma \cup \{\lambda\}$ such that $cg \longrightarrow j$, $ai \longrightarrow j \in T$, and hence $i \in C_{\mathsf{can}(p)}$, giving us $q * g = (\mathsf{can}(p) * b) * g = \mathsf{can}(p) * (b \circ g) = \mathsf{can}(p) * i \in \textsc{Sat}_p(p)$.
Hence in all these cases we have $q * g \longrightarrow^{\mathrm{p}}_{\textsc{Sat}_p(p)} 0$.
The case $q = \mathsf{acan}(p) * b$ is similar in case $\mathsf{HT}(\mathsf{acan}(p)) \equiv t'\mathsf{inv}(a)$. Hence let us assume $\mathsf{HT}(\mathsf{acan}(p)) = t' \circ \mathsf{inv}(a) \not\equiv t'\mathsf{inv}(a)$. Then $t' \equiv t''k$, $t' \circ \mathsf{inv}(a) = t''l$ and $k\mathsf{inv}(a) \longrightarrow l \in T$. The rule corresponding to $b \in C_{\mathsf{acan}(p)}$ then is $lb \longrightarrow c \in T$. We have to distinguish the following two cases. If $\mathsf{HT}(q) \equiv tc$, then $C(tc) = \{d \mid (cd, e) \in T, d \in \Sigma, e \in \Sigma \cup \{\lambda\}\}$ and in case this set is not empty let us look at such a rule $(cd, e) \in T$. Since our presentation is a reduced convergent group presentation, there exists a rule of the form $\mathsf{inv}(l)c \longrightarrow b \in T$ where $|\mathsf{inv}(l)| = 1$. Now this gives us

$$bd \longleftarrow \underline{\mathsf{inv}(l)c}d \equiv \mathsf{inv}(l)\underline{cd} \longrightarrow \mathsf{inv}(l)e$$

and as $d \neq e$ and $b \neq \mathsf{inv}(l)$, there exists an element $f \in \Sigma \cup \{\lambda\}$ such that $bd \longrightarrow f$, $\mathsf{inv}(l)e \longrightarrow f \in T$. Again this results in the situation

$$cd \longleftarrow \underline{lb}d \equiv l\underline{bd} \longrightarrow lf$$

and we either have $b \circ d = \lambda$ in case $f = \lambda$ or there exists a rule $lf \longrightarrow e \in T$. In case $b \circ d = \lambda$ this implies $q * d = (\mathsf{acan}(p) * b) * d = \mathsf{acan}(p) * (b \circ d) = \mathsf{acan}(p)$ and hence $q * d \longrightarrow^{\mathrm{p}}_{\textsc{Sat}_p(p)} 0$. Otherwise, $q * d = (\mathsf{acan}(p) * b) * d = \mathsf{acan}(p) * (b \circ d) = \mathsf{acan}(p) * f$ implies $q * d \longrightarrow^{\mathrm{p}}_{\textsc{Sat}_p(p)} 0$ as $f \in C_{\mathsf{acan}(p)}$ and hence $\mathsf{acan}(p) * f \in \textsc{Sat}_p(p)$. On the other hand, if $\mathsf{HT}(q) \neq tc$ there exists a term $s \in \mathsf{T}(\mathsf{acan}(p))$ such that $\mathsf{HT}(q) = s \circ b$ and $s \circ b \succ tc$. We have to distinguish two cases: In case $|s| < |tl|$ we know $s \circ b \equiv sb$, as $|s \circ b| = |tc|$. If $C(sb)$ is not empty let $be \longrightarrow f \in T$ be a corresponding rule. We get

$$ce \longleftarrow \underline{lb}e \equiv l\underline{be} \longrightarrow lf.$$

As $c \neq l$ we either get $b \circ e = \lambda$ in case $f = \lambda$ implying that $q * e = (\mathsf{acan}(p) * b) * e = \mathsf{acan}(p) * (b \circ e) = \mathsf{acan}(p)$ and hence $q * e \longrightarrow^{\mathrm{p}}_{\textsc{Sat}_p(p)} 0$, or there exists an element $g \in \Sigma \cup \{\lambda\}$ such that $ce \longrightarrow g$, $lf \longrightarrow g \in T$, giving us $q * e = (\mathsf{acan}(p) * b) * e = \mathsf{acan}(p) * (b \circ e) = \mathsf{acan}(p) * f$ and thus $q * e \longrightarrow^{\mathrm{p}}_{\textsc{Sat}_p(p)} 0$ as $f \in C_{\mathsf{acan}(p)}$. On the other hand, if $|s| = |tl|$ with $s \equiv s'd$ and $db \longrightarrow f \in T$ then $s \prec tl$ and $s \circ b \equiv s'f \succ tc$ implies $s' \equiv t$ and $f \succ c$. Now suppose $C(s'f) \neq \emptyset$ and let $fg \longrightarrow h \in T$ be a corresponding rule. Since $db \longrightarrow f \in T$ we also have $\mathsf{inv}(d)f \longrightarrow b \in T$, resulting in

$$bg \longleftarrow \underline{\mathsf{inv}(d)f}g \equiv \mathsf{inv}(d)\underline{fg} \longrightarrow \mathsf{inv}(d)h.$$

Since $g \neq h$ in case $h = \lambda$ we have $bg \longrightarrow \mathsf{inv}(d) \in T$ giving us $cg \longleftarrow \underline{lbg} = l\underline{bg} \longrightarrow l\,\mathsf{inv}(d)$. But then, as $l, c, g, \mathsf{inv}(d)$ all are not equal to λ, there exists $i \in \Sigma \cup \{\lambda\}$ such that $cg \longrightarrow i$, $l\,\mathsf{inv}(d) \longrightarrow i \in T$, and thus $\mathsf{inv}(d) \in C_{\mathsf{acan}(p)}$. This implies $q * g = (\mathsf{acan}(p) * b) * g = \mathsf{acan}(p) * \mathsf{inv}(d) \in \mathrm{SAT}_p(p)$. On the other hand, in case $h \neq \lambda$, there exists $i \in \Sigma \cup \{\lambda\}$ such that $bg \longrightarrow i$, $\mathsf{inv}(d)h \longrightarrow i \in T$. Hence, $cg \longleftarrow \underline{lbg} \equiv l\underline{bg} \longrightarrow li$. In case $i = \lambda$, $bg \longrightarrow \lambda \in T$ immediately implies $q * g = (\mathsf{acan}(p) * b) * g = \mathsf{acan}(p) * (b \circ g) = \mathsf{acan}(p)$. Otherwise there exists $j \in \Sigma \cup \{\lambda\}$ such that $cg \longrightarrow j$, $li \longrightarrow j \in T$, and hence $i \in C_{\mathsf{acan}(p)}$, giving us $q * g = (\mathsf{acan}(p) * b) * g = \mathsf{acan}(p) * (b \circ g) = \mathsf{acan}(p) * i \in \mathrm{SAT}_p(p)$.
Hence in all these cases we have $q * g \longrightarrow^{\mathrm{p}}_{\mathrm{SAT}_p(p)} 0$.

□

Proof of Theorem 4.4:
Note that if (Σ, T) is a convergent interreduced presentation of a cancellative monoid $\mathcal{M}$, then no rules of the form $wa \longrightarrow a$ or $aw \longrightarrow a$ appear in T for $a \in \Sigma$. This is of course always true if such presentations are given for groups.
Let us assume that procedure **normal form** computes a normal form of a polynomial allowing only prefix reduction steps at the respective head terms. The proof now is done in two steps: first we show that all polynomials computed have a certain property that will be used in the second step to ensure termination. We say a polynomial q has property $\mathcal{P}_F$ if and only if

(α) $|\mathsf{HT}(q)| \leq K$, where $K = \max\{|\mathsf{HT}(f)| \mid f \in F\} + 1$.

(β) If $|\mathsf{HT}(q)| = K$ then there exists an element $a \in \Sigma$ such that

(i) all terms of length K in q have a as a common suffix, and

(ii) for all $s \in \mathsf{T}(q)$ with $|s| = K - 1$ we either have $s \equiv s_1 a$ or in case $s \equiv s_1 d$, $d \in \Sigma \backslash \{a\}$ there is a rule $ea \longrightarrow d \in T, e \in \Sigma$.

We will show that all polynomials q computed by the procedure on input F have property $\mathcal{P}_F$.
By the choice of K all input polynomials have $\mathcal{P}_F$. Hence, let G be the actual set of polynomials having $\mathcal{P}_F$, and let q be the next polynomial computed by our procedure. In case q is due to computing the normal form of a polynomial p having $\mathcal{P}_F$ using prefix reduction at head terms only the property is preserved. To see this we can restrict ourselves to a single step reduction. In case $|\mathsf{HT}(p)| < K$ we are done. Therefore, suppose $|\mathsf{HT}(p)| = K$ and $\mathsf{HM}(p)$ is reduced in the reduction step $p \longrightarrow^{\mathrm{p}}_{g \in G} q'$. We have to show that q' satisfies $\mathcal{P}_F$. Let $\mathsf{HT}(p) \equiv \mathsf{HT}(g)w$ and $q' = p - \alpha \cdot g * w$, $\alpha \in \mathbf{K}^*$, $w \in \mathcal{M}$. Now $g * w$ has $\mathcal{P}_F$ as $\mathsf{HT}(g * w) \equiv \mathsf{HT}(g)w$ and for all $s \in \mathsf{T}(\mathsf{RED}(g))$ we either have $|s \circ w| < |sw|$ or sw and $\mathsf{HT}(g)w$ have the same last letter. Since $\mathsf{T}(q') \subseteq \mathsf{T}(p) \cup \mathsf{T}(g * w)$, q' then likewise has $\mathcal{P}_F$. In case q is due to saturating a polynomial as specified e.g. in procedure PREFIX SATURATION on page 19 and results from a polynomial q' having $\mathcal{P}_F$ being overlapped with a rule $ab \longrightarrow c \in T$, $c \in \Sigma \cup \{\lambda\}$[25], we can also show that $\mathcal{P}_F$ is preserved. Note that only the case $|\mathsf{HT}(q)| = K$ is critical. In case $|\mathsf{HT}(q')| < K$ and $|\mathsf{HT}(q)| = K$ we know $\mathsf{HT}(q) \equiv tb$ and for all $s \in \mathsf{T}(q')$ with $|s \circ b| = K - 1$ either $s \circ b \equiv sb \in \mathrm{IRR}(T)$ or $s \equiv s_1 e$ and $s \circ b = s_1 e \circ b \equiv s_1 d$, where $eb \longrightarrow d \in T$. Note that these are the only

[25]The polynomial q' here is said to overlap with the rule $ab \longrightarrow c \in T$ in case $\ell(\mathsf{HT}(q')) = a$.

possibilities to gain a term of length $K-1$ from a term of length less or equal to $K-1$ by multiplication with a letter b. On the other hand, if $|\mathsf{HT}(q')| = K$ with $\mathsf{HT}(q') \equiv ta$ we can only violate $\mathcal{P}_F$ in case we have $t_1, t_2 \in \mathsf{T}(q')$ such that $|t_1| = K, |t_2| = K-1, t_1 \equiv t_1'a$ and $t_1 \circ b \equiv t_1'c, t_2 \circ b \equiv t_2 b$ with $c \neq \lambda$. Therefore, we examine all $s \in \mathsf{T}(q')$ with $|s| = K-1$. If there are none q must have $\mathcal{P}_F$, since then a

term $s \in \mathsf{T}(q')$ can only reach length $K-1$ by multiplication with b in case $|s| = K-2$ and $sb \in \mathrm{IRR}(T)$. Since $ab \longrightarrow c \in T$ and $\mathcal{G}$ is a group including inverses of length 1 for the generators, a has an inverse $\tilde{a}$ and $b \overset{*}{\longleftrightarrow}_T \tilde{a}\underline{ab} \equiv \tilde{a}\underline{ab} \overset{*}{\longleftrightarrow}_T \tilde{a}c$ gives us the existence of a rule $\tilde{a}c \longrightarrow b \in T$ as T is confluent[26]. Now let $s \in \mathsf{T}(q')$ have length $K-1$. Then if $s \equiv s_1 a$ there is nothing to show[27]. On the other hand, in case $s \equiv s_1 d, d \neq a$ we know that there is a rule $ea \longrightarrow d \in T$ as q' has $\mathcal{P}_F$. Then we have $db \longleftarrow \underline{ea}b \equiv e\underline{ab} \longrightarrow ec$ and, since $ea \longrightarrow d \in T$ gives us $e \neq d$, there are rules $db \longrightarrow g, ec \longrightarrow g \in T, g \in \Sigma \cup \{\lambda\}$. Finally let us assume that q is due to s-polynomial computation. But computing s-polynomials can be compared to a single prefix reduction step on the head monomial of a polynomial and we have seen that prefix reduction preserves property $\mathcal{P}_F$.
It remains to show that the procedure does terminate. Thus let us assume the contrary. Then there are infinitely many polynomials $q_i, i \in \mathbf{N}$ resulting from s-polynomial computations added to G. Note that every such polynomial is in prefix normal from with respect to all polynomials in G so far. On the other hand, as $|\mathsf{HT}(q_i)| \leq K$, this would mean that there is a term t, which occurs infinitely often as a head term among these polynomials q_i contradicting the fact that the head terms of all added polynomials are in prefix normal form with respect to the polynomials added to the Gröbner set so far, and hence no head term can appear twice among the head terms of the polynomials ever added to the set G.
□

Proof of Theorem 4.12:
$1 \Longrightarrow 2$:
Let $\mathsf{HT}(f_k) \equiv \mathsf{HT}(f_l)w$ for $f_k, f_l \in G$ and $w \in \mathcal{G}$. Then by definition 3.29 we get

$$\mathsf{spol}_p(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k - \mathsf{HC}(f_l)^{-1} f_l * w \ \in \mathsf{ideal}_r(G) = \mathsf{ideal}_r(F),$$

and hence $\mathsf{spol}_p(f_k, f_l) \overset{*}{\longrightarrow}^{\mathrm{p}}_G 0$.

$2 \Longrightarrow 1$:
We have to show that every non-zero element $g \in \mathsf{ideal}_r(F)$ is $\longrightarrow^{\mathrm{p}}_G$-reducible to zero. Remember that for $h \in \mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$, $h \longrightarrow^{\mathrm{p}}_G h'$ implies $h' \in \mathsf{ideal}_r(G) = \mathsf{ideal}_r(F)$. Thus as $\longrightarrow^{\mathrm{p}}_G$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}_r(F) \backslash \{0\}$ is $\longrightarrow^{\mathrm{p}}_G$-reducible. Let $g = \sum_{j=1}^m \alpha_j \cdot f_j * w_j$ be a representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*, f_j \in F, w_j \in \mathcal{G}$. Further for all $1 \leq j \leq m$, let $w_j \equiv e_j u_j$, with $e_j \in \mathcal{E}$, $u_j \in \mathcal{F}$. Then, we can modify our representation of g to $g = \sum_{j=1}^m \alpha_j \cdot \psi_{e_j}(f_j) * u_j$. Since G is $\mathcal{F}$-prefix saturated and $\psi_{e_j}(f_j) \in G$ we can assume $g = \sum_{j=1}^m \alpha_j \cdot g_j * v_j$, where $\alpha_j \in \mathbf{K}^*, g_j \in G, v_j \in \mathcal{F}$ and $\mathsf{HT}(g_j * v_j) \equiv \mathsf{HT}(g_j)v_j$. Depending on this representation of g and our well-founded total ordering $\succeq$ on $\mathcal{G}$ we define $t = \max\{\mathsf{HT}(g_j)v_j \mid j \in \{1, \ldots m\}\}$ and K is the number of polynomials $g_j * v_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\mathrm{p}}_F$-reducible. We will show that g has a special representation which implies that g is top-reducible using F. This will be done by

[26] This is no longer true in case a has an inverse u_a of length $|u_a| > 1$ or no inverse at all.
[27] Then $s \circ b = s_1 a \circ b = s_1 \circ c$ and either $|s \circ b| < K-1$ or $s \circ b \equiv s_1 c$.

induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[28]. If $t \succ \mathsf{HT}(g)$ there are two polynomials g_k, g_l in the corresponding representation[29] and $\mathsf{HT}(g_k)v_k \equiv \mathsf{HT}(g_l)v_l$. Without loss of generality let us assume $\mathsf{HT}(g_k) \equiv \mathsf{HT}(g_l)z$ for some $z \in \mathcal{F}$ and $v_l \equiv zv_k$. Then by definition 3.29 we have a prefix s-polynomial $\mathsf{spol}_p(g_k, g_l) = \mathsf{HC}(g_k)^{-1} \cdot g_k - \mathsf{HC}(g_l)^{-1} \cdot g_l * z$. We will now change our representation of g by using the additional information on this s-polynomial in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume $\mathsf{spol}_p(g_k, g_l) \neq 0$[30]. Hence, the reduction sequence $\mathsf{spol}_p(g_k, g_l) \xrightarrow{*}{}^{\mathrm{p}}_{G} 0$ yields a prefix standard representation of the form $\mathsf{spol}_p(g_k, g_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v_i'$, $\delta_i \in \mathbf{K}^*$,$h_i \in G$,$v_i' \in \mathcal{F}$ and all terms occurring in the sum are bounded by $\mathsf{HT}(\mathsf{spol}_p(g_k, g_l))$. By lemma 4.11 we can conclude that t is a proper bound for all terms occurring in the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i' * v_k$ and again we can substitute all polynomials h_i, where $\mathsf{HT}(h_i * v_i' * v_k) \neq \mathsf{HT}(h_i)(v_i' \circ v_k)$ without increasing t or K. Similarly, in case $v_i' \in \mathcal{E}$, we can substitute h_i by $\psi_{v_i'}(h_i) \in G$ by our assumption. Therefore, without loss of generality we can assume that the representation has the required form. This gives us:

$$
\begin{aligned}
& \alpha_k \cdot g_k * v_k + \alpha_l \cdot g_l * v_l \\
= \;& \alpha_k \cdot g_k * v_k + \underbrace{\alpha_l' \cdot \beta_k \cdot g_k * v_k - \alpha_l' \cdot \beta_k \cdot g_k * v_k}_{=0} + \alpha_l' \cdot \beta_l \cdot g_l * v_l \\
= \;& (\alpha_k + \alpha_l' \cdot \beta_k) \cdot g_k * v_k - \alpha_l' \cdot \underbrace{(\beta_k \cdot g_k * v_k - \beta_l \cdot g_l * v_l)}_{=\mathsf{spol}_p(g_k, g_l) * v_k} \\
= \;& (\alpha_k + \alpha_l' \cdot \beta_k) \cdot g_k * v_k - \alpha_l' \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * v_i' * v_k) \qquad (3)
\end{aligned}
$$

where $\beta_k = \mathsf{HC}(g_k)^{-1}$, $\beta_l = \mathsf{HC}(g_l)^{-1}$ and $\alpha_l' \cdot \beta_l = \alpha_l$. By substituting (3) in our representation of g either t disappears or in case t remains maximal among the terms occurring in the new representation of g, K is decreased.

□

[28] Note that this ordering is well-founded since $\succeq$ is and $K \in \mathbf{N}$.

[29] Not necessarily $g_l \neq g_k$.

[30] In case $\mathsf{spol}_p(g_k, g_l) = 0$, just substitute 0 for $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i'$ in the equations below.

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.