GENERAL ELECTRIC

General Electric Company
Corporate Research and Development
Schenectady, New York 12345

TECHNICAL INFORMATION SERIES

AUTHOR
Kandri-Rody, A*
Kapur, D

SUBJECT
computer algebra, term-rewriting system

NO.
83CRD286

DATE
December 1983

TITLE
On Relationship between Buchberger's Grobner Basis Algorithm and the Knuth-Bendix Completion Procedure

GE CLASS 1

NO. PAGES 23

ORIGINATING COMPONENT
Information Systems Laboratory

CORPORATE RESEARCH AND DEVELOPMENT SCHENECTADY, N.Y.

SUMMARY

In 1965, Buchberger developed an algorithm for generating the canonical basis (called Grobner Basis) for an ideal of a polynomial ring over rationals. This algorithm has been conjectured to be similar to the completion procedure for equational theories developed by Knuth and Bendix based on term rewriting systems. We develop a general framework for combining a reduction relation with a simplification relation using which we show that the Grobner basis algorithm of Buchberger is an instance of the generalized Knuth-Bendix completion procedure. The treatment for viewing polynomial simplification is based entirely on term rewriting theory. The general framework is also helpful in gaining insight in the behavior of the canonical basis computation in other computer algebra applications.

*On leave from University Mohammed-V, Rabat, Morocco. Presently with the Dept. of Mathematical Sciences, Rensselaer Polytechnic Institute, Troy, NY.

KEY WORDS **Grobner basis, canonical basis, polynomial simplification, polynomials over rationals, Knuth-Bendix completion procedure, residue classes modulo ideal, *S*-polynomial reduction**

INFORMATION PREPARED FOR _____

_____

Additional Hard or Microfiche Copies Available from

**Technical Information Exchange
Bldg. 5 Room 321, Schenectady, N.Y. 12345**

ON RELATIONSHIP BETWEEN BUCHBERGER'S GROBNER BASIS ALGORITHM AND THE KNUTH-BENDIX COMPLETION PROCEDURE*

A. Kandri-Rody and D. Kapur†

1. Introduction

There has been a surge of interest in term-rewriting systems recently because of many applications of the Knuth-Bendix completion procedure [Knuth and Bendix, '70] as an inference mechanism (see Dershowitz ['83] for a discussion of various applications of the Knuth-Bendix completion procedure). The major motivation for the completion procedure as discussed in the paper by Knuth and Bendix was to develop decision procedures for theories of algebraic structures which can be specified using equations. Once the completion procedure generates a set of rewrite rules which forms a canonical set of rules (meaning that every term can be rewritten to its canonical form using the rewrite rules), proving an equation is equivalent to reducing the two sides of the equation to get their canonical forms and checking whether the canonical forms are identical.

In 1965, Buchberger had developed ideas similar to those discussed in [Knuth and Bendix, '70] in a restricted framework of simplifying polynomials and deciding polynomial equivalence [Buchberger '65, quoted in Buchberger '76]. Polynomial simplification with respect to a set of relations defining an ideal can be viewed as a way to reduce polynomials using certain polynomials in the ideal as rewrite rules. Showing polynomial equivalence can then be considered as proving an equation. Based on these insights, Buchberger developed an algorithm for computing the Grobner basis of a finitely generated ideal in a polynomial ring over the field of rationals; if the polynomials in the Grobner basis are used as rewrite rules, then every polynomial in the polynomial ring over rationals has a canonical form. Buchberger's algorithm is considered to be similar to the Knuth-Bendix completion procedure for term rewriting systems [Buchberger '80]. Demonstrating a direct relationship between Buchberger's algorithm and the Knuth-Bendix procedure has been an open problem [Buchberger and Loos '82]. In this paper, we show this relationship which is demonstrated by developing a general framework for combining reduction with simplification over term rewriting systems.

---

* Some of the results reported in this paper will appear in A. Kandri-Rody's doctoral dissertation at RPI, Troy, NY.

† Partially supported by NSF grant MCS-82-11621.

Manuscript received November 29, 1983

Buchberger and Loos ('82) discuss the difficulty in relating the Grobner basis algorithm and the Knuth-Bendix completion procedure. They point out that the main problem is due to the lack of the compatibility property of the reduction relation on polynomials over rationals, where compatibility property is defined as:

$$t_1 \rightarrow t_2 \Rightarrow s[o/t_1] \rightarrow s[o/t_2],$$

where o is a position [Guttag et al., '83] of a monomial in s and $s[o/t_1]$ is the result of replacing the monomial at position o in s by t_1. The polynomial reduction relation is defined to work on polynomials in simplified form obtained after applying the operations (such as + and *) on rationals. In the case of the Knuth-Bendix completion procedure for term rewriting systems, the proof of the lemma that critical pairs of rules generated in the procedure reduce to the same normal form imply local confluence (Knuth and Bendix, 1970), uses the compatibility property of the reduction relation.

For polynomial reduction relation, however, we only have the semi-compatibility property defined as:

$t_1 \rightarrow t_2 \Rightarrow s[o/t_1]$ and $s[o/t_2]$ converge under $\rightarrow$ to a common polynomial s'.

For example, let us assume that we have $3\ x^2 \rightarrow y$ and s is $6\ x^2 - z$, if we replace the monomial z in $6\ x^2 - z$ by $3\ x^2$, we have $6\ x^2 - 3\ x^2$, whose simplified form is $3\ x^2$ which does not reduce to $6\ x^2 - y$; however both $3\ x^2$ and $6\ x^2 - y$ do reduce to y.

In our approach, we decompose the polynomial reduction relation into two independent parts: reduction and simplification. We impose certain restrictions on these relations by introducing the concept of orthogonal relations in which a simplification relation does not affect a reduction relation; this is precisely characterized in the paper. The simplification relation for polynomials over rationals includes only rules describing the operations on rationals, in particular the rules describing + on a positive rational and a negative rational; in this way, the reduction relation does not have the problem mentioned above and satisfies the compatibility property.

We show in a general framework, independent of polynomial reduction, that the canonicalization obtained after combining reduction and simplification such that simplification is performed before every step of reduction (as it is done in Buchberger's Grobner basis algorithm, for example) is the same as the canonicalization obtained if reduction is completely performed first, followed by simplification at the end. We develop conditions for a generalized version of the Knuth-Bendix completion procedure with reduction and simplification. Then we show the equivalence of two versions of the Grobner basis computation algorithm, namely the one discussed in this paper in which simplification is performed all the way to the end of the reduction — the version which turns out to be simpler to prove correct as it is an instance of the generalized Knuth-Bendix completion procedure — and the more efficient version used for implementation and discussed by Buchberger ['76] in which the simplification is performed at every step of reduction.

The results reported in the paper are based on the idea that although the simplification is useful for implementation purposes, it is better for conceptual purposes to work with representations which may not necessarily be simplified until the result needs to be obtained. This idea of separating a reduction relation from simplification process turns out to be helpful in developing the Grobner basis algorithm for polynomials over Z, $Z[i]$, $Q[i]$, etc. These extensions are discussed in another paper [Kandri-Rody and Kapur].

In the next section, we first review the definitions of a ring, polynomial ring, ideal, and canonical form of a polynomial. Later we discuss how a polynomial can be viewed as a rewrite rule. We define the rewriting relation on polynomials induced by a finite set of polynomials. We then review the definition of a Grobner basis for an ideal.

In Section 3, we introduce basic definitions and concepts relating to reduction relations. We define the orthogonality conditions for simplification with respect to reduction. We show how under such conditions, simplification all the way at the end of reduction produces the same results as doing simplification before every step of reduction. The discussion in this section is general and can be useful in other areas also, in particular theorem proving applications.

In Section 4, we apply the results of Section 3 to polynomial simplification. We discuss a Grobner basis algorithm over polynomials over Q, which is equivalent to the Buchberger's algorithm. We show how this algorithm is an instantiation of the generalized Knuth-Bendix completion procedure.

2. Polynomial Ring, Ideal, Polynomials as Rules, and Grobner Basis

We first give basic definitions (see van der Waerdan or any book on algebra).

A ring R with two binary operations $+$ and $*$ is: (i) a commutative group with respect to $+$ along with unary operation $-$ as the inverse of an element with respect to $+$ and 0 as the identity with respect to $+$ such that (ii) $*$ is associative and distributes over $+$ on the left as well as on the right.

R is commutative if $*$ is commutative. A commutative ring R is a field if and only if every element other than 0 has an inverse with respect to $*$. Q, the set of rationals, is a field for instance, whereas Z, the set of integers, is not a field because the inverse with respect to $*$ is not defined in Z.

An ideal I of a ring R is a subset of R such that: (i) for every a, b in I, $a + (-\mathrm{b})$ is also in I, and (ii) for every a in I, every c in R, $a * c$ is in I. An ideal I generated by a finite set of elements $\{a_1, ..., a_k\}$ is the smallest subset of R such that each a_i is in I and the above two properties hold. An equivalent definition of an ideal I generated by $\{a_1, ..., a_k\}$ is the smallest subset of R such that for every $b_1, ..., b_k$ in R, $a_1 * b_1 + ... + a_k * b_k$ is in I. An ideal I has a finite basis if and only if it can be generated by a finite subset of I.

Let $F[x_1, ..., x_n]$ be the polynomial ring over indeterminates $x_1, ..., x_n$ such that the coefficients of terms in a polynomial are taken from a field F.

2.1 Standard Form for Polynomials in a Polynomial Ring

Most of the terminology and notation used in this subsection is either borrowed from Buchberger and Loos ['82] or is an extension of their terminology and notation.

A term in the context of polynomials is any product of indeterminates with possible repetition, for example, $x_1^2 * x_5 * x_3^4$, which is an abbreviation of $x_1\ x_1\ x_5\ x_3\ x_3\ x_3\ x_3$, is a term ($*$ is often omitted); 1 is also considered a term. The degree of a term is the number of times indeterminates appear in it, for example, the degree of the above term is 7; the degree of 1 is 0.

In order to get polynomials in a standard form of sum of products (also called distributive normal form in the literature on computer algebra), we will assume a total ordering on the set $\{x_1, ..., x_n\}$ of indeterminates. Since any term t can be viewed as a sequence over $\{x_1, ..., x_n\}$, we can sort it in nondescending order using the total ordering on indeterminates as $*$ is both associative and commutative. Sorting enables collecting same indeterminates and expressing the term succinctly using power notation. A total ordering on $\{x_1, ..., x_n\}$ induces a total ordering on terms based on their degree as follows:

By a sorted term t_1, we mean $t_1 = y_1 \ldots y_{k_1}$ such that for $1 \leqslant i < k_1$, $y_i \leqslant y_{i+1}$ and the degree of $t_1 = k_1$. Given two sorted terms $t_1 = y_1 \ldots y_{k_1}$ and $t_2 = z_1 \ldots z_{k_2}$, $t_1 < t_2$ if and only if either: (i) $k_1 < k_2$ or (ii) if $k_1 = k_2$, then there is an $i \leqslant k_1$ such that for every $j < i$, $y_j = z_j$ but $y_i < z_i$. And, two sorted terms $t_1 \leqslant t_2$ if and only if $t_1 < t_2$ or $t_1 = t_2$.

The above ordering on sorted terms is used to order two arbitrary terms s and t as follows: Let sort(s) be the term obtained from s after sorting it. Then $s \leqslant t$ if and only if sort(s) $\leqslant$ sort(t).

The above ordering on terms is based on the degree of terms and lexicographic ordering on terms of the same degree. Any other total ordering on terms would also do; another total ordering for example is pure lexicographic ordering based on a total ordering on indeterminates in which the degree of terms is not considered.

Given two monomials (polynomials with a single term) $m_1 = c_1\ t_1$ and $m_2 = c_2\ t_2$, $m_1 > m_2$ if and only if $t_1 > t_2$.

A polynomial can be brought to its standard form using the associative, commutative and distributive laws of the polynomial ring. A polynomial p in standard form is said to be in simplified form if and only if each of the monomials in it have different terms. For certain applications, it is useful to require of the simplified form that the monomials in a simplified polynomial appear in descending order; in that case, if $p = m_1 + m_2 + \ldots + m_k$ is in the simplified form, then $m_1 > m_2 > \ldots > m_k$. The monomial m_1 of p is called the head monomial, the term of m_1 is called the head term of p and the coefficient of m_1 is called the head coefficient of p.

2.2 Polynomials as Reduction Rules

Let E be a finite set of polynomials in $F[x_1, ..., x_n]$, say $\{p_1, ..., p_k\}$. The ideal I generated by E is the set of all polynomials p such that

$$p = f_1 * p_1 + ... + f_k * p_k ,$$

where $f_1, ..., f_k$ are in $F[x_1, ..., x_n]$.

Depending upon the algebraic structure from which the coefficients of terms in a polynomial are picked, reduction rules corresponding to polynomials in an ideal are defined accordingly. Only polynomials in simplified form have a corresponding reduction rule; for other polynomials, the corresponding reduction rule is assumed to be ill-defined.

The reduction (or rewriting) relation induced by a finite set of polynomials is the union over the rewriting relations defined by the rule corresponding to each polynomial in the set. In addition, axioms of the polynomial ring are either included as part of the reduction relation or as part of the simplification relation as discussed later to ensure certain properties.

Let $p = m_1 + ... + m_k$ be a polynomial in the simplified standard form such that m_1 is its head monomial and the term of m_1 is not a term of any other monomial in p. (It is sufficient to require that p be in standard form and all coefficients of its head term are collected together.) The polynomial p defines a rewrite rule

$$c_1\ t_1 \rightarrow (-m_2) + ... + (-m_k), \qquad (*)$$

where $m_1 = c_1 * t_1$ and $c_1 \neq 0$.

Since the coefficients are taken from a field F, in which $/$, the inverse of $*$, is defined for nonzero elements, then the rewrite rules corresponding to simplified polynomials can be further simplified by making the left-hand side (lhs) of a rewrite rule to be a term by dividing the whole rule by c_1. The rule corresponding to the polynomial p above $(*)$ in that case is:

$$t_1 \rightarrow -\ m_2/\ c_1 + ... + -\ m_k/\ c_1.$$

Buchberger's algorithm which is defined for a polynomial ring over a field, uses such polynomials as rewrite rules [Buchberger and Loos, '82]. Henceforth, we will assume that the rules corresponding to polynomials over a field are in this form, i.e., their lhs is always a monomial with the coefficient 1.

The rewriting relation induced by a simplified polynomial on polynomials over a field is defined as follows: Let q be any polynomial such that q contains a term t with coefficient c_1' such that $t = \sigma * t_1$, where σ is a term, i.e., $q = q_1 + c'_1\ \sigma\ t_1 + q_2$. The polynomial q is rewritten by the rule corresponding to the polynomial p as:

$$q \rightarrow q_1 + c_1' * \sigma * (-\ m_2/\ c_1) + ... + c_1' * \sigma * (-\ m_k/\ c_1) + q_2.$$

Note that a term t with coefficient c_1', which is being rewritten using the rule of p, completely disappears from the result of rewriting. By definition, for any rule $l \rightarrow r$ corresponding to a simplified polynomial p, r only has monomials with terms less than l in the ordering on monomials; so the rewriting due to polynomials is always guaranteed to terminate.

For example, consider the ideal I generated by the basis

$$\{2\ x^2\ y - y,\ 3\ x\ y^2 - x\}.$$

The rules corresponding to the above polynomials are:

$$\{\ x^2\ y \rightarrow 1/2\ y,\ x\ y^2 \rightarrow 1/3\ x\ \}.$$

The polynomial $x^2\ y^2$ can be reduced using the above rules to $1/2\ y^2$.

Besides the rules corresponding to polynomials, the reduction relation also includes rules of the polynomial ring, such as the associativity, commutativity, distributivity and laws of identity, which are used to obtain the standard form of polynomials. The rules or axioms describing the + and * operation on the coefficients taken from the underlying field are not included in the reduction relation; instead these relations are included in a simplification relation as discussed later. So, we have:

$$\begin{aligned}
&t * 1 \rightarrow t \\
&1 * t \rightarrow t \\
&t * 0 \rightarrow 0 \\
&0 * t \rightarrow 0 \qquad \text{(laws of identities)} \\
&t + 0 \rightarrow t \\
&0 + t \rightarrow t
\end{aligned}$$

$$\begin{aligned}
&t_1 * (t_2 * t_3) \rightarrow t_1 * t_2 * t_3 \\
&(t_1 * t_2) * t_3 \rightarrow t_1 * t_2 * t_3 \qquad \text{(flattening)} \\
&t_1 + (t_2 + t_3) \rightarrow t_1 + t_2 + t_3 \\
&(t_1 + t_2) + t_3 \rightarrow t_1 + t_2 + t_3
\end{aligned}$$

$$\begin{aligned}
&(t_1 + t_2) * t_3 \rightarrow t_1 * t_3 + t_2 * t_3 \\
&t_1 * (t_2 + t_3) \rightarrow t_1 * t_2 + t_1 * t_3 \qquad \text{(distributivity)}
\end{aligned}$$

as part of the reduction relation. In addition, by using the ordering information on indeterminates, ground rules (i.e., rules involving only ground terms) can be given to state the commutativity law for * so that we have Noetherianness and we do not have to perform AC-matching, AC-unification and AC-critical pairs which would otherwise be needed because of associative and commutative properties of + and *. For example, if x and y are the two indeterminates for $R[x, y]$ and $x < y$ in the ordering, the rule

$$y * x \rightarrow x * y$$

has the effect of the commutative law. Furthermore, for any element c from F, we have

$$\begin{aligned}
&x * c \rightarrow c * x \\
&y * c \rightarrow c * y\ .
\end{aligned}$$

The rule describing the commutativity of + can also be given if the need be to put monomials in a nonascending order:

$1 + c\ x\ t \rightarrow c\ x\ t + 1$

$1 + c\ y\ t \rightarrow c\ y\ t + 1$

$t_1 + t_2 \rightarrow$ if sort(t_1) and sort (t_2) and $t_1 < t_2$ then $t_2 + t_1$

For our purposes, we do not need to introduce the above rules describing commutativity of + to bring the polynomials in the standard form in which the monomials need not be sorted. So they are not to be included in the reduction relation.

For examples, using the rule $y^2 \rightarrow 2\ x$, the polynomial y^3 can be reduced to $y * 2\ x$ which can be reduced further to $2\ x * y$. But in the polynomial $2\ x + x - 2/3\ x - 1/3 * 6\ y$, the monomial $-1/3 * 6\ y$ cannot be reduced to $-2\ y$ or the subterm $2\ x + x - 2/3\ x$ cannot be reduced to $3\ x - 2/3\ x$ or $7/3\ x$ because as stated above, rules describing the operations on the coefficients are not made part of the reduction relation.

The above approach for treating associative-commutative operators avoids the use of associative-commutative unification and associative-commutative rewriting as stated above. This approach cannot be used in general but has been found applicable in many situations.

2.3 Grobner Basis of an Ideal

A finite set E of polynomials is called a Grobner basis for an ideal I generated by E if for any polynomial q, no matter how q is rewritten using the polynomials in E, the simplified standard form of the result is always the same, i.e., it is unique [Buchberger, '76]. An equivalent definition is that for any polynomial g in the ideal I generated by E,

$g \xrightarrow{*} 0.$

The Grobner basis of an ideal generated by a finite set of polynomials is thus like a canonical rewriting system for an equational theory generated by a finite set of axioms.

For the example discussed above in which the ideal I is generated by the basis

$B = \{2\ x^2\ y - y,\ 3\ x\ y^2 - x\},$

B is not a Grobner basis for I as $x^2\ y^2$ has two normal forms $-1/3\ x^2$ and $1/2\ y^2$. So, the polynomial $x^2\ y^2 + y^2 - x^2$ is in I but cannot be reduced to 0 using B. However,

$B' = \{2\ x^2\ y - y,\ 3\ x\ y^2 - x,\ x^2\ y^2 + y^2 - x^2\}$

is a Grobner basis.

A rule set $T = \{l_1 \rightarrow r_1, ..., l_k \rightarrow r_k\}$ is called reduced if for any i, (i) l_1 is a sorted term, and (ii) neither l_i nor r_i can be reduced using any of the other rules in T or the rules of the

polynomial ring. For examples, B'' below is reduced whereas B''' is not reduced as the lhs of the third rule can be reduced using either of the other two rules.

$$B'' = \{x^2\, y \rightarrow 1/2\, y,\ x\, y^2 \rightarrow 1/3\, x\},$$

and

$$B''' = \{\, x^2\, y \rightarrow 1/2\, y,\ x\, y^2 \rightarrow 1/3\, x,\ x^2\, y^2 \rightarrow x^2 - y^2\}$$

3. Orthogonality of Simplification to Reduction

Most of the terminology about term-rewriting systems in this section is borrowed from either Huet ['80] or Guttag, Kapur, and Musser ['83].

3.1 Noetherian, Confluent, Canonical Rewriting Relations

A relation T (also written as $\rightarrow$) over a set U is called Noetherian (or finitely terminating) if and only if T does not allow any infinite sequence, i.e., there isn't any a in U such that

$$a = a_0 \rightarrow a_1 \rightarrow \ldots\ a_i \rightarrow a_{i+1} \rightarrow \ldots$$

So for a Noetherian T, every element a in U has a normal form, denoted by $\hat{a}$; $\hat{a}$ is also called irreducible with respect to T. However, a could have more than one normal form.

Let $\overset{*}{\rightarrow}$ stand for the reflexive, transitive closure of $\rightarrow$, and $\rightarrow^+$ for the transitive closure of $\rightarrow$.

T is confluent if and only if for any x, y, z such that $x \overset{*}{\rightarrow} y$, $x \overset{*}{\rightarrow} z$, there is a w such that $y \overset{*}{\rightarrow} w$ and $z \overset{*}{\rightarrow} w$. Confluence of T ensures that for any x, if x has a normal form, then the normal form of x is unique.

For a Noetherian T, confluence reduces to a simpler and weaker property which is local in nature, called local confluence. T is locally confluent if and only if for any x, y, z such that $x \rightarrow y$, $x \rightarrow z$, there is a w such that $y \overset{*}{\rightarrow} w$ and $z \overset{*}{\rightarrow} w$.

Proposition 3.1: For a Noetherian T, T is confluent if and only if T is locally confluent.
See Huet ['80] for a proof.

If T is Noetherian and confluent, then T is called canonical.

3.2 Reduction and Simplification

Let T and S be two relations such that T is Noetherian and S is canonical; we shall call T the reduction (or rewriting) relation and S the simplification relation because of the way we use the two relations in the paper. Let $\Rightarrow$ stand for S (and recall that $\rightarrow$ stands for T).

Without any loss of generality, we will assume that $x \Rightarrow y$ if and only if y is the canonical form of x under $\Rightarrow$ so that we do not have to consider the details of the simplification process. If $\Rightarrow$ is canonical modulo an equivalence relation or an equational theory, the definition of orthogonality and results discussed below extend in a straightforward way.

We define two relations:

(i) $\Rightarrow\cdot\rightarrow$, to mean that at every step, first apply $\Rightarrow$ and then apply $\rightarrow$, i.e., $x \Rightarrow\cdot\rightarrow y$ if and only if there is a z such that $x \Rightarrow z$ and (a) $z \rightarrow y$ (b) or if z is irreducible with respect to $\rightarrow$, then $z = y \neq x$, and

(ii) $\rightarrow/\Rightarrow$, to stand for getting a normal form under $\rightarrow$ and then using $\Rightarrow$ at the end, i.e., $x \rightarrow/\Rightarrow y$ if and only if there is a z which is a normal form of x under $\rightarrow$ and (a) $z \Rightarrow y$ or (b) if x is already in normal form, then $x \Rightarrow y$ and $x \neq y$.

Note that if x is already in canonical form under $\Rightarrow$, then $x \Rightarrow x$.

Lemma 3.2: y is in normal form with respect to $\Rightarrow\cdot\rightarrow$ implies that y is in normal form with respect to $\rightarrow$ as well $\Rightarrow$.

Proof: Assume the contrary. If y is not in normal form with respect to $\Rightarrow$, i.e., $y \Rightarrow y'$, where $y' \neq y$, then y is not in normal form with respect to $\Rightarrow\cdot\rightarrow$ either, which is a contradiction. If y is not in normal form with respect to $\rightarrow$ but is in normal form with respect to $\Rightarrow$, i.e., $y \rightarrow y'$, then also, y is not in normal form with respect to $\Rightarrow\cdot\rightarrow$ as $y \Rightarrow\cdot\rightarrow y'$, which is a contradiction. □

The relation $\Rightarrow\cdot\rightarrow$ is used to model what goes on in the version of Grobner basis algorithm proposed by Buchberger ['76], i.e., before every reduction, the simplification is performed. The relation $\rightarrow/\Rightarrow$ on the other hand postpones simplifications all the way to the end.

Note that $\rightarrow/\Rightarrow$ is similar to the relation $\rightarrow/\sim$ defined by Huet (except that $\sim$ is an equivalence relation) and almost confluence property of Thue systems [Book '82, Kapur and Narendran '83]. Above, we require $\Rightarrow$ to be a canonical relation.

Observe that with the stated requirements, neither the relation $\rightarrow/\Rightarrow$ nor the relation $\Rightarrow\cdot\rightarrow$ need to be Noetherian as the following simple example shows:

Example 1:

$\rightarrow$: $a \rightarrow b$ $\qquad U = \{a, b, c\}$
$b \rightarrow c$

$\Rightarrow$: $b \Rightarrow a$

$\rightarrow$ is Noetherian and $\Rightarrow$ is canonical. But $\Rightarrow\cdot\rightarrow$ is not Noetherian because of the following infinite sequence:

$$b \Rightarrow a \rightarrow b \Rightarrow a \rightarrow b \ldots$$

Now, if the rule $b \rightarrow c$ is dropped from example 1, $\rightarrow/\Rightarrow$ is also not Noetherian because of the following infinite sequence:

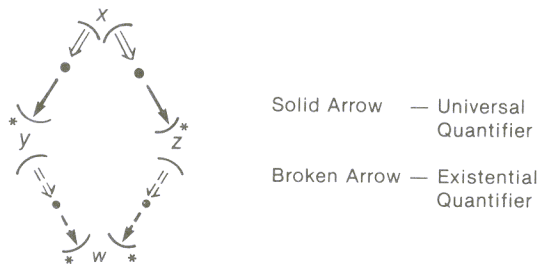
$$a \rightarrow b \Rightarrow a \rightarrow b \Rightarrow a \ldots$$

In fact, for this case, $\rightarrow / \Rightarrow$ and $\Rightarrow \cdot \rightarrow$ are identical. We later introduce a condition on $\rightarrow$ and $\Rightarrow$, called the orthogonality condition, such that if $\Rightarrow$ is orthogonal to $\rightarrow$, then $\rightarrow / \Rightarrow$ as well as $\Rightarrow \cdot \rightarrow$ are Noetherian.

3.3 Reduction Following Simplification at Each Step vs Complete Reduction Then Simplification

In this section, we discuss the relationship between $\Rightarrow \cdot \rightarrow$ and $\rightarrow / \Rightarrow$.

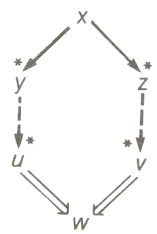
The confluence of $\Rightarrow \cdot \rightarrow$ is defined in the standard way. i.e., for any x, y, z such that $x\ (\Rightarrow \cdot \rightarrow)^*\ y$, $x\ (\Rightarrow \cdot \rightarrow)^*\ z$, there is a w such that $y\ (\Rightarrow \cdot \rightarrow)^*\ w$ and $z\ (\Rightarrow \cdot \rightarrow)^*\ w$. Pictorially,



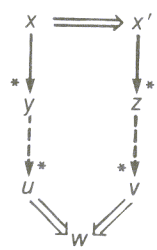
where following Huet ['80], the solid arrow $\rightarrow$ stands for the universal quantifier, and broken arrow $\dashrightarrow$ stands for the existential quantifier.

Below, we define the confluence of $\rightarrow / \Rightarrow$ whose definition is patterned after definitions given in Huet ['80] and Kapur and Narendran.['83].

Definition: $\rightarrow / \Rightarrow$ is confluent if and only if (i) for all x, y, z, $x \overset{*}{\rightarrow} y$, and $x \overset{*}{\rightarrow} z$, there exist u, v, w, such that $y \overset{*}{\rightarrow} u$, $z \overset{*}{\rightarrow} v$, and $u \Rightarrow w$ and $v \Rightarrow w$. Pictorially,



(ii) for all x, x', y, z, $x \Rightarrow x'$, $x \overset{*}{\rightarrow} y$, $x' \overset{*}{\rightarrow} z$, there exist u, v, w such that $y \overset{*}{\rightarrow} u$, $z \overset{*}{\rightarrow} v$, and $u \Rightarrow w$ and $v \Rightarrow w$. Pictorially, we have



The following lemma states another characterization of the confluence of $\rightarrow / \Rightarrow$.

Lemma 3.3: $\rightarrow / \Rightarrow$ is confluent if and only if (i) for every x, y, z, such that $x \stackrel{*}{\rightarrow} y$, $x \stackrel{*}{\rightarrow} z$, and y and z are in normal form with respect to $\rightarrow$, there is a w such that $y \Rightarrow w$ and $z \Rightarrow w$, and (ii) for every x, x', y, z such that $x \Rightarrow x'$, $x \stackrel{*}{\rightarrow} y$ and $x' \stackrel{*}{\rightarrow} z$, and y and z are in normal form, there is a w such that $y \Rightarrow w$ and $z \Rightarrow w$.

Proof: Direct application of the above definition. □

The following is yet another characterization of the confluence of $\rightarrow / \Rightarrow$ which is helpful in relating $\rightarrow / \Rightarrow$ to $\Rightarrow \cdot \rightarrow$.

Theorem 3.4: $\rightarrow / \Rightarrow$ is confluent if and only if for all x, y such that $x\ (\Rightarrow \cdot \rightarrow)^* y$, for all u, v such that u and v are normal forms of x and y repectively with respect to $\rightarrow$, there exists w such that $u \Rightarrow w$ and $v \Rightarrow w$.

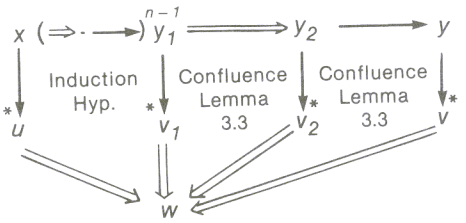
Proof: (a) ($\Leftarrow$) Need to show the two conditions in Lemma 3.3 above for $\rightarrow / \Rightarrow$ to be confluent: (i) Taking $x = y$ ensures the first condition for confluence. (ii) We need to show that for any x, x' such that $x \Rightarrow x'$, for any u, v in normal forms, such that $x \stackrel{*}{\rightarrow} u$ and $x' \stackrel{*}{\rightarrow} v$, there is a w such that $u \Rightarrow w$ and $v \Rightarrow w$.

Either x' is already in normal form with respect to $\rightarrow$, i.e., $x' = v$ or there is a x'' such that $x' \rightarrow x''$. In the former case, $x \Rightarrow \cdot \rightarrow x'$ and in the latter case, $x \Rightarrow \cdot \rightarrow x''$. Hence the proof from the antecedent.

(b) ($\Rightarrow$) By induction on n, where $x\ (\Rightarrow \cdot \rightarrow)^n y$.

basis: $n = 0$, immediate from Lemma 3.3.

inductive step: $n > 0$: the proof is depicted in the following diagram.



□

Theorem 3.6 below establishes that if $\rightarrow / \Rightarrow$ is confluent, so is $\Rightarrow \cdot \rightarrow$. In order to show that the canonical forms generated by $\Rightarrow \cdot \rightarrow$ and $\rightarrow / \Rightarrow$ are the same for any term t, thus implying both relations produce the same result, we need the orthogonality condition on $\Rightarrow$ and $\rightarrow$ which ensures that $\Rightarrow \cdot \rightarrow$ and $\rightarrow / \Rightarrow$ are Noetherian. This will be discussed further in the next subsection.

Theorem 3.5: Let $\rightarrow / \Rightarrow$ be confluent. For every x such that its normal form $\hat{x}$ under $\Rightarrow \cdot \rightarrow$ exists, for any normal form y of x under $\rightarrow$, $y \Rightarrow \hat{x}$.

Proof: Assume $x\ (\Rightarrow \cdot \rightarrow)^*\ \hat{x}$. Further $\hat{x}$ is in normal form with respect to $\rightarrow$ and $\Rightarrow$. By Theorem 3.4, there is a w such that $y \Rightarrow w$ and $\hat{x} \Rightarrow w$. But $\hat{x}$ is already in normal form with respect to $\Rightarrow$, so $y \Rightarrow \hat{x} = w$. □

Theorem 3.6: If $\rightarrow / \Rightarrow$ is confluent, then $\Rightarrow \cdot \rightarrow$ is confluent.

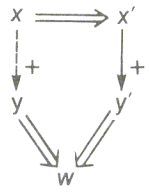
Proof: By the previous theorem, if x has a normal form, say w, under $\Rightarrow \cdot \rightarrow$, then for every normal form y of x under $\rightarrow$, $y \Rightarrow w$. If x has more than one normal form under $\Rightarrow \cdot \rightarrow$, say w_1 and w_2, then $y \Rightarrow w_1$ and $y \Rightarrow w_2$. Since $\Rightarrow$ is canonical, we have $w_1 = w_2$. Hence, $\Rightarrow \cdot \rightarrow$ is confluent. □

Theorem 3.6 states that to show the confluence of $\Rightarrow \cdot \rightarrow$, it is sufficient to show the confluence of $\rightarrow / \Rightarrow$, whereas Theorem 3.5 ensures that the canonical form under $\rightarrow / \Rightarrow$ is the same as the canonical form under $\Rightarrow \cdot \rightarrow$. The two theorems ensure that for generating canonical forms, the two relations have the same effect.

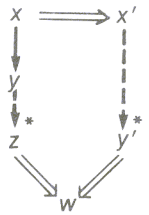
3.4 Orthogonality of Simplification to Reduction

Definition: $S\ (\Rightarrow)$ is orthogonal to $T\ (\Rightarrow)$ if and only if for every x, x' such that $x \Rightarrow x'$,

(i) for every y' such that $x' \rightarrow^+ y'$, there exist y, and w such that $x \rightarrow^+ y$ and $y \Rightarrow w$ and $y' \Rightarrow w$; pictorially, we have



(ii) for every y such that $x \rightarrow y$ there is a z, y', w such that $y \rightarrow^* z$, $x' \rightarrow^* y'$, $z \Rightarrow w$ and $y' \Rightarrow w$; pictorially, we have



The definition of orthogonality roughly states the following requirement: simplifying an element first and then reducing it would get the same simplified result as if the element is reduced first and then simplified. It is precisely to ensure this property of simplification to reduction that every law of the polynomial ring (such as associativity, commutativity, distributivity, etc., of polynomial operations) are considered as part of the reduction relation whereas the relations specifying the + and * operations on coefficients taken from a field are considered as part of the simplification relation. (It is only necessary to include the relation $m - m = 0$ for any monomial m in the simplification relation $\Rightarrow$; every other relation can be included in the reduction relation $\rightarrow$.)

From the definition of orthogonality, we have the following which states that once a term is in a normal form with respect to $\rightarrow$, simplifications by $\Rightarrow$ cannot bring into a position so that the reductions in $\rightarrow$ can be performed again.

Lemma 3.7: If $\Rightarrow$ is orthogonal to $\rightarrow$, and if $t_1 \Rightarrow t_2$ and $t_2 \rightarrow t_3$, then t_1 can be reduced using $\rightarrow$.

Proof: Obvious from the definition. □

Lemma 3.8: If $\Rightarrow$ is orthogonal to $\rightarrow$, then $\rightarrow / \Rightarrow$, $\Rightarrow \cdot \rightarrow$ as well as $\rightarrow^+ \cup (\rightarrow^+ \cdot \Rightarrow)$ are Noetherian.

Proof: That $\rightarrow / \Rightarrow$ is Noetherian is immediate from Lemma 3.7 (as if an element x is irreducible with respect to $\rightarrow$, then its simplified form x' (i.e., $x \Rightarrow x'$) is also irreducible with respect to $\rightarrow$.)

We show that $\Rightarrow \cdot \rightarrow$ is Noetherian by contradiction. Let us assume there is an infinite sequence

$$x_0 \Rightarrow \cdot \rightarrow x_1 \Rightarrow \cdot \rightarrow x_2 \Rightarrow \cdot \rightarrow x_3 \cdots$$

Let us assume that for every $x_i \Rightarrow \cdot \rightarrow x_{i+1}$, we have $x_i \Rightarrow y_i \rightarrow x_{i+1}$. Note that we cannot have $y_i = x_{i+1}$ for all $i > j$ as otherwise, we will not be able to construct an infinite sequence. So, we have

$$x_0 \Rightarrow y_0 \rightarrow x_1 \Rightarrow y_1 \rightarrow x_2 \Rightarrow y_2 \rightarrow x_3 \cdots$$

Using the fact that $\Rightarrow$ is orthogonal to $\rightarrow$, we can construct another sequence from the above sequence

$$x_0 \rightarrow^+ z_0 \Rightarrow y_1 \rightarrow x_2 \Rightarrow y_2 \rightarrow x_3 \cdots$$

$$x_0 \rightarrow^+ z_0 \rightarrow^+ z_1 \Rightarrow y_2 \rightarrow x_3 \cdots$$

$$\vdots$$

This way, we can get an infinite sequence in $\rightarrow$, which is a contradiction as $\rightarrow$ is Noetherian. So, $\Rightarrow \cdot \rightarrow$ is Noetherian.

A proof similar to the proof of Noetherianness of $\Rightarrow \cdot \rightarrow$ shows that $\rightarrow^+ . \Rightarrow$ is also Noetherian.

$$x_0 \rightarrow^+ y_0 \Rightarrow x_1 \rightarrow^+ y_1 \Rightarrow x_2 \rightarrow^+ y_3 \Rightarrow x_3 \ldots$$

By orthogonality of $\Rightarrow$ to $\rightarrow$, we get

$$x_0 \rightarrow^+ y_0 \rightarrow^+ z_0 \Rightarrow x_2 \rightarrow^+ y_3 \Rightarrow x_3 \ldots$$

$$x_0 \rightarrow^+ y_0 \rightarrow^+ z_0 \rightarrow^+ z_1 \Rightarrow x_3 \ldots$$

$$\vdots$$

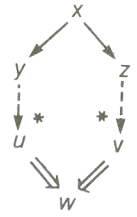
which again gives an infinite sequence in $\rightarrow$ if there is an infinite sequence in $\rightarrow^+ . \Rightarrow$. Hence the proof. □

3.5 Showing Confluence of $\rightarrow / \Rightarrow$

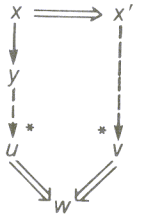
If $\Rightarrow$ is orthogonal to $\rightarrow$, the test for confluence reduces to a local test based on the local confluence property. The local confluence of $\rightarrow / \Rightarrow$ can be defined as follows:

Definition: $\rightarrow / \Rightarrow$ is locally confluent if and only if

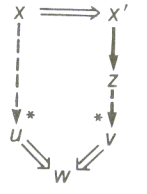
(i) for all $x, y, z, x \rightarrow y$ and $x \rightarrow z$ there exist u, v, w, such that $y \rightarrow^* u$, $z \rightarrow^* v$, and $u \Rightarrow w$ and $v \Rightarrow w$,



(ii) (a) for all $x, x', y, x \Rightarrow x', x \rightarrow y$, there exist u, v, w such that $y \rightarrow^* u$, $x' \rightarrow^* v$, and $u \Rightarrow w$ and $v \Rightarrow w$.



(b) for all $x, x', z, x \Rightarrow x', x' \rightarrow z$, there exist u, v, w such that $x \rightarrow^* u$, $z \rightarrow^* v$, and $u \Rightarrow w$ and $v \Rightarrow w$.



The following theorem establishes the desired relation between confluence and local confluence.

Theorem 3.9: If $\Rightarrow$ is orthogonal to $\rightarrow$, then, $\rightarrow/\Rightarrow$ is confluent if and only if $\rightarrow/\Rightarrow$ is locally confluent.

Proof: Similar to the proof of Lemma 2.7 in Huet ['80]. See the Appendix. □

The local confluence of $\rightarrow/\Rightarrow$ can be ensured by appropriately defining the critical pairs when $\rightarrow$ and $\Rightarrow$ are defined by rewrite rules. The second condition of the local confluence is implied by the orthogonality condition on $\rightarrow$ and $\Rightarrow$.

4. Buchberger's Algorithm and the Knuth-Bendix Completion Procedure

Let $T = \{l_1 \rightarrow r_1, ..., l_k \rightarrow r_k\}$ be the rule set corresponding to a finite basis $\{p_1, ..., p_k\}$ of an ideal I such that $\{l_i \rightarrow r_i\}$ be the rule corresponding to p_i. As stated in Section 2, in addition to the rules corresponding to polynomials in I, rules for the associativity, commutativity and distributivity of $*$ and $+$ on polynomials using the ordering defined in Section 2 are also made part of the reduction $\rightarrow$. The relations specifying the application of $+$ and $*$ on the coefficients of terms in polynomials is however considered as part of the simplification relation $\Rightarrow$. This separation is done to have the compatibility property of the relation $\rightarrow$ for $F[x_1, ..., x_n]$. Note that it is sufficient to rule out the application of $-$ operation on coefficients from the reduction relation for ensuring compatibility.

For example in case of $Q[x, y]$, $p = y + 3\ x - y + 2\ x \rightarrow y - y + 3\ x + 2\ x$ but not $5\ x$.

We now show that the reduction relation $\rightarrow$ is Noetherian and that the simplification relation $\Rightarrow$ is orthogonal to $\rightarrow$. It is easy to see that the simplification relation $\Rightarrow$ always gives a unique normal form for any polynomial under $\Rightarrow$.

The associative, commutative and distributive rules in $\rightarrow$ are applied so as to bring a polynomial to the standard form (the sum of products form such that the indeterminates in each of the monomials are ordered); this part of the reduction relation terminates. As for the part of the reduction relation induced by the polynomials in I, since for every rule corresponding to a polynomial p in I, its rhs has terms less than the term of the lhs, any polynomial q when rewritten using the rules corresponding to polynomials in I, will eventually have terms that cannot be rewritten by the lhs of any rule.

Furthermore, for any polynomial p in normal form under $\rightarrow$, if p' is the simplification of p, i.e., $p \Rightarrow p'$, then p' is included in (or a part of) p (in other words, every term in p' is also in p with possibly different coefficients) as the simplification involves the application of $+$, $-$, $*$ and $/$ over coefficients of terms.

Theorem 4.10: $\Rightarrow$ over $F[x_1, ..., x_n]$ is orthogonal to $\rightarrow$ over $F[x_1, ..., x_n]$.

Proof: For any p, p', $p \Rightarrow p'$, we must show that (i) for every q' such that $p' \rightarrow^+ q'$, there exist q, r' and w such that $p \rightarrow^+ q$, $q' \rightarrow^* r'$ and $q \Rightarrow w$ and $r' \Rightarrow w$, and (ii) for every q such that $p \rightarrow q$ there is an r, q', w such that $q \rightarrow^* r$, $p' \rightarrow^* q'$, $r \Rightarrow w$ and $q' \Rightarrow w$.

For condition (i), let us first consider the case when q' is a mere rearrangement of a p' using a rule of the polynomial ring. Since all terms in p' appear in p, corresponding to a part of p' that is rearranged to get q', there is a part p_1 in p; the same rule that reduces p' to q' can be applied on p_1. By many applications of this rule and possibly other rules of the ring we get the desired q from p. The second case is when q' is obtained from p' by the application of a rule corresponding to a polynomial, to a monomial $m = c_1 \sigma t$ in p', $c_1 \neq 0$. Let the rule be $t \rightarrow r$. Then that rule can be applied on monomials in p whose summation is m to get the desired q.

By a similar case analysis, it can be shown that the condition (ii) of the orthogonality property also hold. □

It is obvious that for any p_1, p_2 such that $p_1 \Rightarrow w \Leftarrow p_2$, for any q, $p_1 + q \Rightarrow w' \Leftarrow (p_2 + q)$ as well as $(p_1 * q) \Rightarrow w'' \Leftarrow (p_2 * q)$.

Note that the relation $\rightarrow$ has the compatibility property (Huet ['80]):

Lemma 4.11: If $p_1 \rightarrow p_2$, then $p[o/p_1] \rightarrow p[o/p_2]$, where $p[o/p_1]$ stands for replacing whatever is at position o in p by p_1.

Proof: Obvious from the definition of $\rightarrow$ since the relations describing the application of + and * on coefficients are not considered as part of $\rightarrow$. □

In fact, a stronger statement can be made about $\rightarrow$, which is that if $p_1 \rightarrow^n p_2$, then $p[o/p_1] \rightarrow^n p[o/p_2]$. The relation $\Rightarrow \cdot \rightarrow$ does not have the compatibility property because some monomials in p may disappear when p_1 is made part of it and simplification is performed. Instead, $\Rightarrow \cdot \rightarrow$ has a weaker property, called the semi-compatibility property by Buchberger and Loos ['82]. As remarked by Buchberger and Loos, it is the lack of compatibility property which has been a major hurdle in showing any direct relationship between Buchberger's Grobner basis algorithm and the Knuth-Bendix completion procedure. Using $\rightarrow$ instead of $\Rightarrow \cdot \rightarrow$ gets rid of this hurdle. Theorems 3.5 and 3.6 above which relate $\rightarrow / \Rightarrow$ to $\Rightarrow \cdot \rightarrow$, ensure that it is indeed possible to use $\rightarrow / \Rightarrow$ for the purpose of proof and showing relationship between the Grobner basis algorithm and the general Knuth-Bendix algorithm since for the purpose of polynomial simplification, $\rightarrow / \Rightarrow$ and $\Rightarrow \cdot \rightarrow$ generate the same canonical forms.

4.1 Critical Pairs or *S*-Polynomials

To show the local confluence of $\rightarrow / \Rightarrow$, we define critical pairs of pairs of rules as follows:

Given two rules $l_i \rightarrow r_i$ and $l_j \rightarrow r_j$, where both l_i and l_j are terms, a critical pair $<p, q>$ is defined as follows:

$p = f_i * r_i$ and
$q = f_j * r_j$

where $f_i * l_i = f_j * l_j = \text{lcm}(l_i, l_j)$. Polynomials p and q are obtained from the superposition $\text{lcm}(l_i, l_j)$ by applying $l_i \rightarrow r_i$ and $l_j \rightarrow r_j$ respectively. The above definition is the same as of Buchberger ['76] where $q - p$ is called an S-polynomial.

The case when $\text{lcm}(l_i, l_j) = l_i\, l_j$, results to p and q such that after applications of rule j to p and rule i to q produces identical terms, so it does not need to be considered. See Buchberger ['79] for conditions under which certain other critical pairs do not have to be considered.

Theorem 4.12: For a reduced T (see subsection 2.3 for definition) such that $\Rightarrow$ is orthogonal to $\rightarrow$, $\rightarrow/\Rightarrow$ is locally confluent if and only if for every critical pair $<p, q>$ for each pair of rules in T, there is an s such that $\text{normalform}(p, \rightarrow) \Rightarrow s$ and $\text{normalform}(q, \rightarrow) \Rightarrow s$.

An alternative statement of the above theorem requires that $\text{normalform}(p - q, \rightarrow) \Rightarrow 0$.

Proof: (i) That local confluence implies for every critical pair $<p, q>$ of rules $l_i \rightarrow r_i$ and $l_j \rightarrow r_j$, p and q have normal forms under $\rightarrow$ which simplify under $\Rightarrow$ to the same element, is immediate from the definition of local confluence. By condition (i) of local confluence, $\text{lcm}(l_i, l_j)$, from which the critical $<p, q>$ is obtained by applying the rules, must have a common normal form after applying $\Rightarrow$.

(ii) To show for every critical pair $<p, q>$, there is an s such that $\text{normalform}(p, \rightarrow) \Rightarrow s$ and $\text{normalform}(q, \rightarrow) \Rightarrow s$, implies local confluence.

The second condition of local confluence is ensured by the property that $\Rightarrow$ is orthogonal to $\rightarrow$. We need to show that for every x, y, z such that $x \rightarrow y$ and $x \rightarrow z$, there is a u, v, and w such that $y \overset{*}{\rightarrow} u$ and $z \overset{*}{\rightarrow} v$ and $u \Rightarrow w$ and $v \Rightarrow w$. The interesting case here is when $x \rightarrow y$ and $x \rightarrow z$ by (not necessarily distinct) rules $l_1 \rightarrow r_1$ and $l_2 \rightarrow r_2$ in T. The remaining cases, which are concerned with the interaction between the rules corresponding to polynomials and rules of the polynomial ring stated in Section 2, are omitted as they are easy to see.

We have $y = x\ [o_1/\sigma_1\ r_1]$, where $x/o_1 = \sigma_1\ l_1$ and σ_1 is a monomial, and $z = x\ [o_2/\sigma_2\ r_2]$, where $x/o_2 = \sigma_2\ l_2$ and σ_2 is a monomial.

There are two cases:

1. o_1 and o_2 are disjoint, i.e., $x = x_1 + x/o_1 + x_2 + x/o_2 + x_3$, where x_1, x_2, x_3 could be empty (i.e., 0).

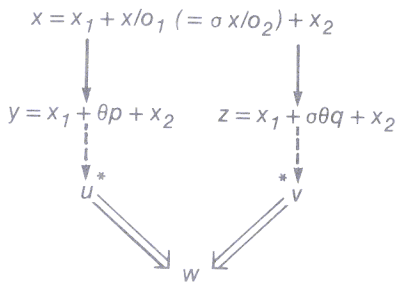
   In this case, y and z can be respectively rewritten in one step to $x_1 + \sigma_1\ r_1 + x_2 + \sigma_2\ r_2 + x_3$, thus establishing the desired condition.

2. $o_1 \leqslant o_2$, i.e., $x = x_1 + x/o_1 + x_2$, where $x/o_1 = \sigma\ x/o_2 = \theta\ \text{lcm}(l_1, l_2)$.

The critical pair $<p, q>$ of $l_1 \rightarrow r_1$ and $l_2 \rightarrow r_2$, where $p = f_1 * r_1$ and $q = f_2 * r_2$ such that $f_1 * l_1 = f_2 * l_2 = \text{lcm}(l_1, l_2)$, have the same normal form under $\rightarrow$ after simplified by $\Rightarrow$.

So, $x/o_1 \rightarrow \theta\ p$ and $\sigma\ x/o_2 \rightarrow \theta\ q$, implying that $\text{normalform}(\theta\ p, \rightarrow)$ and $\text{normalform}(\theta\ q, \rightarrow)$ have a common descendent w_1 because of compatibility property of $\rightarrow$

with respect to $*$. Then, $y \xrightarrow{*} u = x_1 +$ normalform$(\theta\ p, \rightarrow) + x_2$ and $z \xrightarrow{*} v = x_1 +$ normalform$(\theta\ q, \rightarrow) + x_2$ such that $u \Rightarrow w$ and $v \Rightarrow w$.



□

Note that the proof of the above theorem essentially mimics the steps in the proof for the Knuth-Bendix procedure for term rewriting systems as in Huet ['80].

We also obtain from the above theorem, a way to compute the Grobner basis which is an instantiation of the generalized Knuth-Bendix completion procedure for term-rewriting systems. For critical pairs $<p, q>$ such that normalform(p) and normalform(q) do not simplify to the identical polynomial, we add a new rule corresponding to the polynomial $\hat{p} - \hat{q}$, where $\hat{p}$ and $\hat{q}$ are respectively the simplified forms of normal forms of p and q. This process is guaranteed to terminate because of the Noetherian condition of ideals over a Noetherian ring. This version of the Grobner basis algorithm is equivalent to Buchberger's Grobner basis algorithm and as shown above, is an instance of the generalized Knuth-Bendix completion procedure.

5. CONCLUSION

Using a general framework of combining a reduction relation with a simplification relation, we have demonstrated the relationship between the Grobner basis algorithm for ideals in a polynomial ring over rationals and the generalized Knuth-Bendix completion procedure. We have shown that the Grobner basis algorithm is an instance of the general Knuth-Bendix procedure by decomposing the polynomial simplification relation into two orthogonal relations called reduction and simplification. This general framework has been useful in extending the Grobner basis algorithm to an arbitrary Euclidean ring as discussed in another paper [Kandri-Rody and Kapur]. We believe that the approach of combining reduction with simplification with suitable restrictions on them has applications in theorem proving based on rewriting also.

Another plausible approach for establishing relationship between the Grobner Basis algorithm and the generalized Knuth-Bendix completion procedure is to investigate the relationship between the Grobner basis algorithm and the generalized completion procedure discussed by Peterson and Stickel and Lankford and Ballantyne since both $*$ and $+$ are associative and commutative operators.

REFERENCES

[1] Book, R., "Confluent and Other Types of Thue Systems," *JACM*, Vol. 29 No. 1, Jan., 1982, pp. 171-182.

[2] Buchberger, B. "A Theoretical Basis for the Reduction of Polynomials to Canonical Forms," *ACM-SIGSAM Bulletin*, 39, August, 1976, pp. 19-29.

[3] Bachmir, L. and Buchberger, B. "A Simplified Proof of the Characterization Theorem for Grobner-Bases," *ACM-SIGSAM Bulletin*, 14/4, 1980, pp. 29-34.

[4] Buchberger, B., "A Criterion for Detecting Unnecessary Reductions in the Construction of Grobner-Bases," *Proceedings of EUROSAM 79, Marseille,* Springer Verlag Lecture Notes in Computer Science, Vol. 72, 1979, pp. 3-21.

[5] Buchberger, B., and Loos, R., "Algebraic Simplification," in *Computer Algebra: Symbolic and Algebraic Computation.* (Eds. B. Buchberger, G.E. Collins, R. Loos), Computing Suppl. 4, Springer Verlag, New York, 1982, pp. 11-43.

[6] Dershowitz, N., "Applications of the Knuth-Bendix Completion Procedure," Laboratory Operation, Aerospace Corporation, Aerospace Report No. ATR-83(8478)-2, 15 May, 1983.

[7] Guttag, J.V., Kapur, D., Musser, D.R., "On Proving Uniform Termination and Restricted Termination of Term Rewriting Systems," *SIAM Journal of Computing*, Vol. 12 No. 1, Feb., 1983, pp. 189-214.

[8] Huet, G., "Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems," *JACM*, Vol. 27, No. 4, Oct., 1980, pp. 797-821.

[9] Kapur, D., and Narendran, P., "Almost-Confluence and Related Properties of Thue Systems," CRD Report No. CRD83-258, G.E. Research and Development Center, Schenectady, New York, Oct., 1983. Also submitted to *Theoretical Computer Science* for publication.

[10] Kandri-Rody, A. and Kapur, D., "A Practical Algorithm for Computing the Grobner Basis of a Polynomial Ideal over an Euclidean Ring," Unpublished GE CRD Technical Report, Nov. 1983.

[11] Knuth, D.E. and Bendix, P.B., "Simple Word Problems in Universal Algebras," in *Computational Problems in Abstract Algebras.* (ed. J. Leech), Pergamon Press, 1970, pp. 263-297.

[12] Lang, S., *Algebra*, Addison Wesley Publishing Co, New York, 1971.

[13] Lankford, D.S., and Ballantyne, M., *Decision Procedures for Simple Equational Theories with Commutative-Associative Axioms: Complete Sets of Commutative-Associative Reductions* Report ATP-39, University of Texas, Austin, Texas, 1977.

[14] Peterson, G.L., and Stickel, M.E., "Complete Sets of Reductions for Some Equational Theories," *JACM* Vol. 28 No. 2, pp. 233-264, April, 1981.

[15] van der Waerden, B.L., *Modern Algebra*, Vol. I, Fredrick Ungar Publishing Co, New York, 1966.

APPENDIX

Theorem 3.9: If $\Rightarrow$ is orthogonal to $\rightarrow$, then $\rightarrow/\Rightarrow$ is confluent if and only if $\rightarrow/\Rightarrow$ is locally confluent.

Proof: (i) confluence $\Rightarrow$ local confluence: obvious.

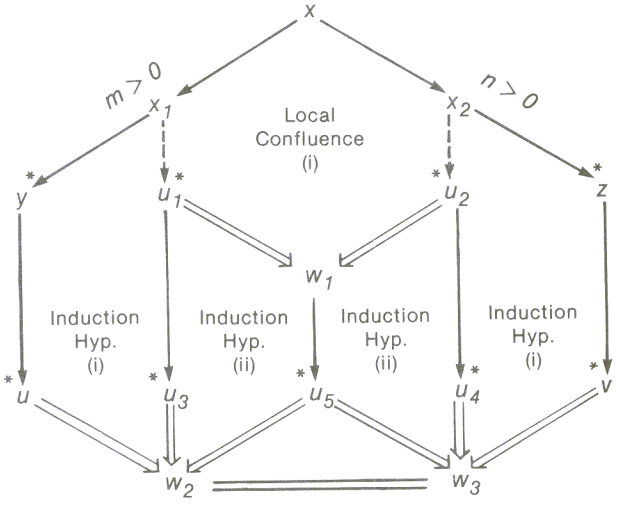
(ii) local confluence $\Rightarrow$ confluence: We will establish the two conditions in the definition of confluence given in subsection 3.3. The proof is by Noetherian induction. We define a relation $RR = \rightarrow^+ U (\rightarrow^+ . \Rightarrow)$ whose termination (Noetherianness) can be shown easily from the Noetherianness of $\rightarrow^+ . \Rightarrow$ (see Lemma 3.8). Using the relation RR, we define a relation $\rightarrow'$ defined of 2-tuples as follows: $<x,x'> \rightarrow' <y,y'>$ if either one of the conditions holds:

(i) $x\ RR\ y,\ x' = y'$,
(ii) $x\ RR\ y, x\ RR\ y'$,
(iii) $x = y, x'\ RR\ y'$, and
(iv) $x'\ RR\ y, x'\ RR\ y'$.

It should be easy to see that $\rightarrow'$ is Noetherian (also see Huet (1980)).

The proofs below are by Noetherian induction using the ordering induced by the relation $\rightarrow'$.

Property (i): Assuming that the two properties of confluence hold for all pairs $<x', y'>$ such that $<x, x> \rightarrow'^+ <x', y'>$, we show that property (i) holds for $<x, x>$. Let $x \rightarrow^* y$ in m steps and $x \rightarrow^* z$ in n steps. When either m is 0 or n is 0, it is easy to see the statement holds. The diagram below establishes for $m > 0$ and $n > 0$.

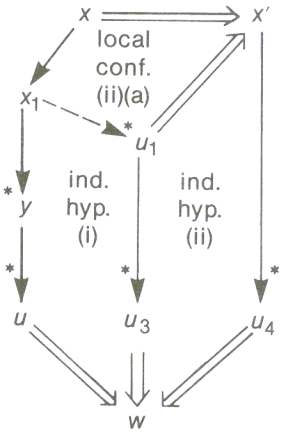


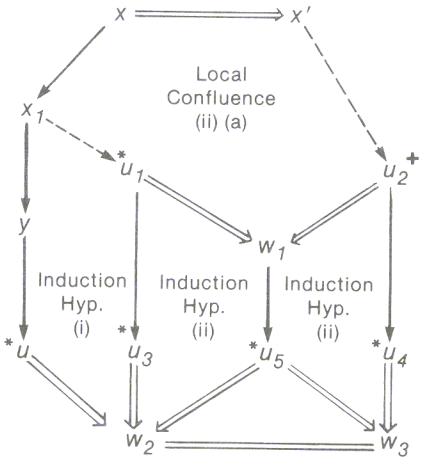
In the diagram, u, u_3, u_4, u_5, v are normal forms of y, u_1, u_2, w_1, and z respectively. w_2 and w_3 are identical as $\Rightarrow$ is canonical. Note that we use inductive hypothesis due to property (i) on pairs $<x_1, x_1>$ and $<x_2, x_2>$, and inductive hypothesis due to property (ii) on pairs $<u_1, w_1>$ and $<u_2, w_1>$.

Property (ii): Consider any x, x', y, z, such that $x \Rightarrow x'$, $x \rightarrow^{*} y$ in m steps and $x' \rightarrow^{*} z$ in n steps. Assuming that the two properties of confluence hold for all pairs $<z_1, z_2>$ such that $<x, x'> \rightarrow'^{+} <z_1, z_2>$, we show that property (ii) holds for $<x, x'>$.

The case of $m = 0$ and $n = 0$ is trivial.

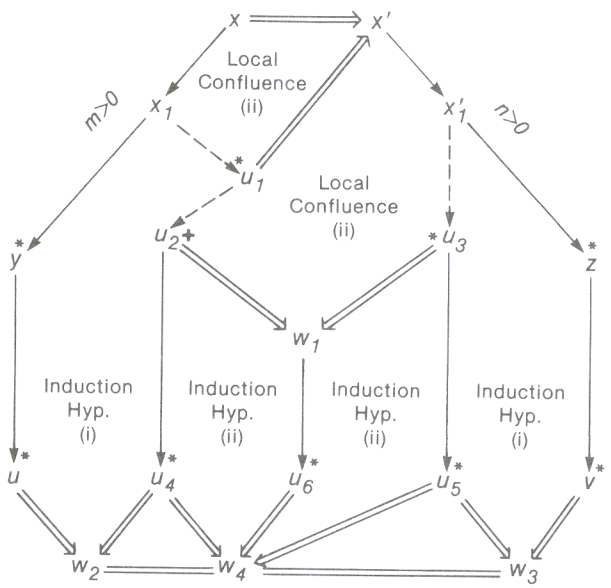
For $n = 0$ and $m > 0$, the property (ii) of confluence is proved using the condition (ii) (a) of local confluence as depicted in the diagrams below. The inductive hypothesis due to property (i) is invoked on $<x_1, x_1>$ and the inductive hypothesis due to property (ii) is invoked on $<u_1, x'>$ in the left diagram and on $<u_1, w_1>$ and $<u_2, w_1>$ in the right diagram. Similarly, for the case $m = 0$ and $n > 0$, the property (ii) of confluence is shown using the condition (ii) (b) of local confluence.

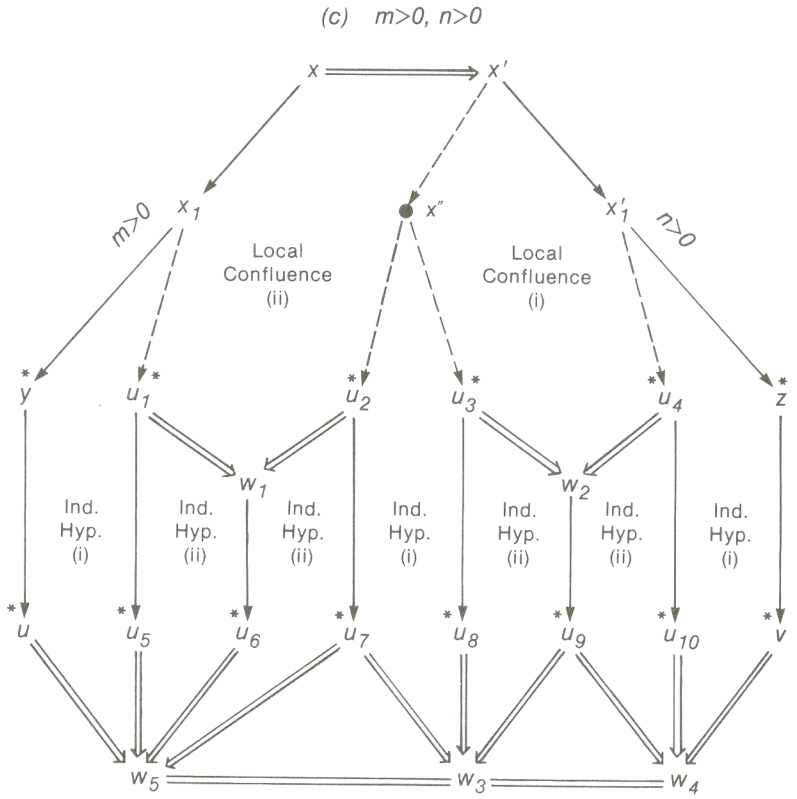




For $m > 0$ and $n > 0$, there are two possibilities based on the second condition of local confluence when we consider $x \Rightarrow x'$ and $x \rightarrow x_1$: there is a u_1 such that $x_1 \rightarrow^{*} u_1$ and (i) $u_1 \Rightarrow x'$, or (ii) there is u_2 such that $x' \rightarrow^{+} u_2$ and $u_1 \Rightarrow w_1$ and $u_2 \Rightarrow w_1$. The proofs are depicted in the diagrams (b) and (c) below.

(b) m>0, n>0





In the diagram (b), u, u_4, u_6, u_5 and v are the normal forms of y, u_2, w_1, u_3 and z respectively, under $\rightarrow$. The inductive hypothesis is invoked on pairs $<x_1, x_1>$, $<u_2, w_1>$, $<u_3, w_1>$, and $<x'_1, x'_1>$.

In the diagram (c), u, u_5, u_6, u_7, u_8, u_9, u_{10} and v are the normal forms of y, u_1, w_1, u_2, u_3, w_2, u_4 and z respectively under $\rightarrow$. The inductive hypothesis is invoked on pairs $<x_1, x_1>$, $<u_1, w_1>$, $<u_2, w_1>$, $<x'', x''>$, $<u_3, w_2>$, $<u_4, w_2>$, and $<x'_1, x'_1>$. □