On Gröbner Bases for Two-Sided Ideals in Nilpotent Group Rings

Klaus Madlener, Birgit Reinert
Fachbereich Informatik,
Universität Kaiserslautern
67663 Kaiserslautern, Germany

SR-95-01

Abstract

An algorithm for constructing Gröbner bases for right and for two-sided ideals in nilpotent group rings is presented.

1 Introduction

In 1965 Buchberger introduced the theory of Gröbner bases for polynomial ideals in commutative polynomial rings over fields (see [Bu65]). It established a rewriting approach to the theory of polynomial ideals. Polynomials can be used as rules by giving an admissible term 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.

Since the theory of Gröbner bases turned out to be of outstanding importance for polynomial rings, extensions of Buchberger's ideas to other algebras followed, for example to free algebras ([Mo85, Mo94]), Weyl algebras ([La85]), enveloping fields of Lie algebras ([ApLa88]), solvable rings ([KaWe90, Kr93]), skew polynomial rings ([We92]), free group rings ([Ro93]) and monoid and group rings ([MaRe93b]).

In [MaRe93a] we have combined the ideas of string rewriting and polynomial rewriting in the field of monoid rings and generalized the concept of Gröbner bases to these rings. We assumed that our monoids were presented by finite convergent semi-Thue systems and ordered with the completion ordering of the presentation. This approach is of

course valid for groups, but it makes no use of the additional structural information we have for groups. Group rings have been studied for special classes of groups, and e.g. for free, Abelian, nilpotent or polycyclic groups the congruence problem for right ideals is known to be solvable (see e.g. [Ro93, BaCaMi81, Si94]). In [Re95] we have enclosed how using group presentations, which make use of the structural composition of the respective groups, lead to algorithms to construct finite Gröbner bases for right ideals for special classes of groups: the class of finite groups, the class of free groups, the class of plain groups, the class of context-free groups, and the class of nilpotent groups. In this report we want to present our results on nilpotent groups and how they can be extended to solve the membership problem in two-sided ideals. It is a well-known fact that every finitely generated nilpotent group $\mathcal{G}$ is an extension of a torsion-free nilpotent group $\mathcal{N}$ by a finite group $\mathcal{E}$. Therefore it can be presented by confluent semi-Thue systems of a special form. Due to this presentation we can define a concept of "commutative prefixes" on the group elements which captures the known fact that in the commutative polynomial ring a divisor of a term is also a commutative prefix of this term. This concept can be used to define a Noetherian reduction in the group ring. Since our structure is no longer commutative we study a special form of right reduction called quasi-commutative (qc-)reduction and at first right ideals. Later on we then show how Gröbner bases of two-sided ideals can be characterized by right Gröbner bases additionally requiring that the right ideal generated coincides with the ideal generated. For Abelian groups the latter is obvious and for nilpotent groups we can give additional conditions when this holds. Since we have no admissible ordering, reduction steps are not preserved under multiplication with group elements, i.e., if a polynomial p is reducible using a polynomial f, a multiple $p*w$ for some group element w need no longer be reducible using f. Remember that this was essential in Buchberger's approach as it implies that in case $p \xrightarrow{*}_F 0$ we can conclude $p * w \xrightarrow{*}_F 0$. Furthermore, qc-reduction does not express the right ideal congruence. We introduce different techniques to repair these defects. For a set of polynomials F the set $\{f * e \mid f \in F, e \in \mathcal{E}\}$ is called the $\mathcal{E}$-closure of F, and F is called $\mathcal{N}$-saturated, if for all $f \in F$, $w \in \mathcal{N}$ we have that the right multiple $f * w$ is in one step qc-reducible to zero using F. Using these concepts we give a characterization of a right Gröbner basis by s-polynomials and present an algorithm to compute finite right Gröbner bases. This approach then is extended to compute Gröbner bases of two-sided ideals.

2 Basic Definitions

Let $\mathcal{G}$ be a group with binary operation $\circ$ and identity λ. The elements of a group ring $\mathbf{K}[\mathcal{G}]$ over a field $\mathbf{K}$ can be presented as polynomials $f = \sum_{g \in \mathcal{G}} \alpha_g \cdot g$ where only finitely many coefficients are non-zero. Addition and multiplication for two polynomials $f = \sum_{g \in \mathcal{G}} \alpha_g \cdot g$ and $h = \sum_{g \in \mathcal{G}} \beta_g \cdot g$ are defined as $f + h = \sum_{g \in \mathcal{G}} (\alpha_g + \beta_g) \cdot g$ and $f * h = \sum_{g \in \mathcal{G}} \gamma_g \cdot g$ with $\gamma_g = \sum_{x \circ y = g \in \mathcal{G}} \alpha_x \cdot \beta_y$. For a subset F of $\mathbf{K}[\mathcal{G}]$ we call the set $\mathsf{ideal}_r(F) = \{\sum_{i=1}^{n} \alpha_i \cdot f_i * w_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, f_i \in F, w_i \in \mathcal{G}\}$ the **right ideal** and $\mathsf{ideal}(F) = \{\sum_{i=1}^{n} \alpha_i \cdot u_i * f_i * w_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, f_i \in F, u_i, w_i \in \mathcal{G}\}$ the **two-sided ideal** generated by F. Notice that we have three different multiplications which will

be denoted in different ways: $\cdot$ denotes multiplication with elements in $\mathbf{K}$, $\circ$ denotes multiplication in $\mathcal{G}$ and $*$ stands for the multiplication of polynomials in the group ring.

As we are interested in constructing Gröbner bases for ideals in $\mathbf{K}[\mathcal{G}]$, we need a presentation of the group $\mathcal{G}$ in order to do computations. Since $\mathcal{G}$ is a finitely generated nilpotent group, we can apply knowledge on its structure[1]. Our approach makes use of the well-known fact that a finitely generated nilpotent group $\mathcal{G}$ is an extension of a torsion-free nilpotent group $\mathcal{N}$ by a finite group $\mathcal{E}$. Now torsion-free nilpotent groups and finite groups have special group presentations by finite convergent semi-Thue systems[2] and these can be combined to group presentations of extensions. Next we give the technical details of such presentations for nilpotent groups which are necessary to understand the proofs of the lemmata and theorems. It is important that these presentations allow to treat the elements of $\mathcal{G}$ as special ordered group words and to define a tuple ordering on these representatives which can be used to define a Noetherian reduction. Let us start by giving a presentation of a torsion-free nilpotent group $\mathcal{N}$. Let $\Sigma = \{a_1, a_1^{-1}, \ldots, a_n, a_n^{-1}\}$ be a finite alphabet where a_i^{-1} is called the formal inverse of the letter a_i. For $1 \leq k \leq n$ we define the subsets $\Sigma_k = \{a_i, a_i^{-1} \mid k \leq i \leq n\}$, $\Sigma_{n+1} = \emptyset$. Using the precedence $a_1^{-1} \succ a_1 \succ \ldots a_i^{-1} \succ a_i \succ \ldots \succ a_n^{-1} \succ a_n$ we can define the set of **ordered group words** $\mathsf{ORD}(\Sigma) = \mathsf{ORD}(\Sigma_1)$ recursively by $\mathsf{ORD}(\Sigma_{n+1}) = \{\lambda\}$, and $\mathsf{ORD}(\Sigma_i) = \{w \in \Sigma_i^* \mid w \equiv uv$ for some $u \in \{a_i\}^* \cup \{a_i^{-1}\}^*, v \in \mathsf{ORD}(\Sigma_{i+1})\}$[3]. The semi-Thue system $T_{NC} \cup T_I$ over Σ where $T_{NC} = \{a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} a_j^{\delta} z \mid j > i, \delta, \delta' \in \{1, -1\}, z \in \mathsf{ORD}(\Sigma_{j+1})\}$, $T_I = \{a_i a_i^{-1} \longrightarrow \lambda, a_i^{-1} a_i \longrightarrow \lambda \mid 1 \leq i \leq n\}$ is a presentation of a torsion-free nilpotent group $\mathcal{N}$. By [Wi89] there exist such presentations which are convergent with respect to the syllable ordering induced by the precedence on Σ as defined below. Multiplication of two elements $u, v \in \mathsf{ORD}(\Sigma)$, i.e., $u \circ v$, corresponds to computing the normal form of the word uv.

Definition 1 *Let Σ be an alphabet and $\succ$ a partial ordering on Σ^*. We define an ordering $\succ^{\text{lex}}$ on m-tuples over Σ^* as follows: $(u_0, \ldots, u_m) \succ^{\text{lex}} (v_0, \ldots, v_m)$ if and only if there exists $0 \leq k \leq m$ such that $u_i = v_i$ for all $0 \leq i < k$ and $u_k \succ v_k$. Let $a \in \Sigma$. Then every $w \in \Sigma^*$ can be uniquely decomposed with respect to a as $w \equiv w_0 a w_1 \ldots a w_k$, where $|w|_a = k \geq 0$ and $w_i \in (\Sigma \backslash \{a\})^*$. Given a total precedence $\succ$ on Σ we can then define $u >_{\text{syll}(\Sigma)} v$ if and only if $|u|_a > |v|_a$ or $|u|_a = |v|_a$ and $(u_0, \ldots, u_m) >^{\text{lex}}_{\text{syll}(\Sigma \backslash \{a\})} (v_0, \ldots, v_m)$ where a is the largest letter in Σ according to $\succ$ and $(u_0, \ldots, u_m)$, $(v_0, \ldots, v_m)$ are the decompositions of u and v with respect to a in case $|u|_a = |v|_a = m$.* $\diamond$

The irreducible elements representing the elements in $\mathcal{N}$ are ordered group words. Restricting the syllable ordering to ordered group words we find that $a_1^{i_1} \ldots a_n^{i_n} <_{\text{syll}} a_1^{j_1} \ldots a_n^{j_n}$ if and only if for some $1 \leq d \leq n$ we have $i_l = j_l$ for all $1 \leq l \leq d-1$ and

[1] E.g. see [KaMe79] for more information on this subject.

[2] E.g. see [BoOt93] and [Wi89] for more information on this subject.

[3] Note that $\equiv$ will be used to denote identity of elements as words.

$i_d <_{\mathbf{Z}} j_d$ with[4]

$$\alpha <_{\mathbf{Z}} \beta \text{ iff } \begin{cases} \alpha \geq 0 \text{ and } \beta < 0 \\ \alpha \geq 0, \beta > 0 \text{ and } \alpha < \beta \\ \alpha < 0, \beta < 0 \text{ and } \alpha > \beta \end{cases}$$

where $\leq$ is the usual ordering on $\mathbf{Z}$. We then will call the letter a_d the **distinguishing letter** of the two elements. Now the following lemma from [Wi89] gives some insight how special multiples influence the representation of the element representing the product. It will be used extensively in the proofs later on.

Lemma 1 *Let $\mathcal{G}$ have a convergent presentation $(\Sigma, T_{NC} \cup T_I)$. Further for some $1 \leq j < i \leq n$ let $w_1 \in \mathsf{ORD}(\Sigma \backslash \Sigma_j)$, $w_2 \in \mathsf{ORD}(\Sigma_{i+1})$. Then we have $a_i \circ w_1 \equiv w_1 a_i z_1$ and $w_2 \circ a_i \equiv a_i z_2$ for some $z_1, z_2 \in \mathsf{ORD}(\Sigma_{i+1})$. In particular the occurrence of the letter a_i is not affected by these multiplications.* □

Let us proceed to give a presentation of $\mathcal{G}$ in terms of $\mathcal{N}$ and $\mathcal{E}$ by assuming that $\mathcal{E}$ is presented by its multiplication table[5] and $\mathcal{N}$ is presented by $(\Sigma, T_{NC} \cup T_I)$ as described above. For all $e \in \mathcal{E}$ let $\phi_e : \Sigma \longrightarrow \mathcal{N}$ be a function such that ϕ_λ is the inclusion and for all $a \in \Sigma$, $\phi_e(a) = \mathsf{inv}(e) \circ_{\mathcal{G}} a \circ_{\mathcal{G}} e$. For all $e_1, e_2 \in \mathcal{E}$ let $z_{e_1,e_2} \in \mathcal{N}$ 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 $e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3$, $e_1 \circ_{\mathcal{G}} e_2 \equiv e_3 z_{e_1,e_2}$. Assuming $(\mathcal{E} \backslash \{\lambda\}) \cap \Sigma = \emptyset$, let $\Gamma = (\mathcal{E} \backslash \{\lambda\}) \cup \Sigma$ and let T consist of the sets of rules T_{NC} and T_I, and the following additional rules:

$$\begin{array}{lll} e_1 e_2 & \longrightarrow & e_3 z_{e_1,e_2} \quad \text{for all } e_1, e_2 \in \mathcal{E} \backslash \{\lambda\}, e_3 \in \mathcal{E} \text{ such that } e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3, \\ a e & \longrightarrow & e \phi_e(a) \quad \text{for all } e \in \mathcal{E} \backslash \{\lambda\}, a \in \Sigma. \end{array}$$

Then (Γ, T) is a convergent presentation of $\mathcal{G}$ as an extension of $\mathcal{N}$ by $\mathcal{E}$. Every element in $\mathcal{G}$ has a representative of the form eu where $e \in \mathcal{E}$ and $u \in \mathcal{N}$. We can specify a total well-founded ordering $\succ$ on our group by combining a total well-founded ordering $\succeq_{\mathcal{E}}$ on $\mathcal{E}$ and the syllable ordering $\geq_{\text{syll}}$ on $\mathcal{N}$: For $e_1 u_1, e_2 u_2 \in \mathcal{G}$ we define $e_1 u_1 \succ e_2 u_2$ if and only if $e_1 \succ_{\mathcal{E}} e_2$ or ($e_1 = e_2$ and $u_1 >_{\text{syll}} u_2$). Furthermore, we can define a tuple ordering on $\mathcal{G}$ as follows: For two elements $w \equiv e a_1^{i_1} \ldots a_n^{i_n}, v \equiv e a_1^{j_1} \ldots a_n^{j_n}$, we define $w \geq_{\text{tup}} v$ if for each $1 \leq l \leq n$ we have either $j_l = 0$ or $\mathsf{sgn}(i_l) = \mathsf{sgn}(j_l)$ and $|i_l| \geq |j_l|$ where $\mathsf{sgn}(i)$ is the sign of the non-zero integer i. Further we define $w >_{\text{tup}} v$ if $w \geq_{\text{tup}} v$ and $|i_l| > |j_l|$ for some $1 \leq l \leq n$ and we define $w \geq_{\text{tup}} \lambda$ for all $w \in \mathcal{G}$. According to this ordering we call v a (commutative) **prefix** of w if $v \leq_{\text{tup}} w$. Notice that this ordering captures the fact that a divisor of a term in the ordinary polynomial ring is also a commutative prefix of the term. The tuple ordering is not total on $\mathcal{G}$ but we find that $v \leq_{\text{tup}} w$ implies $v \preceq w$. Now using such presentations we can state the following lemma which later on will enable a Noetherian definition of reduction.

Lemma 2 *Let $w, v, \tilde{v} \in \mathcal{G}$ with $w \geq_{\text{tup}} v$ and $v \succ \tilde{v}$. Then for $u \in \mathcal{G}$ such that $w = v \circ u$, we get $w \succ \tilde{v} \circ u$. Notice that since $\mathcal{G}$ is a group, u always exists and is unique, namely $u = \mathsf{inv}(v) \circ w$. Moreover, if $v \neq \lambda$, then $u \in \mathcal{N}$.*

[4]This ordering corresponds to $0 < 1 < 2 < \ldots < -1 < -2 < \ldots$.

[5]Similar approaches are possible for other presentations of $\mathcal{E}$ by convergent semi-Thue systems, e.g. nilpotent presentations of the finite group.

Proof : Without loss of generality[6] let us assume that the $\mathcal{E}$-part of w, v and $\tilde{v}$ is λ, i.e., $w, v, \tilde{v} \in \mathsf{ORD}(\Sigma)$. Let $w, v, \tilde{v}, u \in \mathcal{G}$ be presented by ordered group words, i.e., $w \equiv a_1^{w_1} \dots a_n^{w_n}$, $v \equiv a_1^{v_1} \dots a_n^{v_n}$, $\tilde{v} \equiv a_1^{\tilde{v}_1} \dots a_n^{\tilde{v}_n}$, and $u \equiv a_1^{u_1} \dots a_n^{u_n}$ with $w_i, v_i, \tilde{v}_i, u_i \in \mathbf{Z}$.
Further let a_d be the distinguishing letter between v and $\tilde{v}$, i.e., $v_d >_{\mathbf{Z}} \tilde{v}_d$. Since the commutation system only includes rules of the form $a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} a_j^{\delta} z$, $j > i$, $z \in \mathsf{ORD}(\Sigma_{j+1}), \delta, \delta' \in \{1, -1\}$ and we have no P-rules, we can conclude

$$a_1^{v_1} \dots a_{d-1}^{v_{d-1}} \circ a_1^{u_1} \dots a_{d-1}^{u_{d-1}} = a_1^{\tilde{v}_1} \dots a_{d-1}^{\tilde{v}_{d-1}} \circ a_1^{u_1} \dots a_{d-1}^{u_{d-1}} \equiv a_1^{w_1} \dots a_{d-1}^{w_{d-1}} a_d^{s_d} \dots a_n^{s_n}$$

for some $s_i \in \mathbf{Z}$. Moreover, $a_d^{v_d} \circ a_d^{s_d} \circ a_d^{u_d} = a_d^{w_d}$, i.e., $v_d + s_d + u_d = w_d$. To prove $w_d >_{\mathbf{Z}} \tilde{v}_d + s_d + u_d$ and hence $w >_{\text{syll}} \tilde{v} \circ u$, we have to take a closer look at v_d and $\tilde{v}_d$.

1. In case $v_d > 0$ this implies $w_d > 0$ as $w \geq_{\text{tup}} v$. Therefore, $v_d + s_d + u_d = w_d$ and $w_d \geq v_d > 0$ give us $s_d + u_d \geq 0$. Now $v >_{\text{syll}} \tilde{v}$ and $v_d > 0$ imply that $v_d > \tilde{v}_d \geq 0$, as otherwise $\tilde{v}_d \geq_{\mathbf{Z}} v_d$ would contradict our assumption. Hence we get $\tilde{v}_d + s_d + u_d < w_d$, implying $w >_{\text{syll}} \tilde{v} \circ u$.

2. In case $v_d < 0$ this implies $w_d < 0$, $|w_d| \geq |v_d|$ and thus $v_d + s_d + u_d = w_d$ yields $s_d + u_d \leq 0$. Further we know $|v_d| + |s_d + u_d| = |w_d|$. We have to distinguish two cases:

   (a) In case $\tilde{v}_d \leq 0$, then $v >_{\text{syll}} \tilde{v}$ implies $|v_d| > |\tilde{v}_d|$. Therefore, we get $|\tilde{v}_d| + |s_d + u_d| < |w_d|$ and $w >_{\text{syll}} \tilde{v} \circ u$.

   (b) In case $\tilde{v}_d > 0$, as $s_d + u_d \leq 0$ we have to take a closer look at $\tilde{v}_d + s_d + u_d$. In case $\tilde{v}_d + s_d + u_d \geq 0$ we are done as this implies $w >_{\text{syll}} \tilde{v} \circ u$. In case $\tilde{v}_d + s_d + u_d < 0$ we get that $\tilde{v}_d < |s_d + u_d|$ implying $|\tilde{v}_d + s_d + u_d| < |s_d + u_d| < |w_d|$ and hence $w >_{\text{syll}} \tilde{v} \circ u$. □

Notice that assuming $\mathcal{E}$ is presented by a convergent semi-Thue system (Δ, R) in the definition of the tuple ordering we might be able to use additional information we have on the representatives of the elements in $\mathcal{E}$ or the rules in R to refine this ordering in order to allow more multiples for reduction later on. When doing so one has to ensure that the refinements only allow multiplications which are compatible in the sense of the previous lemma.

3 Reduction in Nilpotent Group Rings

Given a non-zero polynomial p in $\mathbf{K}[\mathcal{G}]$, the so-called 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 the head monomial

[6] This assumption can be made as for $w \equiv e_1 w', v \equiv e_2 v', \tilde{v} \equiv e_3 \tilde{v}'$ with $w', v', \tilde{v}' \in \mathsf{ORD}(\Sigma)$, $w \geq_{\text{tup}} v$ implies $e_1 = e_2$ and $v \succ \tilde{v}$ either implies $e_1 \succ e_3$ and we are done as $u \in \mathcal{N}$ or $e_1 = e_3$.

is $\mathsf{HM}(p) = \mathsf{HC}(p) \cdot \mathsf{HT}(p)$. $\mathsf{T}(p)$ is the set of terms occurring in p. The ordering on $\mathcal{G}$ can be lifted to a partial ordering on $\mathbf{K}[\mathcal{G}]$ by setting $p > q$ if and only if $\mathsf{HT}(p) \succ \mathsf{HT}(q)$ or ($\mathsf{HM}(p) = \mathsf{HM}(q)$ and $p - \mathsf{HM}(p) > q - \mathsf{HM}(q)$). Now using the head monomial of a polynomial as a left hand side of a rule, we can define reduction. Frequently in polynomial rings reduction is defined in case the head term of the polynomial is a divisor of the term of the monomial to be reduced. Now in groups every element t is a divisor of every other element s since $t \circ (\mathsf{inv}(t) \circ s) = s$ holds. But defining reduction requiring only divisibility would not be Noetherian as the following example shows.

Example 1 *Let $\Sigma = \{a, a^{-1}\}$ and $T = \{aa^{-1} \longrightarrow \lambda, a^{-1}a \longrightarrow \lambda\}$ be a presentation of a nilpotent group $\mathcal{G}$. Suppose we simply require divisibility of the head term to allow reduction. Then we could reduce the polynomial $a^2 + 1 \in \mathbf{Q}[\mathcal{G}]$ at the monomial a^2 by the polynomial $a^{-1} + a$ as $a^2 = a^{-1} \circ a^3$. This would give*

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

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

Hence we will give additional restrictions on the divisibility property required to allow reduction. Since $\mathcal{G}$ in general is not commutative, we will restrict ourselves to right multiples to define reduction.

Definition 2 *Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{G}]$.*
We say f **quasi-commutatively (qc-)reduces** *p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow_f^{\mathrm{qc}} q$, if*

(a) $t \geq_{\mathrm{tup}} \mathsf{HT}(f)$, and

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

Quasi-commutative reduction by a set $F \subseteq \mathbf{K}[\mathcal{G}]$ is denoted by $p \longrightarrow_F^{\mathrm{qc}} q$ and abbreviates $p \longrightarrow_f^{\mathrm{qc}} q$ for some $f \in F$. ◇

Notice that if f qc-reduces p at $\alpha \cdot t$ to q, then t no longer is a term in q and by lemma 2 $p > q$ holds. This reduction is effective, as it is possible to decide, whether we have $t \geq_{\mathrm{tup}} \mathsf{HT}(f)$. Further it is Noetherian and the translation lemma holds.

Lemma 3
Let F be a set of polynomials in $\mathbf{K}[\mathcal{G}]$ and $p, q, h \in \mathbf{K}[\mathcal{G}]$ some polynomials.

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

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

Proof :

1. Let $p - q \longrightarrow_F^{\mathrm{qc}} h = p - q - \alpha \cdot f * w$, where $\alpha \in \mathbf{K}^*$, $f \in F, w \in \mathcal{G}$ and $\mathsf{HT}(f) \circ w = t \geq_{\mathrm{tup}} \mathsf{HT}(f)$, i.e. $\alpha \cdot \mathsf{HC}(f)$ 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 qc-reduction. We then get $p \longrightarrow_f^{\mathrm{qc}} p - \alpha_1 \cdot f * w = p'$ and $q \longrightarrow_f^{\mathrm{qc}} q - \alpha_2 \cdot f * w = q'$, 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 qc-reduction and get $p \longrightarrow_f^{\mathrm{qc}} p - \alpha \cdot f * w = p'$ 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 qc-reduction and get $q \longrightarrow_f^{\mathrm{qc}} q + \alpha \cdot f * w = q'$ and $p = p'$.

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

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

□

But qc-reduction does not capture the right ideal congruence. One reason is that a reduction step is not preserved under right multiplication with elements of $\mathcal{G}$.

Example 2 *Let $\mathcal{G}$ be the group given in example 1. Then for the polynomials $p = a^2 + a$ and $f = a + \lambda$ we find that p is qc-reducible by f. This is no longer true for the multiple $p * a^{-2} = (a^2 + a) * a^{-2} = \lambda + a^{-1}$. Notice that, since $a^{-1} + \lambda \in \mathsf{ideal}_r(p)$ we have $a^{-1} + \lambda \equiv_{\mathsf{ideal}_r(p)} 0$, but $a^{-1} + \lambda \xleftrightarrow{*}_p 0$ does not hold.* ◇

As we have seen in this example, different terms of a polynomial can come to head position by right multiplication with group elements. This is due to the fact that the well-founded ordering on $\mathcal{G}$ is not compatible with right multiplication[7]. The next lemma states that $\mathcal{N}$-right-multiples which bring other terms to head position can be constructed in case they exist.

Lemma 4 *Let p be a non-zero polynomial in $\mathbf{K}[\mathcal{G}]$. In case there exists an element $w \in \mathcal{N}$ such that $\mathsf{HT}(p * w) = t \circ w$ for some $t \in \mathsf{T}(p)$, let a_d be the distinguishing letter between t and $\mathsf{HT}(p)$. Then one can construct an element $v \in \mathsf{ORD}(\Sigma_d)$ such that $\mathsf{HT}(p * v) = t \circ v$.*

[7] No total, well-founded ordering with this property can exist for a group due to the existence of inverses.

Proof : We show that for all polynomials $q \in \{p * u | u \in \mathcal{G}\}$ the following holds: In case $\mathsf{HT}(q * w) = t_i \circ w$ for some $w \in \mathcal{G}$, $t_i \in \mathsf{T}(q)$ then one can construct an element $v \in \mathsf{ORD}(\Sigma_d)$ where a_d is the distinguishing letter between t_i and $\mathsf{HT}(q)$, and $\mathsf{HT}(q * v) = t_i \circ v$.
This will be done by induction on k where $d = n - k$. Without loss of generality[8] let us assume that the $\mathcal{E}$-part of the terms in p is λ, i.e., for all $t \in \mathsf{T}(p)$ we have $t \in \mathsf{ORD}(\Sigma)$. In the base case let $k = 0$, i.e., a_n is the distinguishing letter between $\mathsf{HT}(q) = t_1 \equiv a_1^{1_1} \ldots a_n^{1_n}$ and $t_i \equiv a_1^{i_1} \ldots a_n^{i_n}$. Hence $1_j = i_j$ for all $1 \leq j \leq n-1$ and $1_n >_{\mathbf{Z}} i_n$.
By our assumption there exists $w \in \mathcal{G}$ such that $\mathsf{HT}(q * w) = t_i \circ w$, with $w \equiv w' a_n^{w_n}$, $w' \in \mathsf{ORD}(\Sigma \backslash \Sigma_n)$, and there exist $k_1, \ldots, k_{n-1}, x \in \mathbf{Z}$ such that $t_1 \circ w = a_1^{1_1} \ldots a_n^{1_n} \circ w = a_1^{1_1} \ldots a_{n-1}^{1_{n-1}} \circ w \circ a_n^{1_n} = (a_1^{1_1} \ldots a_{n-1}^{1_{n-1}} \circ w') \circ a_n^{1_n + w_n} \equiv a_1^{k_1} \ldots a_{n-1}^{k_{n-1}} a_n^{1_n + x}$ and $t_i \circ w = a_1^{1_1} \ldots a_{n-1}^{1_{n-1}} a_n^{i_n} \circ w = a_1^{1_1} \ldots a_{n-1}^{1_{n-1}} \circ w \circ a_n^{i_n} = (a_1^{1_1} \ldots a_{n-1}^{1_{n-1}} \circ w') \circ a_n^{i_n + w_n} \equiv a_1^{k_1} \ldots a_{n-1}^{k_{n-1}} a_n^{i_n + x}$. Thus $1_n + x <_{\mathbf{Z}} i_n + x$ must hold. Let us set $v \equiv a_n^{-1_n}$. We show that for all $t_j \in T(q) \backslash \{t_i\}$ we have $t_i \circ v \succ t_j \circ v$. Note that for all t_j with prefix $a_1^{j_1} \ldots a_{n-1}^{j_{n-1}} \prec a_1^{1_1} \ldots a_{n-1}^{1_{n-1}}$ we have $t_j \circ v \prec t_i \circ v$, as right multiplication with $v \equiv a_n^{-1_n}$ only changes the exponent of a_n in the respective term. It remains to look at those terms t_j with $a_1^{j_1} \ldots a_{n-1}^{j_{n-1}} \equiv a_1^{1_1} \ldots a_{n-1}^{1_{n-1}}$. Hence, let us assume that there exists a term t_j such that $t_j \circ v \succ t_i \circ v$, i.e., $j_n - 1_n >_{\mathbf{Z}} i_n - 1_n$.
Since $\mathsf{HT}(q * w) = t_i \circ w$ we know $j_n + x <_{\mathbf{Z}} i_n + x$ and $1_n + x <_{\mathbf{Z}} i_n + x$. Furthermore, as $t_1 = \mathsf{HT}(q)$ we have $1_n >_{\mathbf{Z}} i_n$ and $1_n >_{\mathbf{Z}} j_n$. We prove that $t_j \circ v \succ t_i \circ v$ yields $j_n + x >_{\mathbf{Z}} i_n + x$ contradicting our assumption by analysing the possible cases for these exponents.
First suppose that $1_n < 0$ and thus $1_n + x <_{\mathbf{Z}} i_n + x$ implies $x \geq |1_n| > 0$[9]. Then in case $i_n \leq 0$ this gives us $|1_n| > |i_n|$. Now $j_n - 1_n >_{\mathbf{Z}} i_n - 1_n > 0$ and $j_n - 1_n > 0$ yield either $j_n > 0$ or ($j_n \leq 0$ and $|j_n| < |i_n|$), both implying $j_n + y > i_n + y$ for all $y \geq |1_n|$, especially for $y = x$.
In case $i_n > 0$ as before $j_n - 1_n >_{\mathbf{Z}} i_n - 1_n > 0$ and $j_n - 1_n > 0$ imply $j_n > i_n$ and for all $y \geq |1_n|$ we get $j_n + y > i_n + y$, especially for $y = x$.
Hence let us assume that $1_n > 0$ and thus $1_n + x <_{\mathbf{Z}} i_n + x$ implies $x < 0$ and $|x| > i_n$, since $1_n > i_n \geq 0$ and $1_n > j_n \geq 0$.
Now $j_n - 1_n >_{\mathbf{Z}} i_n - 1_n$ and $i_n - 1_n < 0$ imply $j_n - 1_n < 0$ and $|i_n - 1_n| < |j_n - 1_n|$. Hence we get $j_n < i_n$ and for all $y < 0$ with $|y| > j_n$ we have $j_n + y >_{\mathbf{Z}} i_n + y$, especially for $y = x$ as $|x| > i_n > j_n$.
In the induction step let us assume that for all polynomials $q \in \{p * u | u \in \mathcal{G}\}$ and $w \in \mathcal{G}$ with $\mathsf{HT}(q * w) = t_i \circ w$, if the distinguishing letter a_d between $\mathsf{HT}(q)$ and t_i has index $d \geq n - (k-1)$ there exists an element $v' \in \mathsf{ORD}(\Sigma_d)$ such that $\mathsf{HT}(q * v') = t_i \circ v'$. Now for $q \in \{p * u | u \in \mathcal{G}\}$, $w \in \mathcal{G}$ with $\mathsf{HT}(q * w) = t_i \circ w$ let us assume that the distinguishing letter between $\mathsf{HT}(q)$ and t_i has index $d = n - k$.
Since $\mathsf{HT}(q * w) = t_i \circ w$, for $w \equiv w' a_d^{w_d} w''$ with $w' \in \mathsf{ORD}(\Sigma \backslash \Sigma_d)$, $w'' \in \mathsf{ORD}(\Sigma_{d+1})$,

[8] This can be done as $\mathcal{N}$-right-multiples do not change the $\mathcal{E}$-part of a term.
[9] $x < 0$ would imply $1_n + x < i_n + x$ and $1_n + x < 0$, hence $1_n + x >_{\mathbf{Z}} i_n + x$.

we know that there exist $k_1, \ldots, k_{d-1}, x \in \mathbf{Z}$ and $z_1, z_i, \tilde{z}_1 \in \mathsf{ORD}(\Sigma_{d+1})$ such that $t_1 \circ w = a_1^{1_1} \ldots a_n^{1_n} \circ w = a_1^{1_1} \ldots a_{d-1}^{1_{d-1}} \circ w' \circ a_d^{1_d} \circ \tilde{z}_1 \equiv a_1^{k_1} \ldots a_{d-1}^{k_{d-1}} a_n^{1_d+x} z_1$ and similarly $t_i \circ w = a_1^{k_1} \ldots a_{d-1}^{k_{d-1}} a_n^{i_d+x} z_i$. As $1_d \neq i_d$ then $1_d + x <_{\mathbf{Z}} i_d + x$ must hold and we can set $v_d \equiv a_n^{-1_d}$.
We have to show that for all $t_j \in T(q) \backslash \{t_i\}$ there exists $v \in \mathsf{ORD}(\Sigma_d)$ such that we have $t_i \circ v \succ t_j \circ v$. Note that for all t_j with prefix $a_1^{j_1} \ldots a_{d-1}^{j_{d-1}} \prec a_1^{1_1} \ldots a_{d-1}^{1_{d-1}}$ we have $t_j \circ v_d \prec t_i \circ v_d$, as right multiplication with $v_d \equiv a_n^{-1_d}$ has no influence on the prefix in $\mathsf{ORD}(\Sigma \backslash \Sigma_d)$.
Therefore, it remains to look at those terms t_j with $a_1^{j_1} \ldots a_{d-1}^{j_{d-1}} \equiv a_1^{1_1} \ldots a_{d-1}^{1_{d-1}}$. Let us assume that there exists a term t_j such that $t_j \circ v_d \succ t_i \circ v_d$, i.e., $j_d - 1_d \geq_{\mathbf{Z}} i_d - 1_d$. We will show that then $j_d = i_d$ and hence our induction hypothesis can be applied since for the polynomial $q * v_d$ the distinguishing letter between $\mathsf{HT}(q * v_d)$ and $t_i \circ v_d$ is of index $d' > d = n - k$ and by our assumption there exists $\mathsf{inv}(v_d) \circ w \in \mathcal{G}$ such that $\mathsf{HT}((q * v_d) * (\mathsf{inv}(v_d) \circ w)) = \mathsf{HT}(q * w) = t_i \circ w = t_i \circ (\mathsf{inv}(v_d) \circ w)$. Hence there exists $\tilde{v} \in \mathsf{ORD}(\Sigma_{d'})$ such that $\mathsf{HT}(q * v_d * \tilde{v}) = t_i \circ v_d \circ \tilde{v}$ and we set $v \equiv v_d \tilde{v} \in \mathsf{ORD}(\Sigma_d)$ and are done.
It remains to show that $j_d = i_d$ must hold. We know $j_d + x \leq_{\mathbf{Z}} i_d + x$ and $1_d + x <_{\mathbf{Z}} i_d + x$ since $\mathsf{HT}(q * w) = t_i \circ w$. Next we prove that $t_j \circ v \succ t_i \circ v$ implies $j_d = i_d$ by analysing the possible cases.
First suppose that $1_d < 0$ and thus $1_d + x <_{\mathbf{Z}} i_d + x$ implies $x \geq |1_d| > 0$ as before.
Then in case $i_d \leq 0$ this gives us $|1_d| > |i_d|$. Now $j_d - 1_d \geq_{\mathbf{Z}} i_d - 1_d > 0$ and $j_d - 1_d > 0$ yield either $j_d > 0$ or ($j_d \leq 0$ and $|j_d| \leq |i_d|$), both implying $j_d + y \geq i_d + y$ for all $y \geq |1_d|$. Thus as $x \geq |1_d|$ we get $j_d + x \geq i_d + x$ yielding $j_d = i_d$.
In case $i_d > 0$ as before $j_d - 1_d \geq_{\mathbf{Z}} i_d - 1_d > 0$ and $j_d - 1_d > 0$ yield $j_d \geq i_d$, and for all $y \geq |1_n|$ we get $j_d + y \geq i_d + y$. Thus as $x \geq |1_d|$, $j_d + x \geq i_d + x$ again yields $j_d = i_d$.
Therefore, let us assume that $1_d > 0$ and thus $1_d + x <_{\mathbf{Z}} i_d + x$ implies $x < 0$ and $|x| > i_d$, since $1_d > i_d \geq 0$ and $1_d \geq j_d \geq 0$. Now $j_d - 1_d \geq_{\mathbf{Z}} i_d - 1_d$ and $i_d - 1_d < 0$ imply $j_d - 1_d < 0$ and $|i_d - 1_d| \leq |j_d - 1_d|$. Hence we get $j_d \leq i_d$ and for all $y < 0$ with $|y| > j_d$, we have $j_d + y \geq_{\mathbf{Z}} i_d + y$. Thus as $|x| > i_d \geq j_d$, then $j_d + x \geq_{\mathbf{Z}} i_d + x$ yields $j_d = i_d$. □

Notice that the proof of this lemma shows that there is an algorithm which computes some $v \in \mathsf{ORD}(\Sigma_d)$ as desired in case it exists and that the element w need not be known for this computation.

Remark 1 *The element v constructed in the proof of the previous lemma can be made "minimal" among all elements having this property by modifying the construction slightly. In case for the distinguishing letter a_d we have $i_d \geq 0 > 1_d$ or $0 \geq i_d > 1_d$ we still use $v_d \equiv a_d^{-1_d}$ in the construction. For the other case $1_d > i_d \geq 0$ we then use $v_d \equiv a_d^{-i_d-1}$.* ◇

For a polynomial p and a term $t \in \mathsf{T}(p)$ we call a term s in a multiple $p * w$ a t-**term** if $s = t \circ w$. The following lemma states that if in two $\mathcal{N}$-right-multiples of a polynomial

the head terms result from the same term t, then there is also a right multiple of the polynomial with a t-term as head term which is in some sense a common commutative prefix of the head terms of the original two multiples. In example 2 for $p * \lambda = a^2 + a$ and $p * a^{-1} = a + \lambda$, both head terms result from the term a^2 and the head term a of $p * a^{-1}$ is a commutative prefix of the head term a^2 of $p * \lambda$.

Lemma 5 *For $u, v \in \mathcal{N}$, let $p * u$ and $p * v$ be two right multiples of a non-zero polynomial $p \in \mathbf{K}[\mathcal{G}]$ such that for some term $t \in \mathsf{T}(p)$ the head terms are t-terms, i.e., $\mathsf{HT}(p * u) = t \circ u \equiv e a_1^{i_1} \dots a_n^{i_n}$ and $\mathsf{HT}(p * v) = t \circ v \equiv e a_1^{j_1} \dots a_n^{j_n}$. Then there exists a term $\tilde{t} \leq_{\text{tup}} e a_1^{\rho_1} \dots a_n^{\rho_n}$ where*

$$\rho_l = \begin{cases} \mathsf{sgn}(i_l) \cdot \min\{|i_l|, |j_l|\} & \mathsf{sgn}(i_l) = \mathsf{sgn}(j_l) \\ 0 & \textit{otherwise} \end{cases}$$

and an element $\tilde{z} \in \mathcal{N}$ such that $\mathsf{HT}(p * \tilde{z}) = t \circ \tilde{z} = \tilde{t}$. In particular, we have $p * u \longrightarrow^{\text{qc}}_{p*\tilde{z}} 0$ and $p * v \longrightarrow^{\text{qc}}_{p*\tilde{z}} 0$.

Proof : Let p, $p * u$ and $p * v$ be as described in the lemma and let the letters corresponding to our presentation be $\Sigma = \{a_1, \dots, a_n, a_1^{-1}, \dots, a_n^{-1}\}$. Without loss of generality[10] let us assume that the $\mathcal{E}$-part of the terms in p and q is λ, i.e., for all $t \in \mathsf{T}(\{p, q\})$ we have $t \in \mathsf{ORD}(\Sigma)$.
We show the existence of $\tilde{z}$ by constructing a sequence $z_1, \dots, z_n \in \mathcal{G}$, such that for $1 \leq l \leq n$ we have $\mathsf{HT}(p * z_l) = t \circ z_l \equiv a_1^{s_1} \dots a_l^{s_l} r_l$ with $r_l \in \mathsf{ORD}(\Sigma_{l+1})$ and $a_1^{s_1} \dots a_l^{s_l} \leq_{\text{tup}} a_1^{\rho_1} \dots a_l^{\rho_l}$. Then for $\tilde{z} = z_n$ our claim holds.
Let us start by constructing an element $z_1 \in \mathcal{G}$ such that $\mathsf{HT}(p * z_1) = t \circ z_1 \equiv a_1^{s_1} r_1$, $r_1 \in \mathsf{ORD}(\Sigma_2)$ and $a_1^{s_1} \leq_{\text{tup}} a_1^{\rho_1}$.
In case $i_1 = j_1$ or $j_1 = 0$ we can set $z_1 = v$ and $s_1 = j_1 = \rho_1$ since $\mathsf{HT}(p * v) = t \circ v \equiv a_1^{j_1} \dots a_n^{j_n}$. Similarly in case $i_1 = 0$ we can set $z_1 = u$ and $s_1 = i_1 = 0 = \rho_1$ since $\mathsf{HT}(p * u) = t \circ u \equiv a_2^{i_2} \dots a_n^{i_n} \in \mathsf{ORD}(\Sigma_2)$. Hence let us assume $i_1 \neq j_1$ and both are non-zero.
First suppose that $\mathsf{sgn}(i_1) = \mathsf{sgn}(j_1)$. Then if $|i_1| \geq |j_1|$ we again set $z_1 = v$ since for $s_1 = j_1 = \rho_1$ our claim holds. In case $|j_1| > |i_1|$ we set $z_1 = u$ because for $s_1 = i_1 = \rho_1$ our claim holds.
Now let us proceed with the case $\mathsf{sgn}(i_1) \neq \mathsf{sgn}(j_1)$, i.e., we construct $z_1 \in \mathcal{G}$ such that $\mathsf{HT}(p * z_1) = t \circ z_1 \in \mathsf{ORD}(\Sigma_2)$ as $\rho_1 = 0$. We claim that the letter a_1 has the same exponent for all terms in $\mathsf{T}(p)$, say b. In case this holds, no term in the polynomial $p * a_1^{-b}$ will contain the letter a_1 and the distinguishing letter between $\mathsf{HT}(p * a_1^{-b})$ and the term $t \circ a_1^{-b}$ is at least of index 2. Furthermore we know $\mathsf{HT}((p * a_1^{-b}) * (a_1^b \circ v)) = \mathsf{HT}(p * v) = t \circ v$. Thus by lemma 4 there exists an element $r \in \mathsf{ORD}(\Sigma_2)$ such that $\mathsf{HT}((p * a_1^{-b}) * r) = t \circ a_1^{-b} \circ r \in \mathsf{ORD}(\Sigma_2)$ and thus we can set $z_1 = a_1^{-b} r$ and $s_1 = 0 = \rho_1$.

[10] As before this can be done as $\mathcal{N}$-right-multiples do not change the $\mathcal{E}$-part of a term.

Hence it remains to prove our initial claim. Suppose we have the representatives $s' \equiv a_1^{b_{s'}} x_{s'}$, $b_{s'} \in \mathbf{Z}$, $x_{s'} \in \mathsf{ORD}(\Sigma_2)$ for the terms $s' \in \mathsf{T}(p)$ and $\mathsf{HT}(p) = s \equiv a_1^{b_s} x_s$. Then we know $b_s \geq_{\mathbf{Z}} b_t$ since $t \in \mathsf{T}(p)$.
Hence in showing that the case $b_s >_{\mathbf{Z}} b_t$ is not possible we find that the exponents of a_1 in s and t are equal. To see this, let us study the possible cases. If $b_s > 0$ we have $b_s > b_t \geq 0$ and hence there exists no $x \in \mathbf{Z}$ such that $b_t + x > b_s + x \geq 0$. On the other hand $b_s < 0$ either implies $b_t > 0$ or ($b_t \leq 0$ and $|b_s| > |b_t|$). In both cases there exists no $x \in \mathbf{Z}$ such that $b_t + x < 0$ and $|b_t + x| > |b_s + x|$. Hence $b_t = b_s$ must hold as we know that t can be brought to head position by u respectively v such that the exponents of a_1 in $\mathsf{HT}(p * u)$ respectively $\mathsf{HT}(p * v)$ have different sign.
It remains to show that there cannot exist a term $s' \in \mathsf{T}(p)$ with $b_{s'} <_{\mathbf{Z}} b_s = b_t$. Let us assume such an s' exists. Since $\mathsf{HT}(p * u) = t \circ u \equiv a_1^{i_1} \ldots a_n^{i_n}$ and $\mathsf{HT}(p * v) = t \circ v \equiv a_1^{j_1} \ldots a_n^{j_n}$ there then must exist $x_1, x_2 \in \mathbf{Z}$ such that $b_{s'} + x_1 <_{\mathbf{Z}} b_t + x_1 = i_1$ and $b_{s'} + x_2 <_{\mathbf{Z}} b_t + x_2 = j_1$. Without loss of generality let us assume $i_1 > 0$ and $j_1 < 0$ (the other case is symmetric). In case $b_t < 0$ we get that $b_t + x_1 = i_1 > 0$ implies $x_1 > |b_t| > 0$. Now, as $b_{s'} <_{\mathbf{Z}} b_t$ either implies $b_{s'} > 0$ or ($b_{s'} \leq 0$ and $|b_{s'}| < |b_t|$), we find $b_{s'} + x_1 > b_t + x_1$ contradicting $b_{s'} + x_1 <_{\mathbf{Z}} b_t + x_1$. On the other hand, in case $b_t > 0$ we know $b_t > b_{s'} \geq 0$. Furthermore, $b_t + x_2 = j_1 < 0$ implies $x_2 < 0$ and $|x_2| > b_t$. Hence we get $b_{s'} + x_2 < 0$ and $|b_{s'} + x_2| > |b_t + x_2|$ contradicting $b_{s'} + x_2 <_{\mathbf{Z}} b_t + x_2$.
Thus let us assume that for the letter a_{k-1} we have constructed $z_{k-1} \in \mathcal{G}$ such that $\mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} r_{k-1} \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ with $r_{k-1} \in \mathsf{ORD}(\Sigma_k)$, $r' \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} \leq_{\mathrm{tup}} a_1^{\rho_1} \ldots a_{k-1}^{\rho_{k-1}}$. We now show that we can find $z_k = z_{k-1} \circ \tilde{w} \in \mathcal{G}$ such that $\mathsf{HT}(p * z_k) = t \circ z_k \equiv a_1^{s_1} \ldots a_k^{s_k} r_k$ with $r_k \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_1^{s_1} \ldots a_k^{s_k} \leq_{\mathrm{tup}} a_1^{\rho_1} \ldots a_k^{\rho_k}$.
This will be done in two steps. First we show that for the polynomials $p * u$ and $p * z_{k-1}$ with head terms $a_1^{i_1} \ldots a_n^{i_n}$ respectively $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ we can find an element $w_1 \in \mathcal{G}$ such that $\mathsf{HT}(p * z_{k-1} * w_1) = t \circ z_{k-1} \circ w_1 \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{\tilde{s}_k} \tilde{r}$, $\tilde{r} \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{\tilde{s}_k} \leq_{\mathrm{tup}} a_k^{\tilde{\rho}_k}$ with

$$\tilde{\rho}_k = \begin{cases} \mathsf{sgn}(i_k) \cdot \min\{|i_k|, |l_k|\} & \mathsf{sgn}(i_k) = \mathsf{sgn}(l_k) \\ 0 & \text{otherwise.} \end{cases}$$

Then in case $a_k^{\tilde{\rho}_k} \leq_{\mathrm{tup}} a_k^{\rho_k}$ we are done and set $z_k = z_{k-1} \circ w_1$ and $s_k = \tilde{s}_k$. Else we can similarly proceed for the polynomials $p * v$ and $p * z_{k-1} * w_1$ with head terms $a_1^{j_1} \ldots a_n^{j_n}$ respectively $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{\tilde{s}_k} \tilde{r}$ and find an element $w_2 \in \mathcal{G}$ such that for $z_k = z_{k-1} \circ w_1 \circ w_2$ we have $\mathsf{HT}(p * z_k) = t \circ z_k \equiv a_1^{s_1} \ldots a_k^{s_k} r_k$, $r_k \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{s_k} \leq_{\mathrm{tup}} a_k^{\tilde{\rho}'_k}$ with

$$\tilde{\rho}'_k = \begin{cases} \mathsf{sgn}(j_k) \cdot \min\{|j_k|, |\tilde{s}_k|\} & \mathsf{sgn}(j_k) = \mathsf{sgn}(\tilde{s}_k) \\ 0 & \text{otherwise.} \end{cases}$$

Then we can conclude $a_k^{s_k} \leq_{\mathrm{tup}} a_k^{\rho_k}$ as in case $s_k = 0$ we are immediately done and otherwise we get $\mathsf{sgn}(j_k) = \mathsf{sgn}(\tilde{s}_k) = \mathsf{sgn}(\tilde{\rho}_k) = \mathsf{sgn}(i_k)$ and $\min\{|i_k|, |\tilde{s}_k|, |j_k|\} \leq$

$\min\{|i_k|, |j_k|\}$.

Let us hence show how to construct w_1. Remember that $\mathsf{HT}(p * u) = t \circ u \equiv a_1^{i_1} \dots a_n^{i_n}$ and $\mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ for some $r' \in \mathsf{ORD}(\Sigma_{k+1})$. In case $i_k = l_k$ or $l_k = 0$ we can set $w_1 = \lambda$ and $\tilde{s}_k = l_k = \tilde{\rho}_k$ as $\mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$. Hence let $i_k \neq l_k$ and $l_k \neq 0$.

First let us assume that $\mathsf{sgn}(i_k) = \mathsf{sgn}(l_k)$. Then in case $|i_k| \geq |l_k|$ we are done by setting $w_1 = \lambda$ as again $\mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ will do with $\tilde{s}_k = l_k = \tilde{\rho}_k$. Therefore, let us assume that $|l_k| > |i_k|$. Then we consider the multiple $p * z_{k-1} * a_k^{-l_k+i_k}$, i.e., the exponent of the letter a_k in the term $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ will be i_k. If $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k}) = t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ we are done because then $t \circ z_{k-1} \circ a_k^{-l_k+i_k} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} \tilde{r}_k$ for some $\tilde{r}_k \in \mathsf{ORD}(\Sigma_{k+1})$ and we can set $w_1 = a_k^{-l_k+i_k}$ and $\tilde{s}_k = i_k = \tilde{\rho}_k$. Otherwise we show that the t-term $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ in this multiple can be brought to head position using an element $r \in \mathsf{ORD}(\Sigma_{k+1})$ thus allowing to set $\tilde{s}_k = i_k = \tilde{\rho}_k$ and $w_1 = a_k^{-l_k+i_k} r$ as then we have $\mathsf{HT}(p * z_{k-1} * w_1) = t \circ z_{k-1} \circ w_1 = a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r' \circ a_k^{-l_k+i_k} r \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} \tilde{r}$ where $a_k^{l_k} r' \circ a_k^{-l_k+i_k} r \equiv a_k^{i_k} \tilde{r}$[11]. This follows immediately if we can prove that the exponent of a_k in the term $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k})$ is also i_k. Then we can apply lemma 4 to the polynomial $p * z_{k-1} * a_k^{-l_k+i_k}$ and the term $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$. Note that $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k})$ and $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ have then distinguishing letter of at least index $k+1$ and further $\mathsf{HT}((p * z_{k-1} * a_k^{-l_k+i_k}) * a_k^{-l_k+i_k}) = \mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1}$. Therefore, we show that the exponent of a_k in the term $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k})$ is also i_k. Let $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{b_k} r''$ with $r'' \in \mathsf{ORD}(\Sigma_{k+1})$ be the term in $p * z_{k-1}$ that became head term[12], i.e., $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{b_k} r'' \circ a_k^{-l_k+i_k} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{c_k} x \succ a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} y \equiv t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ for some $x, y \in \mathsf{ORD}(\Sigma_{k+1})$ and therefore $c_k \geq_{\mathbf{Z}} i_k$. Then by lemma 1 there exist $z_1 \in \mathsf{ORD}(\Sigma \backslash \Sigma_{k-1})$ and $z_2 \in \mathsf{ORD}(\Sigma_k)$ such that $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} y \circ z_1 \equiv a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{i_k+f_k} z$ for some $z \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{i_k+f_k} z \circ z_2 \equiv a_k^{i_k} a_{k+1}^{i_{k+1}} \dots a_n^{i_n}$, i.e., $z_2 \equiv a_k^{-f_k} z_2'$ for some $z_2' \in \mathsf{ORD}(\Sigma_{k+1})$. Note that the t-term is brought to head position by this multiplication. Now multiplying $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k})$ by $z_1 z_2$ we find $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{c_k} x \circ z_1 z_2 \equiv a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{c_k+f_k-f_k} \tilde{x}$ for some $\tilde{x} \in \mathsf{ORD}(\Sigma_{k+1})$. This gives us $c_k \leq_{\mathbf{Z}} i_k$ and thus $i_k \leq_{\mathbf{Z}} c_k$ yields $c_k = i_k$.

Finally, we have to check the case that $\mathsf{sgn}(i_k) \neq \mathsf{sgn}(l_k)$ and $l_k \neq 0$. Let us take a look at the polynomial $p * z_{k-1} * a_k^{-l_k}$, i.e., the exponent of the letter a_k in the term $t \circ z_{k-1} \circ a_k^{-l_k}$ will be 0. Suppose $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k}) \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{c_k} x$, for some term $s \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{b_s} x_s \in \mathsf{T}(p * z_{k-1})$, $x, x_s \in \mathsf{ORD}(\Sigma_{k+1})$, i.e., $c_k = b_s - l_k$. In case this head term is already the corresponding t-term $t \circ z_{k-1} \circ a_k^{-l_k}$, we are done and we set $w_1 = a_k^{-l_k}$ and $\tilde{s}_k = 0 = \tilde{\rho}_k$. Now if we can show $c_k = 0$, by lemma 4 the t-term $t \circ z_{k-1} \circ a_k^{-l_k}$ can be brought to head position using an element in $\mathsf{ORD}(\Sigma_{k+1})$ since the distinguishing letter between $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k})$ and the term $t \circ z_{k-1} \circ a_k^{-l_k}$ then has at least index $k+1$ and we know $\mathsf{HT}((p * z_{k-1} * a_k^{-l_k}) * a_k^{l_k}) = \mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1}$. Hence,

[11] Note that the product of two elements in $\mathsf{ORD}(\Sigma_i)$ is again an element in $\mathsf{ORD}(\Sigma_i)$.

[12] Note that a candidate in $\mathsf{T}(p * z_{k-1})$ for the head term in $p * z_{k-1} * a_k^{-l_k+i_k}$ must have prefix $a_1^{s_1} \dots a_{k-1}^{s_{k-1}}$ since $\mathsf{HT}(p * z_{k-1}) \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} r_{k-1}$ and multiplication with $a_k^{-l_k+i_k}$ only involves r_{k-1}.

in showing that $c_k = 0$ we are done. As before there exist $z_1 \in \mathsf{ORD}(\Sigma \backslash \Sigma_{k-1})$ and $z_2 \in \mathsf{ORD}(\Sigma_k)$ such that $t \circ z_{k-1} \circ a_k^{-l_k} \circ z_1 \equiv a_1^{i_1} \ldots a_{k-1}^{i_{k-1}} a_k^{f_k} z$ for some $z \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{f_k} z \circ z_2 \equiv a_k^{i_k} \ldots a_n^{i_n}$, i.e., $z_2 \equiv a_k^{-f_k+i_k} z_2'$ for some $z_2' \in \mathsf{ORD}(\Sigma_{k+1})$. Remember that this multiplication brings the t-term to head position. Hence multiplying $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k})$ by $z_1 z_2$ we find $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{c_k} x \circ z_1 z_2 \equiv a_1^{i_1} \ldots a_{k-1}^{i_{k-1}} a_k^{c_k+i_k} \tilde{x}$ for some $\tilde{x} \in \mathsf{ORD}(\Sigma_{k+1})$. Thus we know $c_k + i_k \leq_{\mathbf{Z}} i_k$. To see that this implies $c_k = 0$ we have to distinguish three cases. Remember that $c_k = b_s - l_k$ and since our head term is an s-term $s \circ a_k^{-l_k}$ for some $s \in \mathsf{T}(p * z_{k-1})$ we know $b_s \leq_{\mathbf{Z}} l_k$. In case $i_k = 0$, we have $c_k \leq_{\mathbf{Z}} 0$ implying $c_k = 0$. In case $i_k > 0$ then $c_k + i_k = b_s - l_k + i_k \leq_{\mathbf{Z}} i_k$ implies $0 \leq b_s - l_k + i_k \leq i_k$. Furthermore, as $l_k < 0$ we have $-l_k + i_k > i_k$ implying $b_s < 0$ and hence $|b_s| \leq |l_k|$. But then $b_s - l_k \geq 0$ and $0 \leq b_s - l_k + i_k \leq i_k$ yields $c_k = b_s - l_k = 0$. On the other hand, $i_k < 0$ and $l_k > 0$ imply $0 \leq b_s \leq l_k$ and hence $b_s - l_k + i_k < 0$ yielding $|b_s - l_k + i_k| \leq |i_k|$. Since $b_s - l_k \leq 0$ this inequation can only hold in case $c_k = b_s - l_k = 0$. □

These two lemmata now state that given a polynomial, we can construct additional polynomials, which are in fact $\mathcal{N}$-right-multiples of the original polynomial, such that every $\mathcal{N}$-right-multiple of the polynomial is qc-reducible to zero in one step by one of them. This property is called $\mathcal{N}$-saturation. In example 2 the multiples $p * a^{-1} = a + \lambda$ and $p * a^{-2} = a^{-1} + \lambda$ give us a $\mathcal{N}$-saturating set for $p = a^2 + a$.

Definition 3 *A set $S \subseteq \{p * w \mid w \in \mathcal{N}\}$ is called an* **$\mathcal{N}$-saturating set** *for a non-zero polynomial p in $\mathbf{K}[\mathcal{G}]$, if for all $w \in \mathcal{N}$, $p * w \longrightarrow_S^{\mathrm{qc}} 0$. A set of polynomials $F \subseteq \mathbf{K}[\mathcal{G}]$ is called* **$\mathcal{N}$-saturated**, *if for all $f \in F$ and for all $w \in \mathcal{N}$, $f * w \longrightarrow_F^{\mathrm{qc}} 0$.* ◇

A further consequence of the previous lemmata is that finite $\mathcal{N}$-saturating sets exist and that they can be computed.

Procedure SATURATION

Given: A non-zero polynomial $p \in \mathbf{K}[\mathcal{G}]$.
Find: SAT(p), an $\mathcal{N}$-saturating set for p.

for all $t \in \mathsf{T}(p)$ **do**
  $S_t := \emptyset$;
  if t can be brought to head position
    then compute $q = p * w$ with $\mathsf{HT}(p * w) = t \circ w$
      $H_t := \{s \in \mathcal{G} \mid \mathsf{HT}(q) \geq_{\mathrm{tup}} s\}$;
      % These are candidates for "smaller" polynomials with t-head terms[13]
      $q := \min\{p * (\mathsf{inv}(t) \circ s) \mid s \in H_t, \mathsf{HT}(p * (\mathsf{inv}(t) \circ s)) = s\}$;
      $S_t := \{q\}$;
  endif
endfor
SAT(p) := $\bigcup_{t \in \mathsf{T}(p)} S_t$ % S contains at most $|\mathsf{T}(p)|$ polynomials

Gröbner bases as defined by Buchberger can now be specified for right ideals in this setting as follows.

Definition 4 *A set $G \subseteq \mathbf{K}[\mathcal{G}]$ is said to be a* **right Gröbner basis**, *if $\overset{*}{\longleftrightarrow}{}^{\mathrm{qc}}_{G} = \equiv_{\mathsf{ideal}_r(G)}$, and for all $g \in \mathsf{ideal}_r(G)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$.*[14] ◇

We can now characterize such bases by so-called s-polynomials corresponding to qc-reduction.

Definition 5 *For $p_1, p_2 \in \mathbf{K}[\mathcal{G}]$ such that $\mathsf{HT}(p_1) \equiv e a_1^{i_1} \ldots a_n^{i_n}$ and $\mathsf{HT}(p_2) \equiv e a_1^{j_1} \ldots a_n^{j_n}$ with either $i_l = 0$ or $j_l = 0$ or $\mathsf{sgn}(i_l) = \mathsf{sgn}(j_l)$ for $1 \leq l \leq n$ we can define an* **s-polynomial**, *and setting*

$$\rho_l = \begin{cases} \mathsf{sgn}(j_l) & i_l = 0 \\ \mathsf{sgn}(i_l) & \textit{otherwise} \end{cases}$$

the situation $e a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}} = \mathsf{HT}(p_1) \circ w_1 = \mathsf{HT}(p_2) \circ w_2$ for some $w_1, w_2 \in \mathcal{N}$ gives us

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

◇

Notice that $\mathsf{HT}(p_i) \leq_{\mathrm{tup}} e a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}}$ for $i \in \{1,2\}$ holds in case such an s-polynomial exists. Furthermore, if there exists a term t such that $t \geq_{\mathrm{tup}} \mathsf{HT}(p_1) \equiv e a_1^{i_1} \ldots a_n^{i_n}$ and $t \geq_{\mathrm{tup}} \mathsf{HT}(p_2) \equiv e a_1^{j_1} \ldots a_n^{j_n}$ an s-polynomial always exists[15] and we even have $t \geq_{\mathrm{tup}} e a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}}$. 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 a right Gröbner basis in a familiar way after transforming a generating set for the right ideal using these mappings.

Theorem 1 *Let $F, G \subseteq \mathbf{K}[\mathcal{G}]$ such that*

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

(ii) $\{\psi_e(f) | f \in F, e \in \mathcal{E}\} \subseteq G$

(iii) *G is $\mathcal{N}$- saturated.*

Then the following statements are equivalent:

[13] More structural information can be used to rule out unnecessary candidates from the set H_t to make this procedure more efficient.

[14] Notice that on first sight this is the definition of a weak Gröbner basis. Since the translation lemma holds for qc-reduction it also defines a strong Gröbner basis.

[15] Notice that the condition for the existence of an s-polynomial is fulfilled as the tupel-ordering requires that the exponent of a letter a_i in the smaller term is either zero or has the same sign as the exponent of a_i in the tupel-larger term.

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

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

Proof :
$1 \Longrightarrow 2$: By definition 5 in case for $f_k, f_l \in G$ the s-polynomial exists we get

$$\mathsf{spol}(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k * w_1 - \mathsf{HC}(f_l)^{-1} f_l * w_2 \ \in \mathsf{ideal}_r(G) = \mathsf{ideal}_r(F),$$

and then $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\mathrm{qc}}_{G} 0$.

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}_r(F)$ is $\longrightarrow^{\mathrm{qc}}_{G}$-reducible to zero. Without loss of generality we assume that G contains no constant polynomials, as then we are done at once. Remember that for $h \in \mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$, $h \longrightarrow^{\mathrm{qc}}_{G} h'$ implies $h' \in \mathsf{ideal}_r(G) = \mathsf{ideal}_r(F)$. Thus as $\longrightarrow^{\mathrm{qc}}_{G}$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}_r(F) \backslash \{0\}$ is $\longrightarrow^{\mathrm{qc}}_{G}$-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 $e_j \in \mathcal{E}$, $u_j \in \mathcal{N}$. 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 $\mathcal{N}$-saturated and $\psi_{e_j}(f_j) \in G$ by definition 3 there exists $g_j \in G$ such that $\psi_{e_j}(f_j) * u_j \longrightarrow^{\mathrm{qc}}_{g_j} 0$ and hence we can assume $g = \sum_{j=1}^{m} \alpha_j \cdot g_j * v_j$, where $\alpha_j \in \mathbf{K}^*, g_j \in G, v_j \in \mathcal{N}$ and $\mathsf{HT}(g_j * v_j) = \mathsf{HT}(g_j) \circ v_j \geq_{\mathrm{tup}} \mathsf{HT}(g_j)$. Depending on this representation of g and our well-founded total ordering on $\mathcal{G}$ we define $t = \max\{\mathsf{HT}(g_j) \circ v_j \mid j \in \{1, \ldots m\}\}$ 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 $\longrightarrow^{\mathrm{qc}}_{G}$-reducible. Otherwise we show that g has a special representation (a standard representation corresponding to qc-reduction) where all terms are bounded by $\mathsf{HT}(g)$, as this implies that g is top-reducible using G. 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 $K' < K$)[16]. In case $t \succ \mathsf{HT}(g)$ there are two polynomials g_k, g_l in the corresponding representation[17] such that $t = \mathsf{HT}(g_k) \circ v_k = \mathsf{HT}(g_l) \circ v_l$ and we have $t \geq_{\mathrm{tup}} \mathsf{HT}(g_k)$,$t \geq_{\mathrm{tup}} \mathsf{HT}(g_l)$. Hence by definition 5 there exists an s-polynomial $\mathsf{spol}(g_k, g_l) = \mathsf{HC}(g_k)^{-1} \cdot g_k * z_1 - \mathsf{HC}(g_l)^{-1} \cdot g_l * z_2$ and $\mathsf{HT}(g_k) \circ v_k = \mathsf{HT}(g_l) \circ v_l = \mathsf{HT}(g_k) \circ z_1 \circ w = \mathsf{HT}(g_l) \circ z_2 \circ w \geq_{\mathrm{tup}} \mathsf{HT}(g_k) \circ z_1 = \mathsf{HT}(g_l) \circ z_2$ for some $z_1, z_2, w \in \mathcal{N}$. Let us assume $\mathsf{spol}(g_k, g_l) \neq 0$[18]. Hence, $\mathsf{spol}(g_k, g_l) \xrightarrow{*}{}^{\mathrm{qc}}_{G} 0$ implies $\mathsf{spol}(g_k, g_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v'_i, \delta_i \in \mathbf{K}^*, h_i \in G, v'_i \in \mathcal{N}$[19], where the h_i are due to the qc-reduction of the s-polynomial and all terms occurring in the sum are bounded by $\mathsf{HT}(\mathsf{spol}(g_k, g_l))$. By lemma 2, since $t = \mathsf{HT}(g_k) \circ z_1 \circ w \geq_{\mathrm{tup}} \mathsf{HT}(g_k) \circ z_1$ and $\mathsf{HT}(g_k) \circ z_1 \succ \mathsf{HT}(\mathsf{spol}(g_k, g_l))$, we can conclude that t is a proper bound for all terms

[16] Note that this ordering is well-founded since $\geq_{\mathrm{syll}}$ is and $K \in \mathbf{N}$.

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

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

[19] Note that the case $v'_i \in \mathcal{E}$ cannot occur as it implies that h_i is a constant polynomial and we assumed that G does not contain constant polynomials.

occurring in the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i' * w$. Since $w \in \mathcal{N}$ and G is $\mathcal{N}$-saturated, without loss of generality we can assume that the representation has the the required form. We now have:

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

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 (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. □

On first sight this characterization 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 commutative 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 as a set of $\mathcal{N}$-right-multiples since $\mathsf{ideal}_r(F) = \{\sum_{i=1}^{k} \alpha_i \cdot f_i * u_i \mid \alpha_i \in \mathbf{K}, f_i \in F_{\mathcal{E}}, u_i \in \mathcal{N}\}$. If we additionally incorporate the concept of $\mathcal{N}$-saturation, qc-reduction can be used to express the right ideal congruence and then a right Gröbner basis can be characterized as usual by s-polynomials. Now, using the characterization given in theorem 1 we can state a procedure which enumerates right Gröbner bases in nilpotent group rings:

Procedure RIGHT GRÖBNER BASES IN NILPOTENT GROUP RINGS

Given: $F \subseteq \mathbf{K}[\mathcal{G}]$ and a presentation of $\mathcal{G}$ by $\mathcal{E}$ and $\mathcal{N}$ as specified above
Find: $\mathrm{GB}_r(F)$, a right Gröbner basis of $\mathsf{ideal}_r(F)$.

$G := \{\psi_e(f) \mid f \in F, e \in \mathcal{E}\}$; % G contains $F_{\mathcal{E}}$
$G := \bigcup_{g \in G} \mathrm{SAT}(g)$; % G is $\mathcal{N}$-saturated and $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ **do** % Test if statement 2 of theorem 1 is valid
  $(q_1, q_2) :=$ remove(B); % Remove an element using a fair strategy
  if $h := \mathsf{spol}(q_1, q_2)$ exists

then $h' :=$ normalform$(h, \longrightarrow_G^{\mathrm{qc}})$; % Compute a normal form
if $h' \neq 0$ % The s-polynomial does not reduce to zero
then $G := G \cup \{g \mid g \in \mathrm{SAT}(h')\}$;
% G is $\mathcal{N}$-saturated and $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$
$B := B \cup \{(f, g) \mid f \in G, g \in \mathrm{SAT}(h')\}$;
endif
endif
endwhile
$\mathrm{GB}_r(F) := G$

The set G enumerated by this procedure fulfills the requirements of theorem 1, i.e., we have $F_{\mathcal{E}} \subseteq G$ and the set G at each stage generates the right ideal $\mathsf{ideal}_r(F)$ and is $\mathcal{N}$-saturated. Using a fair strategy to remove elements from the test set B ensures that for all polynomials entered into G the s-polynomial is considered in case it exists. Hence, in case the procedure terminates, it computes a right Gröbner basis. Later on we will see that every right Gröbner basis contains a finite one and hence this procedure must terminate. Let us first continue to show how similar to the case of solvable polynomial rings or skew polynomial rings ([Kr93, We92]), Gröbner bases of two-sided ideals can be characterized by right 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 2 *For a set of polynomials $G \subseteq \mathbf{K}[\mathcal{G}]$, assuming that $\mathcal{G}$ is presented by (Γ, T) as described above, the following properties are equivalent:*

1. *G is a right Gröbner basis and $\mathsf{ideal}_r(G) = \mathsf{ideal}(G)$.*
2. *For all $g \in \mathsf{ideal}(G)$ we have $g \xrightarrow{*}{}_G^{\mathrm{qc}} 0$.*
3. *G is a right Gröbner basis and for all $w \in \mathcal{G}$, $g \in G$ we have $w * g \in \mathsf{ideal}_r(G)$.*
4. *G is a right Gröbner basis and for all $a \in \Gamma$, $g \in G$ we have $a * g \in \mathsf{ideal}_r(G)$.*

Proof :
$1 \Longrightarrow 2$: 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 right Gröbner basis we have to prove $\xleftrightarrow{*}{}_G^{\mathrm{qc}} = \equiv_{\mathsf{ideal}_r(G)}$ and for all $g \in \mathsf{ideal}_r(G)$, $g \xrightarrow{*}{}_G^{\mathrm{qc}} 0$. 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 $g \xrightarrow{*}{}_G^{\mathrm{qc}} 0$. The inclusion $\xleftrightarrow{*}{}_G^{\mathrm{qc}} \subseteq \equiv_{\mathsf{ideal}_r(G)}$ is obvious. Hence let $f \equiv_{\mathsf{ideal}_r(G)} g$, i.e., $f - g \in \mathsf{ideal}_r(G)$. But then we have $f - g \xrightarrow{*}{}_G^{\mathrm{qc}} 0$ and hence by lemma 3 there exists a polynomial $h \in \mathbf{K}[\mathcal{G}]$ such that $f \xrightarrow{*}{}_G^{\mathrm{qc}} h$ and $g \xrightarrow{*}{}_G^{\mathrm{qc}} h$, yielding $f \xleftrightarrow{*}{}_G^{\mathrm{qc}} g$. Finally, $w * f \in \mathsf{ideal}(G)$ and $w * f \xrightarrow{*}{}_G^{\mathrm{qc}} 0$ 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 $u_i, w_i \in \mathcal{G}$. We will show by induction on $|u_i|$ that for $u_i \in \mathcal{G}$, $g_i \in G$, $u_i * g_i \in \mathsf{ideal}_r(G)$ 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 $a \in \Gamma$ and by our assumption we know $a * g_i \in \mathsf{ideal}_r(G)$. Let $a * g_i = \sum_{j=1}^{m} \beta_j \cdot g'_j * v_j$ for some $\beta_j \in \mathbf{K}$, $g'_j \in G$ and $v_j \in \mathcal{G}$. 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 $u_i * g_i \in \mathsf{ideal}_r(G)$. □

Statement 4 enables a constructive approach to use procedure RIGHT GRÖBNER BASES IN NILPOTENT GROUP RINGS in order to compute Gröbner bases of two-sided ideals and item 2 states that such bases can be used to decide the membership problem for the two-sided ideal by using qc-reduction. The following corollary of the previous two theorems will be the foundation of a procedure to compute two-sided Gröbner bases.

Corollary 1 *Let $F, G \subseteq \mathbf{K}[\mathcal{G}]$ such that*

(i) $\mathsf{ideal}(F) = \mathsf{ideal}(G)$

(ii) $\{\psi_e(f) | f \in F, e \in \mathcal{E}\} \subseteq G$

(iii) *G is $\mathcal{N}$- saturated.*

Then the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}(F)$ we have $g \xrightarrow{*}{}^{\mathrm{qc}}_{G} 0$.*
2. *(a) For all polynomials $f_k, f_l \in G$ we have $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\mathrm{qc}}_{G} 0$.*
   (b) For all $a \in \Gamma$, $g \in G$ we have $a * g \xrightarrow{*}{}^{\mathrm{qc}}_{G} 0$.

Proof :
$1 \Longrightarrow 2$: By definition 5 we find that in case for $f_k, f_l \in G$ an s-polynomial exists,

$$\mathsf{spol}(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k * w_1 - \mathsf{HC}(f_l)^{-1} f_l * w_2 \ \in \mathsf{ideal}(G) = \mathsf{ideal}(F),$$

and then $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\mathrm{qc}}_{G} 0$. Similarly, since $g \in G$ implies $a * g \in \mathsf{ideal}(G) = \mathsf{ideal}(F)$ for all $a \in \Gamma$, we have $a * g \xrightarrow{*}{}^{\mathrm{qc}}_{G} 0$.

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}(F)$ is $\xrightarrow{}{}^{\mathrm{qc}}_{G}$-reducible to zero. Without loss of generality we assume that G contains no constant polynomials, as then we are done at once. Let $g = \sum_{j=1}^{m} \alpha_j \cdot u_j * f_j * w_j$ be a representation of such a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*$, $f_j \in F, u_j, w_j \in \mathcal{G}$ and suppose for $1 \leq j \leq m$ we have $w_j \equiv e_j v_j$ with $e_j \in \mathcal{E}$ and $v_j \in \mathcal{N}$. Then we can modify this representation to

$g = \sum_{j=1}^{m} \alpha_j \cdot u_j * \psi_{e_j}(f_j) * v_j$ as $\psi_{e_j}(f_j) \in G$ by our assumption. Next we will show that every multiple $u_j * \psi_{e_j}(f_j)$ has a representation $u_j * \psi_{e_j}(f_j) = \sum_{i=1}^{m_j} \beta_i \cdot g_i * v_i'$ with $\beta_i \in \mathbf{K}^*$, $g_i \in G$ and $v_i' \in \mathcal{N}$. More general, we will show that this is true for every multiple $u * g$, $u \in \mathcal{G}$, $g \in G$. As in the previous theorem this will be done by induction on $|u|$. The case $|u| = 0$ is obvious. Hence let $u \equiv u'a$ for some $a \in \Gamma$. By our assumption we know $a * g \xrightarrow{*}{}^{\mathrm{qc}}_{G} 0$ and as we assume that G does not contain constant polynomials, this reduction sequence results in a representation $a * g = \sum_{i=1}^{k} \gamma_i \cdot g_i' * v_i''$ with $\gamma_i \in \mathbf{K}^*$, $g_i' \in G$ and $v_i'' \in \mathcal{N}$. Hence, $u * g = u' * (a * g) = u' * (\sum_{i=1}^{k} \gamma_i \cdot g_i' * v_i'') = \sum_{i=1}^{k} \gamma_i \cdot (u' * g_i') * v_i''$ and now our induction hypothesis can be applied to each multiple $u' * g_i'$, and since products of elements in $\mathcal{N}$ are again in $\mathcal{N}$, we are done. Therefore, we find that g has a representation $g = \sum_{j=1}^{n} \alpha_j' \cdot f_j' * w_j'$ where $\alpha_j' \in \mathbf{K}^*, f_j' \in G, w_j' \in \mathcal{N}$ and now we can proceed as in theorem 1 to prove our claim. □

Procedure GRÖBNER BASES IN NILPOTENT GROUP RINGS

Given: $F \subseteq \mathbf{K}[\mathcal{G}]$ and a presentation (Γ, T) of $\mathcal{G}$ by $\mathcal{E}$ and $\mathcal{N}$ as specified above.
Find: $\mathrm{GB}(F)$, a Gröbner basis of $\mathsf{ideal}(F)$.

$G := \{\psi_e(f) \mid f \in F, e \in \mathcal{E}\}$; % G contains $F_{\mathcal{E}}$ and $\mathsf{ideal}(F) = \mathsf{ideal}(G)$
$G := \bigcup_{g \in G} \mathrm{SAT}(g)$; % G is $\mathcal{N}$-saturated
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
$M := \{a * f \mid f \in G, a \in \Gamma\}$;
while $M \neq \emptyset$ or $B \neq \emptyset$ **do**
  if $M \neq \emptyset$
    then $h :=$ remove(M); % Remove an element using a fair strategy
      $h' :=$ normalform$(h, \longrightarrow^{\mathrm{qc}}_{G})$;
      if $h' \neq 0$
        then $G := G \cup \mathrm{SAT}(h')$;
          % G is $\mathcal{N}$-saturated and $\mathsf{ideal}(F) = \mathsf{ideal}(G)$
          $B := B \cup \{(f, g) \mid f \in G, g \in \mathrm{SAT}(h')\}$;
          $M := \{a * g \mid a \in \Gamma, g \in \mathrm{SAT}(h')\}$;
      endif
  endif
  if $B \neq \emptyset$
    then $(q_1, q_2) :=$ remove(B); % Remove an element using a fair strategy
      if $h := \mathsf{spol}(q_1, q_2)$ exists
        then $h' :=$ normalform$(h, \longrightarrow^{\mathrm{qc}}_{G})$;
          if $h' \neq 0$ % The s-polynomial does not reduce to zero
            then $G := G \cup \mathrm{SAT}(h')$;
              % G is $\mathcal{N}$-saturated and $\mathsf{ideal}(F) = \mathsf{ideal}(G)$
              $B := B \cup \{(f, g) \mid f \in G, g \in \mathrm{SAT}(h')\}$;
              $M := \{a * g \mid a \in \Gamma, g \in \mathrm{SAT}(h')\}$;
          endif
      endif

endif
endwhile
$\text{GB}(F) := G$

Correctness of this procedure follows from corollary 1. For the set G enumerated by this procedure we have $F_{\mathcal{E}} \subseteq G$ and the set G at each stage generates the ideal $\mathsf{ideal}(F)$ and is $\mathcal{N}$-saturated. Using a fair strategy to remove elements from the test sets B and M ensures that for all polynomials entered into G the existing s-polynomials and the critical left multiples are considered. To show termination we need the following theorem which makes use of Dickson's lemma due to the special representatives of the group elements.

Theorem 3 *Every (right) Gröbner basis contains a finite one.*

Proof : Let F be a subset of $\mathbf{K}[\mathcal{G}]$ and G a Gröbner basis[20] of $\mathsf{ideal}(F)$, i.e., $\mathsf{ideal}(F) = \mathsf{ideal}(G) = \mathsf{ideal}_r(G)$ and for all $g \in \mathsf{ideal}(F)$ we have $g \xrightarrow[G]{*}{}^{\text{qc}} 0$. We can assume that G is infinite as otherwise we are done. Further let $H = \{\mathsf{HT}(g) \mid g \in G\} \subseteq \mathcal{G}$. Then for every polynomial $f \in \mathsf{ideal}(F)$ there exists a term $t \in H$ such that $\mathsf{HT}(f) \geq_{\text{tup}} t$. H can be decomposed into $H = \bigcup_{e \in \mathcal{E}} H_e$ where H_e contains those terms in H starting with e. For each element of $eu \in H_e$ the element u then can be viewed as an n-tuple over $\mathbf{Z}$ as it is presented by an ordered group word. But we can also view it as a 2n-tuple over $\mathbf{N}$ by representing each element $u \in \mathcal{N}$ by an extended ordered group word $u \equiv a_1^{-i_1} a_1^{j_1} \ldots a_n^{-i_n} a_n^{j_n}$, where $i_l, j_l \in \mathbf{N}$ and the representing 2n-tuple is $(i_1, j_1, \ldots, i_n, j_n)$. Notice that at most one of the two exponents i_l and j_l is non-zero. Now only considering the ordered group word parts of the terms, each set H_e can be seen as a (possibly infinite) subset of a free commutative monoid $\mathcal{T}_{2n}$ with $2 \cdot n$ generators. Thus by Dickson's lemma there exists a finite subset B_e of H_e such that for every $w \in H_e$ there is a $b \in B_e$ with $w \geq_{\text{tup}} b$. Now we can use the sets B_e to distinguish a finite Gröbner basis in G as follows. To each term $t \in B_e$ we can assign a polynomial $g_t \in G$ such that $\mathsf{HT}(g_t) = t$. Then the set $G_B = \{g_t \mid t \in B_e, e \in \mathcal{E}\}$ is again a Gröbner basis since for every polynomial $f \in \mathsf{ideal}(F)$ there still exists a polynomial g_t now in G_B such that $\mathsf{HT}(f) \geq_{\text{tup}} \mathsf{HT}(g_t) = t$. Hence all polynomials in $\mathsf{ideal}(F)$ are qc-reducible to zero using G_B. □

Since both procedures enumerate respective Gröbner bases and the sets enumerated contain finite Gröbner bases, the procedures terminate as soon as all polynomials of the contained bases are entered into G. Therefore we now are able to solve problems related to right and two-sided ideals in nilpotent group rings using reduction similar to Buchberger's approach to commutative polynomial rings.

[20] The proof for the existence of a finite right Gröbner basis for $\mathsf{ideal}_r(F)$ is similar.

4 Concluding Remarks

One problem of this approach is that computing the $\mathcal{E}$-closure of a set involves $|\mathcal{E}|$ multiplications in case $\mathcal{E}$ is presented by its multiplication table. Many finite groups allow more compact convergent presentations. We close this paper by sketching how information on such a presentation can be used. Let (Δ, R) be a convergent presentation of $\mathcal{E}$ and $(\Sigma, T_{NC} \cup T_I)$ a presentation of $\mathcal{N}$ as described before. Then assuming $\Delta \cap \Sigma = \emptyset$, we get a convergent presentation of $\mathcal{G}$ by setting $\Gamma = \Delta \cup \Sigma$ and T besides the rules in T_I and T_{NC} includes the following additional rules

$$\begin{array}{lll} u & \longrightarrow vw & \text{for all } (u,v) \in R,\ w \in \mathsf{ORD}(\Sigma),\ [u]_{\mathcal{G}} \equiv vw, \\ ae & \longrightarrow e\phi_e(a) & \text{for all } e \in \Delta, a \in \Sigma. \end{array}$$

Now we can refine the definition of the tuple ordering to allow further multiplications for reduction which are compatible on the representative of the $\mathcal{E}$ part of the group element. Further, information on the representatives and the rules can be used to reduce the number of the polynomials needed. For example if we assume that $\mathcal{E}$ is presented by a convergent $PCNI$-presentation $\Delta = \{b_1, b_1^{-1}, \ldots b_m, b_m^{-1}\}$, $R = \{b_i^{s_i} \longrightarrow w_i, b_i^{-1} \longrightarrow w_i' \mid w_i \in \mathsf{ORD}(\Sigma \backslash \Sigma_i), w_i' \in \mathsf{ORD}(\Sigma \backslash \Sigma_{i-1}), s_i \in \mathbf{N}\} \cup R_{NC}$ (compare [Wi89]), then we can combine prefix and quasi-comutative reduction to improve the results given here.

Notice that we require a presentation of a finitely generated nilpotent group as an extension of a torsion-free nilpotent group by a finite group. A related question is, how we can compute such a presentation when given an arbitray presentation of a nilpotent group.

The approach given in this paper describes and computes Gröbner bases of two-sided ideals using qc-reduction. Another way to describe them is in terms of two-sided reduction, but then one again has to find suitable restrictions on the multiples allowed for reduction in order to keep the number of s-polynomials small.

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 special axioms, e.g., allowing to compute finite Gröbner bases for ideals in the coefficient domain. Hence the results of this paper also hold for nilpotent group rings over reduction rings, e.g., the integers $\mathbf{Z}$.

References

[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.

[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.* Dissertation. Universität Innsbruck. 1965.

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

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

[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.

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

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

[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.

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

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

[Re95] B. Reinert. *Gröbner Bases in Monoid and Group Rings* PhD Thesis. Universität Kaiserslautern. (to appear spring 1995)

[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.

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

[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.

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