Computers and Mathematics

Erich Kaltofen Stephen M. Watt
Editors

Computers and Mathematics

pringer-Verlag
ew York Berlin Heidelberg
ondon Paris Tokyo

Erich Kaltofen
Rensselaer Polytechnic
Department of Computer Science
Troy, NY 12180, U.S.A.

Stephen M. Watt
IBM Watson Research Center
Yorktown Heights, NY 10598, U.S.A.

Library of Congress Cataloging-in-Publication Data

Computers and mathematics / Erich Kaltofen, Stephen M. Watt, editors.
p. cm.
To be used at conference on computers & mathematics at Massachusetts Institute of Technology, June 12, 1989.
1. Mathematics—Data processing—Congresses. I. Kaltofen, Erich.
II. Watt, Stephen M. III. Massachusetts Institute of Technology.
QA76.95.C64 1989
510'.28'5—dc20 89-6259

Printed on acid-free paper.

Camera-ready text provided by authors
Printed and bound by R.R. Donnelley & Sons, Harrisonburg, Virginia
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-97019-3 Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-97019-3 Springer-Verlag Berlin Heidelberg New York

About the Cover

Page from Ramanujan's Lost Notebook. Ramanujan's Lost Notebook is a collection of pages of formulas and calculations done by Ramanujan during the last year of his life. It was apparently in the possession of G. H. Hardy and G. N. Watson between 1920 and 1965; however neither one ever mentioned it in print. R. Rankin and J. M. Whittaker assisted Watson's widow in placing the Lost Notebook in the Wren Library in Cambridge. It was examined by G. E. Andrews in 1976, and he published the first discussion of its contents in the *American Mathematical Monthly* in 1979.

This is one of the most amazing pages in the Lost Notebook. The last four formulas are examples of the Mock Theta Conjectures (settled in 1988 by D. R. Hickerson). The formulas for $F(q^{1/5})$ and $f(q^{1/5})$ are, in fact, crucial to the explanation of certain partition congruences found by Dyson, Atkin, Swinnerton-Dyer and Garvan. (This page was reproduced by courtesy of Narosa Publishing House, New Delhi.)

Trefoil Tube. Building a tube around a space curve provides a powerful technique for analyzing local properties like curvature and torsion as well as global properties such as knottedness. The tube around a trefoil knot, produced by Thomas Banchoff and associates at Brown University, is related to the stereographic projection of an orbit of a dynamical system on the unit sphere in 4-dimensional space. This example was studied in collaboration with Hüeseyin Koçak, Fred Bisshopp, David Laidlaw and David Margolis.

Cover design by Alexandra Gatje/Richard Jenks

Preface

Computers and Mathematics '89 is the third in a series of conferences devoted to the use of computers in mathematics and the mathematical sciences. This is interpreted in a broad sense; computers are used in mathematics not just for approximate numerical calculation but in virtually every area of pure and applied mathematics, including algebra, geometry, number theory, group theory, integration and differential equations.

Each of the conferences in this series has had a strong, interdisciplinary program of invited speakers. In *Computers and Mathematics '89* the contributed research papers have assumed an equally important role. This volume contains the contributed papers accepted for presentation, selected from 85 drafts submitted in response to the call for papers.

The program committee wishes to thank all who submitted papers for consideration and all who assisted in the selection process. The program committee chairman would like to express his thanks to Mrs. Donna Carr for her untiring assistance in the secretarial work.

Conferences in the Computers and Mathematics Series

Computer Algebra as a Tool for Research in Mathematics and Physics,
April 5–6, 1984, Courant Institute of Mathematical Sciences, New York.

Computers and Mathematics '86,
July 30–August 1, 1986, Stanford University, California.

Computers and Mathematics '89,
June 13–17, 1989, Massachusetts Institute of Technology.

Table of Contents

Session 4, Track A (10:45am–12:05pm)
Chair: Fritz Schwarz

Session 4, Track B (10:45am–12:05pm)
Chair: Neil Soiffer

List of Contributors

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 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 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.

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:

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

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 biggest 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 the polynomial $p - q$ must be in $k[\mathcal{R}]$. Also observe that an element of k always reduces to 0 using any basis by taking $d_{j_1} = \cdots = d_{j_l} = 0$. 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.

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. Further details and proofs are given in an expanded version of this paper [Kapur and Madlener, 1989].

2 k-Subalgebras and Canonical bases

Let $k[x_1, \cdots, x_n]$ be the polynomial 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 Zariski and Samuel for definitions). Following Shannon and Sweedler, we write this k-subalgebra as $k[f_1, \cdots, f_m]$. 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 $k[f_1, \cdots, f_m]$. 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) $k[f_1, \cdots, f_m] = k[g_1, \cdots, g_r]$, (ii) for every element $p \in k[f_1, \cdots, f_m]$, $p \rightarrow_G^* 0$, and (iii) for every element $q \in k[x_1, \cdots, x_n]$, q has a unique normal form with respect to $\rightarrow_G$. Further, for any p and q, p and q have the same normal form if and only if $p - q \in k[f_1, \cdots, f_m]$. Such

[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.

We believe that Robbiano and Sweedler [1988] defined the reduction relation in a similar way except that they consider only the head-term of p instead of any term in p. In their approach, if the head-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^6 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 $\rightarrow$ is terminating.

This follows from the fact that (i) the left side of a rule is the head-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.

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 $p \rightarrow^* q$ 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 $\mathcal{R}$.

Theorem 3.3: The relation $\leftrightarrow^*$, 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, $p \leftrightarrow^* q$ 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.

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 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 $\{L_{j_1}, L_{j_2}, \cdots, L_{j_l}\}$ 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 $< d_{j_1}, d_{j_2}, \cdots, d_{j_l} >$, which are exponents associated with rules $\{L_{j_1}, L_{j_2}, \cdots, L_{j_l}\}$, 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

$$L_{j_1}{}^{d_{j_1}} L_{j_2}{}^{d_{j_2}} \cdots L_{j_l}{}^{d_{j_l}} = L_{i_1}{}^{e_{i_1}} L_{i_2}{}^{e_{i_2}} \cdots L_{i_{l'}}{}^{e_{i_{l'}}}.$$

The vector $< d_{j_1}, d_{j_2}, \cdots, d_{j_l} >$ 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 ($< c_1, c_2, \cdots, c_l >$ is *smaller* than $< c'_1, c'_2, \cdots, c'_l >$ if and only if they are distinct and each $c_i \leq c'_i, 1 \leq i \leq l$). 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 $< d_{j_1}, d_{j_2}, \cdots, d_{j_l} >$ satisfying the above property about the left sides of the rules. In that case, the rule subset $\{L_{j_1}, L_{j_2}, \cdots, L_{j_l}\}$ is said to superpose in more than one ways.

The *critical pair* associated with this superposition is:

$$< L_{j_1}{}^{d_{j_1}} L_{j_2}{}^{d_{j_2}} \cdots L_{j_l}{}^{d_{j_l}} - (L_{j_1} - R_{j_1})^{d_{j_1}} (L_{j_2} - R_{j_2})^{d_{j_2}} \cdots (L_{j_l} - R_{j_l})^{d_{j_l}},$$
$$L_{i_1}{}^{e_{i_1}} L_{i_2}{}^{e_{i_2}} \cdots L_{i_{l'}}{}^{e_{i_{l'}}} - (L_{i_1} - R_{i_1})^{e_{i_1}} (L_{i_2} - R_{i_2})^{e_{i_2}} \cdots (L_{i_{l'}} - R_{i_{l'}})^{e_{i_{l'}}} >.$$

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

$$(L_{j_1} - R_{j_1})^{d_{j_1}} (L_{j_2} - R_{j_2})^{d_{j_2}} \cdots (L_{j_l} - R_{j_l})^{d_{j_l}} - (L_{i_1} - R_{i_1})^{e_{i_1}} (L_{i_2} - R_{i_2})^{e_{i_2}} \cdots (L_{i_{l'}} - R_{i_{l'}})^{e_{i_{l'}}}.$$

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

The set of critical pairs for a finite set $\mathcal{R}$ of rules is always finite; a bound can be computed using the degree of the indeterminates appearing in the left sides of rules [Stickel, 1981; Huet, 1978]. The finiteness of the number of critical pairs also follows from the fact that the vectors of exponents $< d_1, \cdots, d_m, e_1, \cdots, e_m >$, with $d_j, e_i \geq 0$, satisfying the following equation, form an abelian monoid which has a finite basis.

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

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]. 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.

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

5 A Test for a Canonical Basis

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

Theorem 5.1: The set $\mathcal{R} = \{L_1 \rightarrow R_1, \cdots, L_m \rightarrow R_m, \cdots\}$ 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 $p \rightarrow^* 0$, then for any $L_i \rightarrow R_i \in \mathcal{R}$, $(L_i - R_i)p \rightarrow^* 0$.

Note that it is not necessarily the case that $t\ p \rightarrow^* 0$ 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 $p \rightarrow^* 0$, for any $c \in k$, and any natural numbers $d_{j_1}, \cdots, d_{j_l}$,
$(c\,(L_{j_1} - R_{j_1})^{d_{j_1}} \cdots (L_{j_l} - R_{j_l})^{d_{j_l}}\ p) \rightarrow^* 0$.

In addition, we have:

Lemma 5.4: If $p_1 - p_2 \rightarrow^* 0$, then p_1 and p_2 are joinable, i.e., there is a q such that $p_1 \rightarrow^* q$ and $p_2 \rightarrow^* q$.

Sketch of Proof of Theorem 5.1: The only if part of the proof is easy and is omitted. The proof of the if part follows. Consider a polynomial p that can be reduced in two different ways. Since the reduction is defined by rewriting the biggest possible monomial which can be reduced using a finite subset of rules in $\mathcal{R}$, the only case to consider is when p has a monomial ct' which can be reduced in two different ways and no monomial greater than ct' in p can be reduced. So there exist two m-vectors $< a_1, \cdots, a_m >$ and $< b_1, \cdots, b_m >$ with some a_i and b_j possibly 0, such that $t' = L_1^{a_1} \cdots L_m^{a_m} = L_1^{b_1} \cdots L_m^{b_m}$ and $p \rightarrow p_1 = p - c(L_1 - R_1)^{a_1} \cdots (L_m - R_m)^{a_m}$ as well as $p \rightarrow p_2 = p - c(L_1 - R_1)^{b_1} \cdots (L_m - R_m)^{b_m}$. Let $c_1 = min(a_1, b_1), \cdots, c_m = min(a_m, b_m)$; c_i's correspond to the common powers of the rules applied on both sides. Let $d_1 = a_1 - c_1, \cdots, d_m = a_m - c_m$ and $e_1 = b_1 - c_1, \cdots, e_m = b_m - c_m$. Because of Corollary 5.3, and Lemma 5.4, it suffices to show that

$$q = (L_1 - R_1)^{d_1} \cdots (L_m - R_m)^{d_m} - (L_1 - R_1)^{e_1} \cdots (L_m - R_m)^{e_m} \rightarrow^* 0, \qquad (*)$$

such that for any i, if $d_i \neq 0$ then $e_i = 0$, and if $e_i \neq 0$ then $d_i = 0$.

This is shown by Noetherian induction using the well-founded ordering $<$ on the head-term $t = L_1^{d_1} \cdots L_m^{d_m} = L_1^{e_1} \cdots L_m^{e_m}$. The basis step of $t = 1$ is trivial. The induction hypothesis is to assume that $(*)$ holds for $t' < t$.

There are two cases: (i) t cannot be decomposed into $t_1 \neq 1$ and $t_2 \neq 2$ such that $t = t_1\ t_2$, and both t_1 and t_2 can be reduced by the rules in $\mathcal{R}$. This implies that the exponent vector $< d_1, \cdots, d_m, e_1, \cdots, e_m >$ belongs to a minimal basis set of solutions obtained from diophantine equations associated with $\mathcal{R}$ since this exponent vector cannot be expressed as a sum of two non-zero exponent vectors. The S-polynomial corresponding to this exponent vector reduces to 0 by the assumption that all the S-polynomials of $\mathcal{R}$ reduce to 0.

(ii) $t = t_1\ t_2$, and $t_1,\ t_2 \neq 1$: By the induction hypothesis, for $i = 1, 2$,

$$s_i = (L_1 - R_1)^{d_{i1}} \cdots (L_m - R_m)^{d_{im}} - (L_1 - R_1)^{e_{i1}} \cdots (L_m - R_m)^{e_{im}} \rightarrow^* 0,$$

where $t_i = L_1^{d_{i1}} \cdots L_m^{d_{im}} = L_1^{e_{i1}} \cdots L_m^{e_{im}}$. Obviously, $d_j = d_{1j} + d_{2j}$ and $e_j = e_{1j} + e_{2j}$.

If s_1 reduces to 0 in l_1 reduction steps by reducing terms $r_{11}, \cdots, r_{1l_1}$ in the first, $\cdots$, l_1-th step, respectively, then by Corollary 5.3, $(L_1 - R_1)^{d_{21}} \cdots (L_m - R_m)^{d_{2m}}\ s_1$ also reduces to 0 in exactly

l_1 steps by reducing terms $t_2\, r_{11}, \cdots, t_2\, r_{1l_1}$ in the respective steps. A similar reduction sequence can be obtained for $(L_1 - R_1)^{e_{11}} \cdots (L_m - R_m)^{e_{1m}}\, s_2$ reducing to 0 from the reduction sequence $s_2 \rightarrow^{l_2} 0$. Now $q = (L_1 - R_1)^{d_{21}} \cdots (L_m - R_m)^{d_{2m}}\, s_1 + (L_1 - R_1)^{e_{11}} \cdots (L_m - R_m)^{e_{1m}}\, s_2$ and a reduction sequence from q to 0 can be constructed by appropriately mixing the reduction steps from the above reduction sequences and additional reduction sequences available using the induction hypothesis. These details can be found in the proof given in an expanded version of this paper [Kapur and Madlener, 1989].

Thus $\mathcal{R}$ is a canonical basis. □

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, and the completion procedure will never abort because of the inability to make a rule.

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.

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

Further, such a finite canonical basis is unique with respect to $<$ if it is reduced (i.e., for every polynomial in the basis, none of its monomials can be reduced using the remaining set of polynomials in the basis).

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.

For the univariate case, the completion procedure always terminates.

Theorem 6.3: A k-subalgebra over $k[x]$ always has a finite canonical basis which is gener-

ated by the completion procedure.

Sketch of Proof: Suppose r polynomials with the degrees $d_1, \ldots, d_r$ are already generated in a basis. There is a number $bound(d_1, \cdots, d_r)$ that is a multiple of $d = gcd(d_1, \cdots, d_r)$ such that every multiple of d which is $\geq bound(d_1, \cdots, d_r)$ can be expressed as a nonnegative linear combination of $\{d_1, \cdots, d_r\}$. Since a polynomial will be added to the basis only if the degree of its head-term cannot be expressed as a nonnegative linear combination of $\{d_1, \cdots, d_r\}$, one can only add to the basis, polynomials of degree $< bound(d_1, \cdots, d_r)$ or of degree d_{r+1} which is not a multiple of d. In the second case, the $gcd(d_1, \cdots, d_r, d_{r+1}) < d$. □.

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:

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

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

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

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

$$2'.\ x \rightarrow 0.$$

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.