A Completion Procedure for Computing a Canonical Basis for a k-Subalgebra*

Deepak Kapur
Department of Computer Science
State University of New York at Albany
Albany, NY 12222
kapur@albanycs.albany.edu

Klaus Madlener
Fachbereich Informatik
Universität Kaiserslautern
D-6750, Kaiserslautern, W. Germany

Abstract

A completion procedure for computing a canonical basis for a k-subalgebra is proposed. Using this canonical basis, the membership problem for a k-subalgebra can be solved. The approach follows Buchberger's approach for computing a Gröbner basis for a polynomial ideal and is based on rewriting concepts. A canonical basis produced by the completion procedure shares many properties of a Gröbner basis such as reducing an element of a k-subalgebra to 0 and generating unique normal forms for the equivalence classes generated by a k-subalgebra. In contrast to Shannon and Sweedler's approach using tag variables, this approach is direct. One of the limitations of the approach however is that the procedure may not terminate for some term orderings thus giving an infinite canonical basis. The procedure is illustrated using examples.

1 Introduction

A procedure and related theory for computing a canonical basis for a finitely presented k-subalgebra are presented. With a slight modification, the procedure can also be used for the membership problem of a unitary subring generated by a finite basis using a Gröbner basis like approach.

The procedure is based on the rewriting approach following Buchberger [1965, 1976, 1985] and Knuth and Bendix [1970]. The structure of the procedure is the same as that of Buchberger's

*A condensed and preliminary version of this paper appeared in the Proceedings of *Computers and Mathematics, 1989* Conference, held in June 1989 at MIT.

algorithm for computing a Gröbner basis of a polynomial ideal. The definitions of reduction and critical pairs (also called S-polynomials) are different; they can be considered as a generalization of these concepts in Buchberger's algorithm. This approach for solving the membership problem for a k-subalgebra is quite different from the approach taken by Shannon and Sweedler [1987, 1988] in which *tag variables* are used to transform the subalgebra membership problem to the ideal membership problem. The proposed approach is direct, more in the spirit of the recent work of Robbiano and Sweedler [1988]. However, it is based on rewriting concepts and employs completion using critical pairs.

The proposed approach has a disadvantage however over the indirect approach of Shannon and Sweedler in the sense that for some orderings on indeterminates and terms, the completion procedure may not terminate and thus generate an infinite canonical basis. This raises an interesting open question: Given a finitely presented k-subalgebra, does there exist an ordering on terms for which the completion procedure will terminate? If so, how can such an ordering be computed?

In the next section, definitions are given. Section 3 discusses how rules are made from polynomials, and a reduction relation is defined using a set of rules corresponding to a k-subalgebra basis. Properties of this reduction relation are stated and it is shown that the reduction relation is strong enough so that its reflexive, symmetric and transitive closure is precisely the equivalence relation induced by the associated k-subalgebra. A canonical basis of a k-subalgebra is defined. Section 4 defines superpositions, critical pairs and S-polynomials which lead to a finite test for checking whether a given finite basis of a k-subalgebra is a canonical basis. Section 5 is the main result which shows that if all S-polynomials corresponding to critical pairs of a set of rules reduce to 0, then the corresponding basis is canonical. Section 6 outlines a completion procedure based on the test of Section 5, and properties of canonical bases generated by a completion procedure are discussed. A finite canonical basis always exists for a k-subalgebra over $k[x]$. A number of examples taken from papers by Shannon and Sweedler as well as Robbiano and Sweedler are discussed illustrating the procedure. Some comments on how this approach can be modified to be applicable to unitary subrings are given in the final section.

2 k-Subalgebras and Canonical bases

Let $k[x_1, \cdots, x_n]$ be the polymonial ring over a field k with $x_1, \cdots, x_n$ as indeterminates. A unitary subring generated by a finite basis $F = \{f_1, \cdots, f_m\}$, each $f_i \in k[x_1, \cdots, x_n]$, is the smallest subring containing 1 and the elements of F (i.e., if p and q are in the subring, then $p - q$ as well as $p * q$ are in the subring[1]).

A k-subalgebra generated by F is the smallest unitary subring generated by F and containing k (see van der Waerden or Zariski and Samuel for definitions). We also write this k-subalgebra as $k[f_1, \cdots, f_m]$ as well as $k[F]$. It is easy to see that a k-subalgebra $k[f_1, \cdots, f_m]$ defines an equivalence relation on the polynomial ring $k[x_1, \cdots, x_n]$, just like a congruence relation defined by an ideal. Polynomials p and q are equivalent modulo $k[f_1, \cdots, f_m]$ if and only if $p - q \in k[f_1, \cdots, f_m]$.

Our goal is to compute canonical forms for equivalence classes induced by a k-subalgebra

[1]Contrast this definition with that of an ideal which is closed under multiplication with respect to any element of the polynomial ring $k[x_1, \cdots, x_n]$ instead of only the elements of the subring.

$k[f_1, \cdots, f_m]$. We follow the approach proposed by Buchberger [1965, 1985] for computing canonical forms for congruence classes defined by a polynomial ideal. As in Buchberger's approach, with each basis F, we associate a reduction relation $\rightarrow_F$; we will often omit the subscript whenever it is obvious from the context. This reduction relation is associated after first defining a total well-founded ordering on polynomials in $k[x_1, \cdots, x_n]$. Such an ordering can be defined in the same way as is usually done in the case of the Gröbner basis algorithm for polynomial ideals using admissible orderings on terms [Buchberger, 1985].

From a given basis F, the goal is to compute another basis (preferably finite) $G = \{g_1, \cdots, g_r\}$ such that

(i) $k[F] = k[G]$,

(ii) for every element $p \in k[F]$, $p \rightarrow_G^{\star} 0$,

(iii) for every element $q \in k[x_1, \cdots, x_n]$, q has a unique normal form with respect to $\rightarrow_G$, and

(iv) for any p and q, p and q have the same normal form if and only if $p - q \in k[F]$.

Such a G is called a *canonical basis* (or even a *Gröbner basis*) of the k-subalgebra generated by F. The unique normal form of a polynomial p with respect to G is called the *canonical form* of the polynomial p with respect to G. For definitions of various properties of rewriting relations, the reader may consult [Loos and Buchberger]. Below, we assume that polynomials are in the sum of products form and they are simplified (i.e., in a polynomial, there are no terms with zero coefficients, monomials with identical terms are collected together using the operations over the field k).

3 Making Rules from Polynomials

Let $<$ be a total admissible term ordering which extends to a well-founded ordering on polynomials [Buchberger, 1985]. Let $ht(f)$ be the head-term of f with respect to $<$. For each polynomial f, we can define a *rewrite rule* (*simplification rule*) as follows (for making a rule, we can assume without any loss of generality that the head-coefficient of f is 1):

$$ht(f) \rightarrow -(f - ht(f)).$$

Associated with a basis $\{f_1, \cdots, f_m, \cdots\}$ of polynomials is a set $\mathcal{R} = \{L_1 \rightarrow R_1, \cdots, L_m \rightarrow R_m, \cdots\}$ of rules made as above. We will also use $k[\mathcal{R}]$ to stand for the k-subalgebra generated by $\{f_1, \cdots, f_m, \cdots\}$. We define a reduction relation induced by $\mathcal{R}$ on polynomials as follows:

$$p \rightarrow q \qquad \text{if and only if}$$

i. $p = ct + p'$, where ct is a monomial in p ($c \in k$, $c \neq 0$, and t is a term) and p' does not have any monomial whose term is t,

ii. there are $1 \leq j_1 < j_2 < \cdots < j_l$, $l \geq 0$, natural numbers $d_{j_1}, \cdots, d_{j_l}$ such that $t = {L_{j_1}}^{d_{j_1}} {L_{j_2}}^{d_{j_2}} \cdots {L_{j_l}}^{d_{j_l}}$,

iii. the term t' in any monomial bigger than ct in p cannot be expressed as a product of powers of the left sides of a non-empty subset of the rules in $\mathcal{R}$, and

iv. $q = p - c(L_{j_1} - R_{j_1})^{d_{j1}}(L_{j_2} - R_{j_2})^{d_{j2}} \cdots (L_{j_l} - R_{j_l})^{d_{jl}}$.

It is easy to see that $p - q \in k[\mathcal{R}]$.

Unlike in Gröbner basis algorithms for polynomial ideals or in term rewriting systems, a single step reduction can thus simultaneously involve many rules.

The third condition above is strictly not necessary but is motivated by implementation concerns. If this condition is not imposed and a weaker reduction relation is defined using (i), (ii) and (iv), in which any monomial (instead of the largest possible) monomial can be reduced, the results below work also (some proofs may have to be modified though). Using the above definition of a reduction relation, it is possible to consider monomials in descending order for rewriting since any monomial in p once reduced will not reappear in the polynomials obtained by rewriting p.

Even if t satisfies condition (ii) above, we cannot rewrite a proper subterm of t; we must always rewrite the whole term t. This is to so because if $p \rightarrow^{\star} q$, then the polynomial $p - q$ must be in the k-subalgebra $k[\mathcal{R}]$. Also observe that an element of k always reduces to 0 using any basis by taking $d_1 = \cdots = d_m = 0$. Thus $\mathcal{R}$ need not contain rules corresponding to elements of k as well as the right sides of rules need not have elements of k as monomials. It is assumed that all elements in a subalgebra generated by an element of k can be reduced to 0 using an empty set of rewrite rules.

We believe that Robbiano and Sweedler [1988] defined the reduction relation in a similar way except that they consider only the highest term in p instead of any term in p. In their approach, if the highest term cannot be reduced (i.e., cannot be expressed as a product of powers of the left sides of any subset of rules), then the polynomial p cannot be reduced.

Consider the following example from Shannon and Sweedler [1988]. Let

$$F = \{1.\ \ x^3 - x,\ \ 2.\ \ x^2\}$$

be a basis over $Q[x]$. Using the degree ordering, the rules corresponding to the above polynomials are:

$$\mathcal{R} = \{1.\ \ x^3 \rightarrow x,\ \ 2.\ \ x^2 \rightarrow 0\}.$$

Any polynomial which has a term whose degree is a multiple of 3 or a multiple of 2, can be reduced using the rule 1 or rule 2 respectively. A polynomial containing x^5 or x^7 as a term can also be reduced using both the rules 1 and 2. However, a monomial with term x cannot be reduced by $\mathcal{R}$. For example,

$$x^7 - 2x^6 + 3x^5 - 2 \rightarrow -2x^6 + 4x^5 - 2 \rightarrow 4x^5 - 2 \rightarrow 4x^3 - 2 \rightarrow 4x - 2 \rightarrow 4x.$$

The polynomial $4x$ cannot be reduced further.

3.1 Properties of Reduction Relations

Proposition 3.1: The reduction relation $\rightarrow$ defined by a set of rules $\mathcal{R}$ is terminating.

Proof: This follows from the fact that (i) the left side of a rule is the leading term of a polynomial with respect to an admissible ordering $<$ which is well-founded and (ii) the reduction relation always completely reduces a monomial by replacing it by a strictly smaller polynomial. $\Box$

A polynomial p is said to be *irreducible* (or *in normal form*) if and only if there is no q such that $p \rightarrow q$. A polynomial p *has a normal form* q if and only if $p \rightarrow^{\star} q$ and q is in normal form. For example, $4x$ above is a normal form of $x^7 - 2x^6 + 3x^5 - 2$. Thus,

Proposition 3.2: Every $p \in k[x_1, \cdots, x_n]$ has a normal form with respect to the reduction relation $\rightarrow$ defined by a set of rules $\mathcal{R}$.

Proof: Follows from Proposition 3.1. $\Box$

Theorem 3.3: The relation $\leftrightarrow^{\star}$, the reflexive, symmetric and transitive closure of $\rightarrow$, is the k-subalgebra equivalence relation induced by $k[\mathcal{R}]$ associated with $\mathcal{R}$, i.e. for any p and q, $p \leftrightarrow^{\star} q$ if and only if $p - q \in k[\mathcal{R}]$.

The proof of this theorem is very similar to those given in [Buchberger, 1976] for the congruence relation defined by an ideal over a polynomial ring over a field and in [Kandri-Rody and Kapur; 1984] for the congruence relation defined by an ideal over a polynomial ring over a Euclidean domain. The proof is given in the Appendix.

A reduction relation $\rightarrow$ is said to be *canonical* if and only if $\rightarrow$ is terminating and is *confluent*, i.e., for every polynomial p, p has a unique normal form (called the *canonical form* of p) with respect to $\rightarrow$. A basis is called a *canonical basis* if and only if the associated reduction relation $\rightarrow$ is canonical. In the next section, we discuss a finite test for checking whether a finite basis is a canonical basis using the concepts of superpositions, critical pairs and S-polynomials.

4 Superposition, Critical-pair and S-polynomial

We now define the notions of *superposition* and *critical pairs* for rules in $\mathcal{R} = \{L_1 \rightarrow R_1, \cdots, L_m \rightarrow R_m, \cdots\}$. Just as a reduction relation is defined using many rules, the critical pair and S-polynomial are defined, in general, using more than two rules (equivalently, polynomials). This is quite different from the definitions of critical pair and S-polynomial in [Buchberger, 1976; 1985] as well as in [Kandri-Rody and Kapur, 1984], or for that matter in term rewriting systems. These definitions can in fact be considered generalizations of the definitions of M-polynomials given in [Kapur and Narendran, 1985]. Below, we give two different ways to define superpositions and S-polynomials; the first one is intuitively appealing whereas the second one is suitable for computations and proofs.

A finite non-empty subset $\{L_{j_1}, L_{j_2}, \cdots, L_{j_k}\}$ of $\mathcal{R}$ is said to *superpose* (or *overlap*) with another disjoint subset $\{L_{i_1}, L_{i_2}, \cdots, L_{i_l}\}$ of $\mathcal{R}$ (i.e., rule numbers j_j's and i_i's are disjoint) if and only if there is a *minimal* vector of positive natural numbers $< d_{j_1}, d_{j_2}, \cdots, d_{j_k} >$, which are exponents associated with rules $\{L_{j_1}, L_{j_2}, \cdots, L_{j_k}\}$, and another vector of positive numbers $< e_{i_1}, e_{i_2}, \cdots, e_{i_l} >$, exponents associated with rules $\{L_{i_1}, L_{i_2}, \cdots, L_{i_l}\}$, such that

$$L_{j_1}{}^{d_{j_1}} L_{j_2}{}^{d_{j_2}} \cdots L_{j_k}{}^{d_{j_k}} = L_{i_1}{}^{e_{i_1}} L_{i_2}{}^{e_{i_2}} \cdots L_{i_l}{}^{e_{i_l}}.$$

The vector $< d_{j_1}, d_{j_2}, \cdots, d_{j_k} >$ is minimal in the sense that for no vector that is smaller than it, there are positive numbers $< e_{i_1}, e_{i_2}, \cdots, e_{i_l} >$ satisfying the above property about the left sides of the rules ($< c_1, c_2, \cdots, c_k >$ is *smaller* than $< c'_1, c'_2, \cdots, c'_k >$ if and only if they are distinct and each $c_i \leq c'_i, 1 \leq i \leq k$). It is possible to have two non-comparable l vectors $< e_{i_1}, e_{i_2}, \cdots, e_{i_l} >$ and $< e'_{i_1}, e'_{i_2}, \cdots, e'_{i_l} >$ for the same minimal k-vector $< d_{j_1}, d_{j_2}, \cdots, d_{j_k} >$ satisfying the above property about the left sides of the rules. In that case, the rule subset $\{L_{j_1}, L_{j_2}, \cdots, L_{j_k}\}$ is said to superpose in more than one way.

The *critical pair* associated with this superposition is

$$\begin{aligned} &< {L_{j_1}}^{d_{j1}} {L_{j_2}}^{d_{j2}} \cdots {L_{j_k}}^{d_{jk}} - (L_{j_1} - R_{j_1})^{d_{j1}} (L_{j_2} - R_{j_2})^{d_{j2}} \cdots (L_{j_k} - R_{j_k})^{d_{jk}}, \\ &\quad {L_{i_1}}^{e_{i1}} {L_{i_2}}^{e_{i2}} \cdots {L_{i_l}}^{e_{il}} - (L_{i_1} - R_{i_1})^{e_{i1}} (L_{i_2} - R_{i_2})^{e_{i2}} \cdots (L_{i_l} - R_{i_l})^{e_{il}} >. \end{aligned}$$

The *S-polynomial* corresponding to the critical pair is:

$$(L_{j_1} - R_{j_1})^{d_{j1}} (L_{j_2} - R_{j_2})^{d_{j2}} \cdots (L_{j_k} - R_{j_k})^{d_{jk}} - (L_{i_1} - R_{i_1})^{e_{i1}} (L_{i_2} - R_{i_2})^{e_{i2}} \cdots (L_{i_l} - R_{i_l})^{e_{il}}.$$

It is obvious that the S-polynomials of $\mathcal{R}$ belong to $k[\mathcal{R}]$.

The set of critical pairs of a finite set $\mathcal{R}$ of rules is always finite. This follows from the fact that the vectors of exponents $< d_1, \cdots, d_m, e_1, \cdots, e_m >$ satisfying the following equation

$${L_1}^{d_1} {L_2}^{d_2} \cdots {L_m}^{d_m} = {L_1}^{e_1} {L_2}^{e_2} \cdots {L_m}^{e_m}.$$

forms an abelian monoid which has a finite basis [Clifford and Preston].

An alternate way of computing the exponents of the left sides of rules above is to set up a finite set of diophantine equations from the left sides of rules for a finite $\mathcal{R}$[2]. For each indeterminate x_i, there is a linear diophantine equation

$$d_1 v_{i_1} + d_2 v_{i_2} + \cdots + d_m v_{i_m} = e_1 v_{i_1} + e_2 v_{i_2} + \cdots + e_m v_{i_m},$$

where $v_{i_1}, \cdots, v_{i_m}$ are, respectively, the degrees of x_i in the left sides of rules $1, \cdots, m$. So there are n such linear diophantine equations. These equations are solved for $d_1, \cdots, d_m$ and $e_1, \cdots, e_m$ and a basis of *minimal* non-zero simultaneous solutions in which if $d_j \neq 0$, then $e_j = 0$ and if $e_i \neq 0$, then $d_i = 0$, can be computed. Using these basis vectors, any solution to these simultaneous equations can be obtained as a nonnegative linear combination of the vectors in the basis (i.e., the multipliers are nonnegative). Further, only one of the two solutions $< d_1, \cdots, d_m, e_1, \cdots, e_m >$ and $< e_1, \cdots, e_m, d_1, \cdots, d_m >$ need to be considered because of the symmetric nature of the diophantine equations. These equations can be solved using algorithms proposed for solving linear diophantine equations arising in associative-commutative unification problems [Stickel, 1981; Huet, 1978; Romeuf, 1989; Kapur and Zhang, 1989]. The finiteness of a basis from which all solutions to the above set of equations can be generated, also follows from the results related to these algorithms.

It will be interesting to compare these definitions with the corresponding concepts in Robbiano and Sweedler's approach.

5 A Test for a Canonical Basis

The following is a Church-Rosser theorem for k-subalgebras.

[2] This formulation however extends to be applicable to an infinite $\mathcal{R}$ also.

Theorem 5.1: The set $\mathcal{R} = \{L_1 \to R_1, \cdots, L_m \to R_m, \cdots\}$ is canonical or equivalently, the corresponding basis $\{f_1, \cdots, f_m, \cdots\}$ is a canonical basis if and only if all S-polynomials generated using every finite subset of $\mathcal{R}$ reduce to 0.

The proof of the theorem uses the following lemmas.

Lemma 5.2: If $p \to^\star 0$, then for any $L_i \to R_i \in \mathcal{R}$, $(L_i - R_i)\ \ p \to^\star 0$.

Note that it is not necessarily the case that if $p \to^\star 0$, then $t\ p \to^\star 0$ for any term t or even for $t = L_i$, the left side of a rule in $\mathcal{R}$.

It follows by induction from the above lemma that

Corollary 5.3: If $p \to^\star 0$, for any $c \in k$, and any natural numbers $d_{j_1}, \cdots, d_{j_l}$,

$$(c\ (L_{j_1} - R_{j_1})^{d_{j_1}} \cdots (L_{j_l} - R_{j_l})^{d_{j_l}}\ p) \to^\star 0.$$

The following lemma is the key to the proof of Theorem 5.1. Its proof uses Corollary 5.3.

Lemma 5.4: Let $\mathcal{R}$ be such that all of its S-polynomials reduce to 0. If $p_j \to^\star 0$, for each $j = 1, \cdots, n$, then $\sum_{j=1}^{n} (\prod_{i=1}^{m}\ (L_i - R_i)^{d_{j,i}})\ \ p_j \to^\star 0$ for any natural numbers $d_{j,1}, \cdots, d_{j,m}$, for each $j = 1, \cdots, n$.

In addition, we have:

Lemma 5.5: If $p_1 - p_2 \to^\star 0$, then p_1 and p_2 are joinable, i.e., there is a q such that $p_1 \to^\star q$ and $p_2 \to^\star q$.

We can now give the proof of Theorem 5.1.

Proof of Theorem 5.1: $(\Rightarrow:)$ Since $\mathcal{R}$ is canonical and by Theorem 3.3, polynomials p and q have the same normal form if and only if $p - q \in k[\mathcal{R}]$. So, any S-polynomial, say s, of $\mathcal{R}$ and 0 have the normal form, which implies that $s \to^\star 0$.

$(\Leftarrow:)$ Consider any polynomial $p = p' + c\ t$, where p' does not have any monomial whose term is t. Let $c\ t$ be the largest monomial in p which is rewritten in two different ways to $p_1 = p - c\ \prod_{i=1}^{m}\ (L_i - R_i)^{a_i}$ and $p_2 = p - c\ \prod_{i=1}^{m}\ (L_i - R_i)^{b_i}$, respectively.

By Lemma 5.4, $(c\ \prod_{i=1}^{m}\ (L_i - R_i)^{b_i} - c\ \prod_{i=1}^{m}\ (L_i - R_i)^{a_i}) \to^\star 0$. Since $p_1 - p_2 = c\ \prod_{i=1}^{m}\ (L_i - R_i)^{b_i} - c\ \prod_{i=1}^{m}\ (L_i - R_i)^{a_i}$, by Lemma 5.5, p_1 and p_2 are joinable. This implies that $\mathcal{R}$ is confluent, and hence canonical. $\square$.

6 Completion Procedure

From the above theorem, one also gets a completion procedure similar to Buchberger's Gröbner basis algorithm [1985] or the Knuth-Bendix procedure [1970] (see also Huet, 1981) whose correctness can be established using methods similar to the one given in Buchberger's papers. If a given basis of a k-subalgebra is not a canonical basis, then it is possible to generate a canonical basis equivalent to a given basis of a k-subalgebra using the completion procedure. For every S-polynomial of a basis that does not reduce to 0, the current basis is augmented with a normal form of the S-polynomial and the basis is inter-reduced. This process of generating S-polynomials, checking whether they reduce to 0, and augmenting the basis with normal forms of S-polynomials is continued until all S-polynomials of the final basis reduce to 0. Optimizations and heuristics can be introduced into the completion procedure in regards to the order in which various finite subsets of a basis are considered; further, since a finite subset of a basis may result in many S-polynomials, if some S-polynomial results in a new rule which simplifies any rule in the subset under consideration, then the subset does not have to be considered.

Unlike Gröbner basis algorithms, this process of adding new polynomials to a basis may not always terminate. An example below illustrates the divergence of the completion procedure. We consider this a major limitation of this approach in contrast to Shannon and Sweedler's approach. However, the following results are immediate consequences of general results in term rewriting theory [Huet, 1981; Butler and Lankford, 1980; Avenhaus, 1985; Dershowitz et al, 1988] since orderings on polynomials are total, thus a rule can always be made from a polynomial, so the completion procedure will never abort because of the inability to make a rule.

A strategy is called *fair* if and only if all superpositions among all possible finite subsets of rules are eventually considered. There can be many ways to generate superpositions and critical pairs which would constitute a fair strategy. A simple fair strategy is to consider superpositions in the degree ordering irrespective of the ordering $<$ used for making rules from polynomials.

Theorem 6.1: If a completion procedure follows a fair strategy in computing superpositions and critical pairs, then the completion procedure serves as a semi-decision procedure for k-subalgebra membership even when the completion procedure does not terminate.

Proof: If the completion procedure does not terminate on a finite basis F, every superposition is eventually considered during its execution since the procedure employs a fair strategy. Using Theorem 5.1, the limit basis, G_∞, consisting of the polynomials which persist during the execution of the completion procedure, is canonical [Huet, 1981] (a polynomial is said to persist if after a certain iteration of the completion procedure, it never get deleted in later iterations). So, if a polynomial $p \in k[F]$, then $p \rightarrow^\star 0$ after some iteration of the completion procedure since $p \rightarrow^\star 0$ in G_∞. To use the completion procedure as a semi-decision procedure for k-subalgebra membership, keep reducing p as new polynomials are generated by the completion procedure. If $p \in k[F]$, then $p \rightarrow^\star 0$ during the execution of the completion procedure on F irrespective of whether it terminates or not. □

Theorem 6.2: Given a polynomial ordering $<$, if a k-subalgebra generated by F has a finite canonical basis G with respect to $<$, then a completion procedure with a fair strategy would generate a finite canonical basis.

Proof: Suppose that the completion procedure does not generate a finite canonical basis from F but there exists a finite canonical basis G for $k[F]$ with respect to $<$. By Theorem 6.1, the completion procedure on F is a semi-decision procedure, every polynomial in G reduces to 0 during some iteration of the completion procedure. So, in the iteration by which all the polynomials in G have been reduced to 0, the basis generated by the completion procedure generates $k[G] = k[F]$ and further this basis is a canonical basis for $k[F]$, which is a contradiction. □

A basis F (or equivalently, a set of rules $\mathcal{R}$) is called *reduced* if for every polynomial in F

(equivalently, every rule in $\mathcal{R}$), none of its monomials can be reduced using the remaining set of polynomials in F (equivalently, the remaining set of rules in $\mathcal{R}$).

Theorem 6.3 If a completion procedure generates from a basis F, a finite canonical basis G for an ordering $<$ and G is reduced, then G is unique with respect to the ordering $<$.

Proof: Suppose that there are two different finite reduced canonical bases G and G' for $k[F]$ with respect to $<$. The polynomials in them can be ordered using $<$. Let p in G and p' in G' be the smallest polynomials on which they differ. Since $k[G] = k[G']$, if $p < p'$, then $p \rightarrow^* 0$ using polynomials smaller than p' in G'. That means, that p can be reduced using other polynomials in G thus implying that G is not reduced, which is a contradiction. A similar argument applies if $p' < p$. $\square$

For the univariate case, the completion procedure always terminates.

Theorem 6.4: A k-subalgebra over $k[x]$ always has a finite canonical basis which is generated by the completion procedure.

Proof: Consider any finite basis over $k[x]$. Let $\{x^{d_1}, \cdots, x^{d_n}\}$ be the head-terms of polynomials in this basis. The completion procedure can generate new polynomials and add to them to the basis only if the degree of the head-term of each new polynomial cannot be reduced by the polynomials already in the basis i.e., the leading degree cannot be expressed as a linear combination of $d_1, \cdots, d_n$ with nonnegative multipliers. It will be shown that there are only finitely many such polynomials.

Let $d = gcd(d_1, \cdots, d_n)$; we have $d = a_1 d_1 + \cdots + a_n d_n$, and $d_1 = m_1 d, \cdots, d_n = m_n d$ where for each $1 \leq i \leq n$, a_i is an integer and m_i is a positive integer.

Claim: There exists a number r, which is a multiple of d, such that every multiple of d that is greater than or equal to r can be expressed as a nonnegative linear combination of $d_1, \cdots, d_n$.

Proof: Let a_i be the largest negative number among $a_1, \cdots, a_n$ and m_j be the smallest number among $m_1, \cdots, m_n$. Let $r = m_j |a_i| (d_1 + \cdots + d_n)$. We must show that for any $s \geq 0$, $r + s\ d$ can be expressed a nonnegative linear combination of $d_1, \cdots, d_n$. For any $s \geq 0$, it is possible to find $0 \leq s' \leq m_j$ such that $s - s' = b_1 m_1 + \cdots + b_n m_n, \quad b_l \geq 0, 1 \leq l \leq n$. Then, $r + sd = (m_j|a_i| + b_1 + s'a_1)d_1 + \cdots + (m_j|a_i| + b_n + s'a_n)d_n$, so each multiplier of d_l is nonnegative. $\square$

Because of this claim, we can add to the basis, either polynomials with the leading term of degree $< r$ or a polynomial with the leading term of degree between $r + sd$ and $r + sd + d$ for some nonnegative number s. If the basis has to be infinite, a polynmial with $x^{d_{n+1}}$ as the leading term, where $(r + s\ d) < d_{n+1} < (r + s\ d + d)$, must be added, but then $gcd(d_1, \cdots, d_n, d_{n+1}) < d$ since d_{n+1} is not a multiple of d. This means that we cannot add infinitely many polynmials with irreducible leading terms to a finite basis. So, the completion procedure will always terminate for a k-subalgebra over $k[x]$. $\square$

6.1 Examples

Example 1: Consider the example from Shannon and Sweedler [1988] which was discussed earlier. The basis is $F_1 = \{1.\ x^3 - x,\ \ 2.\ x^2\}$ and the rules corresponding to the basis are:
$\mathcal{R}_1 = \{1.\ x^3 \rightarrow x,\ \ 2.\ x^2 \rightarrow 0\}$. A critical pair can be obtained by solving the following diophantine equation:

$$3d_1 + 2d_2 = 3e_1 + 2e_2.$$

The basis of the solutions to this equation is: $< 2, 0, 0, 3 >$. The superposition is x^6 and the critical pair is: $< 2x^4 - x^2, 0 >$. The S-polynomial $2x^4 - x^2$ reduces to 0. So, F is a canonical basis. In contrast, Shannon and Sweedler's approach using tagged variables will have to perform more complex computations to get a Gröbner basis involving tag variables.

Example 2: Let us consider an example given by Robbiano, $F_2 = \{x^3, x^4, x^5 + x^2 + x\}$. The rules corresponding to them are:

$$\mathcal{R}_2 = \{1.\ x^3 \to 0, \quad 2.\ x^4 \to 0, \quad 3.\ x^5 \to -x^2 - x\}.$$

Superpositions and critical pairs can be computed by setting up a diophantine equation:

$$3d_1 + 4d_2 + 5d_3 = 3e_1 + 4e_2 + 5e_3.$$

A minimal basis for the solutions to the above equation is:
$\{< 1, 0, 1, 0, 2, 0 >, < 0, 1, 1, 3, 0, 0 >, < 0, 0, 2, 2, 1, 0 >, < 4, 0, 0, 0, 3, 0 >, < 5, 0, 0, 0, 0, 3 >,$
$< 1, 3, 0, 0, 0, 3 >, < 0, 5, 0, 0, 0, 4 >\}$.
Corresponding to the first solution, the critical pair is obtained by a superposition generated by the product of the left sides of rules 1 and 3 which is equal to the square of the left side of rule 2. The superposition is x^8, and the critical pair is $< x^5 + x^4, 0 >$. The S-polynomial $x^5 + x^4$ can be reduced to its normal form $-x^2 - x$. This means that the given basis is not a canonical basis.

A canonical basis can be obtained however by augmenting the original basis with normal forms of S-polynomials thus computed and repeating this process. So the superposition x^8 gives an additional rule

$$4.\ x^2 \to -x.$$

It is always better to use this rule to simplify the existing rules. Rule 2 gets simplified to x thus giving

$$2'.\ x \to 0.$$

Rule 2' deletes every other rule. As a result, we did not have to consider critical pairs generated by the rules 1, 2, and 3, which got deleted. This is in contrast to having to consider all superpositions generated from the basis solutions of the above diophantine equation which would have resulted in unnecessary computations.

The basis $\{x\}$ is a canonical basis for the k-subalgebra generated by $\{x^3, x^4, x^5 + x^2 + x\}$. It should be easy to see from Theorem 5.1 that a singleton basis is always a canonical basis.

Example 3: Let us consider another example given by Robbiano, $F_3 = \{x, y^2 - xy, xy^2\}$. Using the total degree ordering defined by the variable ordering $y > x$, we get

$$\mathcal{R}_3 = \{1.\ x \to 0, \quad 2.\ y^2 \to xy, \quad 3.\ xy^2 \to 0\}.$$

Rule 3 is normalized using rules 1 and 2 to $3'.\ x^2y \to 0$.

This set of rules gives the following diophantine equations for generating superpositions:

$$d_1 + 2d_3 = e_1 + 2e_3,$$

$$2d_2 + d_3 = 2e_2 + e_3.$$

The basis of common solutions to these equations: $\{< 4, 1, 0, 0, 0, 2 >\}$. So, the only superposition is generated by squaring the left side of rule 3' which is equal to the product of the fourth power of the left side to rule 1 and the left side of rule 2. The critical pair is $< 0, x^5y >$ and its S-polynomial x^5y reduces to 0. So, $\{x, y^2 - xy, x^2y\}$ is a canonical basis for the k-subalgebra generated by $\{x, y^2 - xy, xy^2\}$.

For the same basis F_3, if we use a different total degree ordering defined by the variable ordering $x > y$, then the rule set is slightly different:

$$\{1.\ x \to 0, \quad 2.\ xy \to y^2, \quad 3.\ xy^2 \to 0\}.$$

A critical pair is generated by identifying that the square of the left side of rule 2 is equal to the product of the left sides of rules 1 and 3. The S-polynomial in this case is $2xy^3 - y^4$, which gives a new rule:

$$4.\ xy^3 \to 1/2\, y^4.$$

There is no other superposition from the first three rules.

Rules 1 and 4 superpose with rules 2 and 3. The superposition is x^2y^3 and the critical pair is $< 1/2xy^4, xy^4 >$. The corresponding S-polynomial $1/2xy^4$ does not reduce any further, which gives a rule:

$$5.\ xy^4 \to 0.$$

Also, the cube of the left side of rule 2 is equal to the product of the left side of rule 4 with the square of the left side of rule 1. This gives the critical pair $< y^6 - 3x^2y^4 + 3xy^5, 1/2\, x^2y^4 >$. If the corresponding S-polynomial is reduced, we obtain $y^6 - 3xy^5$ which gives another new rule:

$$6.\ xy^5 \to 1/3\, y^6.$$

There is again a superposition since the fifth power of the left side of rule 2 is equal to the product of the left side of rule 5 and the fourth power of the left side of rule 1. This gives another new rule. It can be shown that this process of generating new rules continue and does not terminate thus resulting in an infinite canonical basis, which is $\{xy^{2j+1} - 1/(j+1)y^{2j+2},\ \ xy^{2j} \mid j \geq 0\}$.

This example illustrates that unlike in the case of ideals over Noetherian rings, this completion procedure need not terminate. Further, there are finitely generated k-subalgebras which have finite canonical basis under one ordering but do not have a finite canonical basis under a different ordering. These observations are similar to the ones made by Robbiano and Sweedler. The situation here is very similar to the one encountered in generating canonical basis for finitely presented monoids (Thue systems) or for first-order equational theories; the reduction orderings there also affect the termination of completion procedures.

It will be interesting to compare the computational performance of the above procedure with Shannon and Sweedler's method.

7 Extension to Unitary Subrings

The approach discussed in this paper can be generalized to compute canonical bases for unitary subrings. The coefficient field k is not included in every unitary subring even though Z is included in every unitary subring if k is of characteristic 0. When rules are made, the coefficient of the left side cannot be made 1, and the definition of reduction relation must be modified to take into consideration the coefficients of the head-terms also. Similarly, the definitions of superpositions, critical pairs and S-polynomials have to be changed to deal with the coefficients. We are also investigating the extensions of this approach to unitary subrings of $R[x_1, \cdots, x_n]$, where R is a commutative ring.

Acknowledgement: Most of this work was initiated while the first author visited University of Kaiserslautern during the summer of 1986 and during the winter of 1986 at the Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS) at New Delhi. The first author would like to thank Lorenzo Robbiano for his encouragement to write this work; this paper would not have been written but for Robbiano's prodding after his talk on this subject at a Gröbner basis workshop in October 1988 at the Mathematical Sciences Institute of Cornell University. We also thank Moss Sweedler for many helpful comments on the first draft of this paper.

References

1. Avenhaus, J. (1985). On the termination of the Knuth-Bendix algorithm. Report 120/84, Universität Kaiserslautern, West German.

2. Buchberger, B. (1965). *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal.* (in German) Ph.D. Thesis, Univ. of Innsbruck, Austria.

3. Buchberger, B. (1976). A theoretical basis for the reduction of polynomials to canonical forms. *ACM-SIGSAM Bulletin* 10/3, 39, 19-29.

4. Buchberger, B., and Loos, R. (1982). Algebraic simplification. In: *Computer algebra: Symbolic and algebraic computation.* (eds. Buchberger, Collins, and Loos), Computing Suppl. 4, Springer Verlag, 11-43.

5. Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. In: N.K. Bose (ed.) *Multidimensional Systems Theory*, Reidel, 184-232.

6. Butler, G., and Lankford, D.S. (1980). Experiments with computer implementations of procedures which often derive decision algorithms for the word problem in abstract algebras. Memo MTP-7, Dept. of Mathematics, Louisiana Tech. University, Ruston, LA, August 1980.

7. Dershowitz, N., Marcus, L., and Tarlecki, A. (1988). Existence, uniqueness, and construction of rewrite systems. *SIAM J. of Computing*, to appear.

8. Huet, G. (1978). An algorithm to generate the basis of solutions to homogeneous linear diophantine equations. *Information Processing letters*, 7, 3, 144-147.

9. Huet, G. (1981). A complete proof of correctness of the Knuth-Bendix completion procedure. *J. of Computer and Systems Sciences*, 23, 1, 11-21.

10. Kandri-Rody, A., and Kapur, D. (1984). An algorithm for computing a Gröbner basis of a polynomial ideal over a Euclidean ring. G.E. Corporate Research and Development Report 84CRD045, Schenectady, NY. A revised version appeared in *J. of Symbolic Computation*, August 1988.

11. Kapur, D., and Narendran, P. (1985). Existence and construction of a Gröbner basis for a polynomial ideal. Presented at a workshop on *Combinatorial algorithms in algebraic structures,* Europaische Akademie, Otzenhausen, W. Germany.

12. Kapur, D., and Zhang, H. (1989). An improved upper bound for nonnegative basis solutions of a linear diophantine equation. Technical Report 89-9, Department of Computer Science, State University of New York at Albany, NY.

13. Knuth, D., and Bendix, P. (1970). Simple word problems in universal algebras. In: J. Leech (ed.) *Computational Problems in Abstract Algebras*, Pergamon Press.

14. Lankford, D. S., and Ballantyne, A. M. (1983). On the uniqueness of term rewriting systems. Unpublished note, Dept. of Mathematics, Louisiana Tech. University, Ruston, LA.

15. Robbiano, L., and Sweedler, M. (1988). Computing a canonical basis of a k-subalgebra. Presented at a Mathematical Sciences Institute workshop on Gröbner bases, Cornell University.

16. Romeuf, J.-F. (1989). Solutions of a linear system in the free commutative monoid. Laboratoire d'Informatique de Rouen, Universite de Rouen - Faculte des Sciences. Mont-Saint-Aignan, France.

17. Shannon, D., and Sweedler, M. (1987). Using Gröbner bases to determine algebra membership, split surjective algebra homomorphisms and determine bilateral equivalence. Unpublished Manuscript, Dept. of Mathematics, Cornell University. To appear in *J. of Symbolic Computation.*

18. Shannon, D., and Sweedler, M. (1988). Using Gröbner bases to determine subalgebra membership. Unpublished Manuscript, Dept. of Mathematics, Cornell University.

19. Stickel, M.E. (1981). A unification algorithm for associative-commutative unification. *Journal ACM*, 28, 3, 423-434.

20. van der Waerden, B.L. (1966). *Modern Algebra, Vol. I and II.* Frederick Ungar Publishing Co., New York.

21. Zariski, O., and Samuel, P. (1958). *Commutative Algebra, Vol. I.* Springer Verlag, New York.

Appendix: Proofs of Lemmas and Theorems

Theorem 3.3: The relation $\leftrightarrow^\star$, the reflexive, symmetric and transitive closure of $\rightarrow$, is the k-subalgebra equivalence relation induced by $k[\mathcal{R}]$ associated with $\mathcal{R}$, i.e. for any p and q, $p \leftrightarrow^\star q$ if and only if $p - q \in k[\mathcal{R}]$.

Proof: ($\Rightarrow$) Assume that $p \leftrightarrow^n q$ and show that $p - q \in k[\mathcal{R}]$. This is proved by induction on n.

Basis: $n = 0$. Then $p = q$ and $0 \in k[\mathcal{R}]$.

Induction Step: By induction hypothesis, $p \leftrightarrow^n p' \Rightarrow (p - p') \in k[\mathcal{R}]$. Let $p \leftrightarrow^n p' \leftrightarrow q$. From the definition it follows that $p' - q \in k[\mathcal{R}]$. Hence $(p - p') - (p' - q) = (p - q) \in k[\mathcal{R}]$.

($\Leftarrow$) Assume that $p - q \in k[\mathcal{R}]$ and show that $p \leftrightarrow^\star q$. It is easy to see that $p = q + \sum_{j=1}^{n} c_j (\prod_{i=1}^{m} (L_i - R_i)^{d_{j,i}})$. The proof is by induction on n.

Basis: $n = 0$. Then $p = q$, hence $p \leftrightarrow^\star q$.

Induction step: $p = q + c_1 \prod_{i=1}^{m} (L_i - R_i)^{d_{1,i}} + \sum_{j=2}^{n} c_j (\prod_{i=1}^{m} (L_i - R_i)^{d_{j,i}})$. By the induction hypothesis, $p \leftrightarrow^\star q_1$ where $q_1 = q + c_1 \prod_{i=1}^{m} (L_i - R_i)^{d_{1,i}}$. Let t_1 be the term in q_1 which can be reduced, and let t be the head-term of $\prod_{i=1}^{m} (L_i - R_i)^{d_{1,i}}$.

Case 1: $t_1 \geq t$: Apply the same reductions on q and q_1 until t (or a lesser term) needs to be reduced. Let the results of these reductions be q' and $q_1{}'$, respectively, i.e, $q \rightarrow^\star q'$ and $q_1 \rightarrow^\star q_1{}'$. Then, $q_1{}' - q' = c_1 \prod_{i=1}^{m} (L_i - R_i)^{d_{1,i}}$. Now apply the appropriate reduction on $q_1{}'$ and q' to reduce t which will have the same result, say q''. We have $q \rightarrow^\star q''$ as well as $q_1 \rightarrow^\star q''$, so $q \leftrightarrow^\star q_1$. Using the induction hypothesis, $p \leftrightarrow^\star q$.

Case 2: $t_1 < t$: The head-coefficient of $c_1 \prod_{i=1}^{m} (L_i - R_i)^{d_{1,i}}$ cancels out with the coefficient of t in q and t is the head-term of q. So, $q \rightarrow q_1$ by applying the reduction at t. Thus, $p \leftrightarrow^\star q$. Hence the proof. $\Box$.

Lemma 5.2: If $p \rightarrow^\star 0$, then for any $L_i \rightarrow R_i \in \mathcal{R}$, $(L_i - R_i)p \rightarrow^\star 0$.

Proof: By induction on number, say n, of reduction steps in $p \rightarrow^\star 0$.

Basis: $n = 0$: This is trivial as then $p = 0$ which implies that $(L_i - R_i)p = 0$.

Induction step: The induction hypothesis is that for every $0 \leq n' < n$, if $p \rightarrow^{n'} 0$, then $(L_i - R_i)p \rightarrow^{n'} 0$.

Now, $p \rightarrow^{n} 0$, i.e., $p = ct + p' \rightarrow q \rightarrow^{n-1} 0$, where $c\ t$ is the head monomial of p and q is the result of rewriting p at the monomial ct in a single step. This must be the case as otherwise if $c\ t$ cannot be reduced, p cannot be reduced to 0.

Let $q = p - c(L_{j_1} - R_{j_1})^{d_{j1}}(L_{j_2} - R_{j_2})^{d_{j2}} \cdots (L_{j_k} - R_{j_k})^{d_{jk}}$. Consider $(L_i - R_i)p = L_i ct - R_i ct + L_i p' + R_i p'$; since $L_i ct$ is the head monomial in $(L_i - R_i)p$, it can be reduced by slightly modifying the reduction step used for ct and the result is

$$(L_i - R_i)p - c(L_i - R_i)(L_{j_1} - R_{j_1})^{d_{j1}}(L_{j_2} - R_{j_2})^{d_{j2}} \cdots (L_{j_k} - R_{j_k})^{d_{jk}}.$$

Collecting the terms, we have: $L_i(p - c(L_{j_1} - R_{j_1})^{d_{j1}}(L_{j_2} - R_{j_2})^{d_{j2}} \cdots (L_{j_k} - R_{j_k})^{d_{jk}}) - R_i(p - c(L_{j_1} - R_{j_1})^{d_{j1}}(L_{j_2} - R_{j_2})^{d_{j2}} \cdots (L_{j_k} - R_{j_k})^{d_{jk}}) = L_i q - R_i q = (L_i - R_i)q$. By the induction hypothesis, $(L_i - R_i)q \rightarrow^{\star} 0$. So, $(L_i - R_i)p \rightarrow^{\star} 0$. □

Corollary 5.3: If $p \rightarrow^{\star} 0$, for any $c \in k$, and any natural numbers $d_{j_1}, \cdots, d_{j_l}$,

$$(c\ (L_{j_1} - R_{j_1})^{d_{j1}} \cdots (L_{j_l} - R_{j_l})^{d_{jl}}\ p) \rightarrow^{\star} 0.$$

Proof: The proof is by induction on $n = d_{j_1} + \cdots + d_{j_l}$.

Basis: $n = 0$. If $p \rightarrow^{\star} 0$, it needs to be proved that for any $c \in k$, $c\ p \rightarrow^{\star} 0$ also. If $c = 0$, then $c\ p = 0$. For an nonzero c, every reduction step in $p \rightarrow^{\star} 0$ can be repeated on $c\ p$ also, so using the same reduction steps, $cp \rightarrow^{\star} 0$.

Induction step: Assume that the statement of the corollary is true for n. By the induction hypothesis and Lemma 5.2, the statement is true for $n+1$ also. □

Lemma 5.4: Let $\mathcal{R}$ be such that all of its S-polynomials reduce to 0. If $p_j \rightarrow^{\star} 0$, for $j = 1, \cdots, n$, then $\sum_{j=1}^{n} (\prod_{i=1}^{m} (L_i - R_i)^{d_{j,i}})\ p_j \rightarrow^{\star} 0$ for any natural numbers $d_{j,1}, \cdots, d_{j,m}$, for each $j = 1, \cdots, n$.

Proof: The proof is by induction on the maximum term, say t, among the head-terms of $\prod_{i=1}^{m} (L_i - R_i)^{d_{j,i}}\ p_j$, $1 \leq j \leq n$, using the well-founded term ordering $<$.

Basis: $t = 1$. Then $\sum_{j=1}^{n} \prod_{i=1}^{m} (L_i - R_i)^{d_{j,i}}\ p_j = c \in k$, which reduces to 0.

Induction step: Assume that the statement of the lemma holds for all terms $t' < t$.

Let n' be the number of summands $\prod_{i=1}^{m} (L_i - R_i)^{d_{j,i}}\ p_j$ whose head-term is t. Without any loss of generality, let these summands be be the first n' summand in $\sum_{j=1}^{n} \prod_{i=1}^{m} (L_i - R_i)^{d_{j,i}}\ p_j$. We now perform induction on n'.

Basis: $n' = 1$, i.e., there is only one summand whose head-term is t, which is $q = \prod_{i=1}^{m}(L_i - R_i)^{d_{1,i}}\ p_1$. By Corollary 5.3, $\prod_{i=1}^{m}(L_i - R_i)^{d_{1,i}}\ p_1 \to^\star 0$; in particular, the first reduction step reduces the head-term t. If $q \to q_1 \to^\star 0$, then by the first induction hypothesis, $(q_1 + \sum_{j=2}^{n} \prod_{i=1}^{m} (L_i - R_i)^{d_{j,i}}\ p_j) \to^\star 0$ since the maximum term among the head-terms of the summands is $< t$. Thus, $(q + \sum_{j=2}^{n} \prod_{i=1}^{m} (L_i - R_i)^{d_{j,i}}\ p_j) \to^\star 0$.

Induction step: Assume the statement of the lemma holds for t and n', and prove it for t and $n' + 1$.

By Corollary 5.3, $q = \prod_{i=1}^{m}(L_i - R_i)^{d_{1,i}}\ p_1 \to^\star 0$ and by the induction hypothesis, $r = (\sum_{j=2}^{n} \prod_{i=1}^{m} (L_i - R_i)^{d_{j,i}}\ p_j) \to^\star 0$. Let $q \to q_1 \to^\star 0$ with the first reduction at term t. Similarly, let $r \to r_1 \to^\star 0$ with the first reduction at term $s \le t$. If $s < t$, which implies that the head-coefficients of n' summands with t as the head-term cancel out; then this is the same as the basis case since we can replace the n summands by r.

Below we consider the case when $s = t$. Let $q_1 = q - c_1 \prod_{i=1}^{m} (L_i - R_i)^{a_i}$ and $r_1 = r - c_2 \prod_{i=1}^{m} (L_i - R_i)^{b_i}$, where $ht(\prod_{i=1}^{m} (L_i - R_i)^{a_i}) = ht(\prod_{i=1}^{m} (L_i - R_i)^{b_i}) = t$. The coefficient of t in $q + r$ is $c_1 + c_2$.

Case 1: The coefficients of the head-term t of the $n' + 1$ summands cancel out, i.e., $c_1 + c_2 = 0$. So, $q + r = q_1 + r_1 - c_2(\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i})$.

Case 2: The coefficients of the head-term t of the $n' + 1$ summands do not cancel out: Since the head-term of $q + r$ can be reduced, we rewrite it using the same rules used to rewrite q to q_1, i.e., $(q + r) \to (q + r) - (c_1 + c_2)\prod_{i=1}^{m} (L_i - R_i)^{a_i} = q_1 + r_1 - c_2(\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i})$.

In both cases, since $q_1 \to^\star 0$ and $r_1 \to^\star 0$ and if it can be proved that

$$(\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i}) \to^\star 0,$$

by the first induction hypothesis, we have

$$q_1 + r_1 - c_2(\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i}) \rightarrow^\star 0$$

since the head-terms of q_1, r_1 and $(\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i})$ are less than t. This would imply that $(q + r) \rightarrow^\star 0$, which will complete the proof of Lemma 5.4.

Claim: If $ht(\prod_{i=1}^{m} (L_i - R_i)^{a_i}) = ht(\prod_{i=1}^{m} (L_i - R_i)^{b_i})$, then $(\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i}) \rightarrow^\star 0$.

Proof: By induction on the head-term of $\prod_{i=1}^{m} (L_i - R_i)^{a_i}$ in a well-founded ordering $<$.

Basis: If $ht(\prod_{i=1}^{m} (L_i - R_i)^{a_i}) = 1$, this is trivially true.

Induction step: Assume the claim is true if $ht(\prod_{i=1}^{m} (L_i - R_i)^{a_i}) = t' < t$.

If $a_i = b_i$, for $1 \leq i \leq m$, then the claim is true also since $\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i} = 0$.

If we can factor the common part of $\prod_{i=1}^{m} (L_i - R_i)^{a_i}$ and $\prod_{i=1}^{m} (L_i - R_i)^{b_i}$, i.e., there exists a non-zero vector $f_i = min(a_i, b_i), 1 \leq i \leq m$, then by the induction hypothesis,

$$\prod_{i=1}^{m}(L_i - R_i)^{a_i - f_i} - \prod_{i=1}^{m}(L_i - R_i)^{b_i - f_i} \rightarrow^\star 0.$$

By Corollary 5.3, we have $\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i} \rightarrow^\star 0$.

Consider the case when t can be decomposed into t_1 and t_2 such that $t_1 \neq 1, t_2 \neq 1, t = t_1\, t_2$ and there exists $a_{1,i}, a_{2,i}, b_{1,i}, b_{2,i}, 1 \leq i \leq m$, such that $ht(\prod_{i=1}^{m}(L_i - R_i)^{a_{1,i}}) = ht(\prod_{i=1}^{m}(L_i - R_i)^{b_{1,i}}) = t_1$ and $ht(\prod_{i=1}^{m}(L_i - R_i)^{a_{2,i}}) = ht(\prod_{i=1}^{m}(L_i - R_i)^{b_{2,i}}) = t_2$.

By the induction hypothesis of the claim, we have

$$\prod_{i=1}^{m}(L_i - R_i)^{a_{1,i}} - \prod_{i=1}^{m}(L_i - R_i)^{b_{1,i}} \rightarrow^\star 0,$$

as well as

$$\prod_{i=1}^{m}(L_i - R_i)^{a_{2,i}} - \prod_{i=1}^{m}(L_i - R_i)^{b_{2,i}} \rightarrow^\star 0.$$

Further, by Corollary 5.3,

$$\prod_{i=1}^{m}(L_i - R_i)^{a_{2,i}}(\prod_{i=1}^{m}(L_i - R_i)^{a_{1,i}} - \prod_{i=1}^{m}(L_i - R_i)^{b_{1,i}}) \rightarrow^\star 0,$$

as well as

$$\prod_{i=1}^{m}(L_i - R_i)^{b_{1,i}}(\prod_{i=1}^{m}(L_i - R_i)^{a_{2,i}} - \prod_{i=1}^{m}(L_i - R_i)^{b_{2,i}}) \rightarrow^\star 0.$$

Since $\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i} = \prod_{i=1}^{m}(L_i - R_i)^{a_{2,i}}(\prod_{i=1}^{m}(L_i - R_i)^{a_{1,i}} - \prod_{i=1}^{m}(L_i - R_i)^{b_{1,i}})$ $+\prod_{i=1}^{m}(L_i - R_i)^{b_{1,i}}(\prod_{i=1}^{m}(L_i - R_i)^{a_{2,i}} - \prod_{i=1}^{m}(L_i - R_i)^{b_{2,i}})$,
and the head-terms of each of the summands above is $< t$, by the first induction hypothesis,

$$\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i} \rightarrow^\star 0.$$

If none of the above conditions holds, then there is a superposition whose S-polynomial is exactly $\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i}$ (or $\prod_{i=1}^{m} (L_i - R_i)^{b_i} - \prod_{i=1}^{m} (L_i - R_i)^{a_i}$), in which case by the assumption of Lemma 5.4, $\prod_{i=1}^{m} (L_i - R_i)^{a_i} - \prod_{i=1}^{m} (L_i - R_i)^{b_i} \rightarrow^\star 0$. This completes the proof of the claim. $\Box$.

The proof of Lemma 5.4 is also completed. $\Box$

Lemma 5.5: If $p_1 - p_2 \rightarrow^\star 0$, then p_1 and p_2 are joinable, i.e., there is a q such that $p_1 \rightarrow^\star q$ and $p_2 \rightarrow^\star q$.

Proof: By induction on the number of steps in $p_1 - p_2 \rightarrow^\star 0$.

Basis: This is trivially true since $p_1 = p_2$.

Induction step: Let $p_1 - p_2 \rightarrow h \rightarrow^\star 0$, we will show that there exist h_1 and h_2 such that $h = h_1 - h_2$, $p_1 \rightarrow^\star h_1$ and $p_2 \rightarrow^\star h_2$; then by the induction hypothesis, h_1 and h_2 are joinable, implying that p_1 and p_2 are joinable.

If p_1 and p_2 have different head-terms, then if $ht(p_1) > ht(p_2)$, then $p_1 \rightarrow h_1$ using the same reduction step as on $p_1 - p_2$ and $h_2 = p_2$. A similar argument works for the case when $ht(p_2) > ht(p_1)$.

If $ht(p_1) = ht(p_2)$ but their head-coefficients are different, then $p_1 \rightarrow h_1$ and $p_2 \rightarrow h_2$ using the reduction step used on $p_1 - p_2$. If their head-coefficients are also the same, then $p_1 \rightarrow^\star h_1$ and

$p_2 \rightarrow^{\star} h_2$ obtained by rewriting p_1 and p_2 using the same reduction steps on identical monomials till the largest monomial on which p_1 and p_2 differ are reduced. This completes the proof of Lemma 5.5. $\square$