J. Symbolic Computation (1988) **6**, 37–57

Computing a Gröbner basis of a polynomial ideal over a Euclidean domain

Abdelilah Kandri–Rody†
Department des Mathematiques
Faculte des Sciences
University Cadi Ayyad
Marrakech, Morocco

Deepak Kapur*
Computer Science Branch
General Electric Company
Corporate Research and Development
Schenectady, New York 12345

(Received 30 September 1985)

An algorithm for computing a Gröbner basis of a polynomial ideal over a Euclidean domain is presented. The algorithm takes an ideal specified by a finite set of polynomials as its input; it produces another finite basis of the same ideal with the properties that using this basis, every polynomial in the ideal reduces to 0 and every polynomial in the polynomial ring reduces to a unique normal form. The algorithm is an extension of Buchberger's algorithms for computing Gröbner bases of polynomial ideals over an arbitrary field and over the integers as well as our algorithms for computing Gröbner bases of polynomial ideals over the integers and the Gaussian integers. The algorithm is simpler than other algorithms for polynomial ideals over a Euclidean domain reported in the literature; it is based on a natural way of simplifying polynomials by another polynomial using Euclid's division algorithm on the coefficients in polynomials. The algorithm is illustrated by showing how to compute Gröbner bases for polynomial ideals over the integers, the Gaussian integers as well as over algebraic integers in quadratic number fields admitting a division algorithm. A general theorem exhibiting the uniqueness of a reduced Gröbner basis of an ideal, determined by an admissible ordering on terms (power products) and other conditions, is discussed.

1. Introduction

A general algorithm for computing a Gröbner basis of a polynomial ideal in which the coefficients of monomials in polynomials are taken from a Euclidean domain is presented. Such domains include, for example, the rings of integers, Gaussian integers, univariate polynomials over a field as well as rings of algebraic integers in quadratic fields admitting Euclid's division algorithm (Hardy and Wright, 1938). The algorithm is a generalization of a Gröbner basis algorithm for polynomial ideals over an arbitrary field introduced by Buchberger (1965, 1976a). The algorithm also generalizes our algorithms (Kandri-Rody and Kapur, 1984a; 1984b) for computing Gröbner bases for polynomial ideals over the integers, the Gaussian integers and univariate polynomials over a field as well as Buchberger's algorithm (1984) for polynomial ideals over the integers.

The input to this general algorithm is an ideal specified by a finite set of polynomials; the algorithm produces another finite basis of the ideal which can be used to

† This work was done during the period from May 1983 to May 1984 when Kandri-Rody was a graduate student at Rensselaer Polytechnic Institute, Troy, NY.

* Partially supported by the NSF grant MCS-82-11621.

0747–7171/88/040037+21 $03.00/0

reduce polynomials so that every polynomial in the ideal reduces to 0 and every polynomial in the polynomial ring reduces to a unique normal form. Furthermore, under certain conditions discussed later in the paper, the algorithm produces a unique reduced Gröbner basis of a polynomial ideal, once an ordering on monomials is chosen. An interested reader may wish to refer to a survey article by Buchberger (1985) for applications of a Gröbner basis algorithm as well as a brief introduction to the subject.

The approach adopted in this paper is based on the rewrite rule theory (Huet and Oppen, 1980; Musser and Kapur, 1982), similar to the approaches taken in (Bachmair and Buchberger, 1980; Buchberger and Loos, 1982; Buchberger, 1984). A polynomial ideal can be considered an equational theory; its Gröbner basis is then a complete (canonical) rewriting system when polynomials are viewed as rewrite rules, which can be used to generate canonical forms for residue classes defined by the ideal on a polynomial ring. In this approach, polynomials are simplified (reduced) using a single polynomial at a time. New polynomials (called *S-polynomials* by Buchberger) added to *complete* a basis are computed between pairs of polynomial in the basis; the concept of S-polynomials is closely related to the concept of critical pairs between rules in a term rewriting system as pointed out in (Buchberger and Loos, 1982; Kandri-Rody and Kapur, 1983).

The proposed algorithm differs from more general algorithms reported in the literature (Shtokhamer, 1976; Trinks, 1978; Zacharias, 1978; Schaller, 1979) for Noetherian rings with certain conditions in the way reduction and S-polynomials are defined. In this paper, the notion of reduction of polynomials with respect to a polynomial is defined in a natural way using a division algorithm over a Euclidean domain. The definition of S-polynomials is also simpler and more natural than in more general algorithms; see the subsection on related work for comparison. Because of these difference, a Gröbner basis generated by the proposed algorithm is different from those generated by more general algorithms.

The paper is organized as follows: the next subsection gives an overview of related work in the subject. Section 2 gives preliminary definitions; a well-founded ordering on polynomials is defined using a well-founded ordering on the elements of a Euclidean domain. Section 3 defines the rewriting relation induced by a polynomial using a division algorithm over a Euclidean domain. The termination of rewriting is shown using the well-founded ordering defined in the previous section. Further, it is shown that the rewriting relation is strong enough in the sense that the reflexive, symmetric and transitive closure of the rewriting relation induced by a finite set of polynomials is the same as the congruence relation induced by the ideal generated by the finite set of polynomials.

A Gröbner basis of an ideal is defined using this rewriting relation in Section 4. A test for a Gröbner basis is developed by defining critical pairs between a pair of polynomials viewed as rewrite rules. Section 5 describes an algorithm for generating a Gröbner basis from any basis of a polynomial ideal. The algorithm is illustrated using examples over Z, $Z[i]$ (Gaussian integers), $Q[s]$, as well as algebraic integers in quadratic fields $Q[\sqrt{-3}]$ and $Q[\sqrt{2}]$ in Section 6. A particular instance of this algorithm over Z has been implemented in ALDES (Collins, 1968; Loos, 1974) and LISP, and experimented with on a number of examples using different strategies for choosing critical pairs, normalization and ordering on polynomials; an interested reader may refer to (Kandri-Rody and Kapur, 1984b; Kandri-Rody, Kapur and Narendran, 1985) for

examples. Section 7 outlines extensions of the algorithm to other structures. Section 8 discusses additional properties needed of a Euclidean domain which result in the proposed algorithm generating a unique reduced Gröbner basis of a polynomial ideal (subject to an admissible term ordering and an ordering on a Euclidean domain).

Proofs of most of the lemmas and theorems have been omitted from this paper as their structure closely resembles the structure of the proofs of related lemmas and theorems in (Bachmair and Buchberger, 1980). An interested reader can find the proofs in an expanded version of this paper (Kandri-Rody and Kapur, 1984c).

1.1 Related Work

Szekeres (1952) showed the existence of a canonical basis for an ideal generated by a finite set of polynomials in $Z[x]$. Independently, in 1964, Buchberger introduced the concept of a Gröbner bases for a polynomial ideal over a field; for some earlier related work, the reader may consult (Buchberger, 1985). Shtokhamer (1976) developed a generalization of the construction suggested by Szekeres to define a canonical basis for polynomial ideals over a principal ideal domain; see also (Shtokhamer, 1986). Richman (1974) gave a totally different treatment of related concepts.

Lauer (1976a) attempted to relate Shtokhamer's results and Buchberger's algorithm. He also developed an algorithm for polynomial ideals over the integers which could be generalized to polynomial ideals over a Euclidean domain (1976b). His algorithm and a version of an algorithm presented in Section 5.1 of this paper are closely related. Buchberger's work was also extended by Trinks (1978), Zacharias (1978) and Schaller (1979), who proposed closely related approaches to generating Gröbner bases for polynomial ideals over general Noetherian rings satisfying certain conditions.

In contrast to Buchberger's approach in which a single polynomial is used to reduce other polynomials and new polynomials to complete a basis are generated by considering pairs of polynomials, approaches proposed by Shtokhamer, Trinks, Zacharias and Schaller used finite subsets of polynomials in a basis for reduction as well as for generating new polynomials to be added to the basis. As a result, reduction as well as the method of generating new polynomials in their approaches are quite complex. In order to perform these computations, one needs to solve linear nonhomogeneous equations over the ground ring as well as compute a basis for syzygies over the ground ring. Further, Shtokhamer's algorithm is recursive in nature, considering one indeterminate at a time; in that sense, it computes Gröbner bases with respect to a lexicographic ordering on terms. In these respects, their algorithms are not in the spirit of Buchberger's algorithm; see also (Buchberger, 1984; 1985) for comments on differences between their approaches and the approaches based on rewriting techniques.

Following Buchberger's approach, we developed in 1983 a Gröbner basis algorithm to work on polynomial ideals over the integers and subsequently extended it to work on polynomial ideals over Gaussian integers and polynomial ideals with univariate polynomial over a field as coefficients.[1] In this paper, we generalize these algorithms to

1. The polynomial ring Q[u][x1, ..., xn] is isomorphic to Q[u, x1, ..., xn]. A Gröbner basis computation over Q[u][x1, ..., xn] using the algorithm discussed in the paper is, however, quite different from a Gröbner basis computation over Q[u, x1, ..., xn] using Buchberger's algorithm over a field as illustrated later in the paper.

an algorithm for polynomial ideals over a Euclidean domain. Since the definition of reduction used in our approach is different from the definitions of reduction in the approaches of Shtokhamer, Trinks, Zacharias, as well as Schaller, a Gröbner basis of an ideal computed by our algorithm in general includes more elements than in Gröbner bases produced by algorithms based on other approaches. Further, our algorithm works for any admissible ordering on terms. We now illustrate some of these differences using a simple example.

Consider an ideal I over $Z[x, y]$ generated by $B = \{ 2x, 3y \}$; the polynomial xy is in I. As we show later in the paper, this basis is not a Gröbner basis by our definition as xy does not reduce to 0; neither $2x$ nor $3y$ can reduce xy. Our algorithm will compute a critical pair for the two polynomials as follows: there is a superposition $3xy$ which can be reduced in two different ways; using $2x$, it reduces to xy which cannot be reduced any further; using $3y$, $3xy$ reduces to 0. This gives a new polynomial xy, which is added to the original basis. The basis $\{ 2x, 3y, xy \}$ is a Gröbner basis by our approach. However, B is a Gröbner basis according to the definitions in (Shtokhamer, 1976; Trinks, 1978; Zacharias, 1978; Schaller, 1979). Since in their approaches, more than one polynomial is used for reduction, xy can be reduced to 0 using both $2x$ and $3y$; the equation $1 = 2a + 3b + c$ can be solved for a value of c less than 1 and the solution is $a = -1$, $b = 1$, and $c = 0$.

Other differences between our approach and those of Shtokhamer, Trinks, Zacharias and Schaller are discussed later in the paper. Relationship between computation of syzygies for determining new polynomials to be added to a basis as proposed by Shtokhamer, Trinks, Zacharias and Schaller and the critical pair computation as discussed by Buchberger and us is explored in (Kapur and Narendran, 1985c).

Buchberger (1984) also developed a general version of the Gröbner basis algorithm for commutative rings which satisfy certain conditions. He identified conditions on a ground ring such that the ground ring admits the Gröbner basis computation and furthermore, these conditions are preserved when going from the ground ring to a polynomial ring over the ground ring; he called such rings *reduction* rings. His general algorithm works for polynomial ideals over the integers as the ring of integers is a reduction ring.

Le Chenadec (1983) independently developed an algorithm for solving the uniform word problem for finitely presented commutative rings with unity based on extensions of the Knuth-Bendix completion procedure (1970) developed by Lankford and Ballantyne (1977), as well as Peterson and Stickel (1981). This algorithm also computes a Gröbner basis of a polynomial ideal over the integers. Ayoub (1983) also developed an algorithm to work on polynomial ideals over the integers.

Pan (1985) extended our algorithm to compute *D-bases* of polynomial ideals over a principal ideal domain. A D-basis of an ideal is the same as its *weak* Gröbner basis as defined in (Kapur and Narendran, 1985c) which has the property that every element of an ideal reduces to 0 with respect to its weak Gröbner basis. In contrast, every element in a ring has a unique normal form with respect to a *strong* Gröbner basis as defined in (Kapur and Narendran, 1985c); the normal form of the elements in the ideal generated by a strong Gröbner basis is obviously 0. A Gröbner basis computed by our algorithm is a strong Gröbner basis.

Based on their work on computing Gröbner basis over modules (Möller and Mora, 1986), Möller (1985) also claimed to have developed an extension of Buchberger's Gröbner basis algorithm to a subclass of commutative rings.

2. Polynomial Rings

Let $E[x_1, \cdots, x_n]$ be the polynomial ring over indeterminates $x_1, \cdots, x_n$, where the coefficients of terms in a polynomial are taken from a Euclidean domain E. A *term* is any power product $\prod_{i=1}^{n} x_i^{k_i}$, where $k_i \geq 0$, including 1; the *degree* of a term is $\sum_{i=1}^{n} k_i$. An admissible ordering (Buchberger, 1985) on terms is an ordering satisfying the following properties:

(i) $1 < t$, for any term $t \neq 1$, and

(ii) if $t_1 < t_2$, then for any term t, $t * t_1 < t * t_2$.

Different total well-founded admissible orderings on terms can be defined; two most commonly used orderings are total-degree ordering and lexicographic ordering induced by a total ordering on indeterminates. Let $<$ be a total well-founded admissible ordering on terms in $E[x_1, \cdots, x_n]$.

Let $p = m + r$ be a polynomial such that the term of the monomial m is greater than those within r (if p is a single monomial, let $p = m$); then m is called the *head-monomial* of p, written as $hm(p)$, the term of m is called the *head-term* of p, written as $ht(p)$, and the coefficient of m is called the *head-coefficient* of p, written as $hc(p)$. A monomial is written as ct, where t is a term and $c \in E$; we will often omit the multiplication symbol '*.'

2.1 Well-founded ordering on a Euclidean domain

Associated with a Euclidean domain E is a norm function $g: E \rightarrow N$ that is related to a division algorithm over it. In particular,

(i) for $a \neq 0$, $b \neq 0$ in E and $a\ b \neq 0$, $g(a\ b) \geq g(a)$ as well as $\geq g(b)$, and

(ii) for $a \neq 0$, b in E, there exist q and r such that $b = q\ a + r$, and either $q = 0$ or $g(r) < g(a)$.

The function g defines a quasi-ordering on the elements of E :

$a \leq_g b$ if and only if $g(a) \leq g(b)$.

Further, $<_g$, a subset of $\leq_g$, is defined as:

$a <_g b$ if and only if $g(a) < g(b)$.

It is easy to see that $<_g$ is a Noetherian relation. We will often drop the subscript g from $<_g$ and use $<$ instead.

To simplify the presentation as well as for obtaining a reduced unique Gröbner basis for a polynomial ideal (subject to an admissible term ordering), it was required in an earlier version of this paper (Kandri-Rody and Kapur, 1984c) that E admit a total well-founded ordering that is a refinement of $<_g$. We had said that the algorithm for computing a Gröbner basis given in (Kandri-Rody and Kapur, 1984c) did not depend upon this requirement. In this paper, we do not require that E have a total well-founded ordering; instead, we assume additional properties of E and division algorithms on E as we need them.

The reader will notice that the proofs of Theorem 3.2 in Section 3 and Theorem 4.1 in Section 4 require that a division algorithm on a Euclidean domain used for defining reduction relation satisfy the following property: For any non-zero divisor d of a Euclidean domain, the difference of any two distinct remainders resulting from division by d is not a multiple of d. This property is equivalent to the property used by Pan (1985) that for every principal ideal over a Euclidean domain, every quotient class modulo the principal ideal has a unique remainder. We will call it the *unique remainder* property of a division algorithm over E.

Subsequently, in Section 8, another property on E is required to obtain the result that every polynomial ideal over E has a reduced unique Gröbner basis subject to an admissible term ordering. This property is the existence of a function to pick unique representatives from every equivalence class of associate elements in E.

2.2 Well-founded Ordering on Polynomial Ring

A total well-founded ordering on terms in $E[x_1, \cdots, x_n]$ and a well-founded ordering on E defines a well-founded ordering $<$ on polynomials in $E[x_1, \cdots, x_n]$ in a natural way: (i) $0 < p \neq 0$, and (ii) a polynomial $p_1 < p_2$, if and only if $ht(p_1) < ht(p_2)$ or $(ht(p_1) = ht(p_2)$ and $hc(p_1) < hc(p_2))$ or $(hm(p_1) = hm(p_2)$ and $(p_1 - hm(p_1)) < (p_2 - hm(p_2)))$.

3. Polynomials as Rewrite Rules

Let $m_1 = c_1\ t_1$ be the head-monomial of a polynomial p in $E[x_1, \cdots, x_n]$; let $rest(p)$ be $p - m_1$. The rewrite rule corresponding to p is:

$$c_1\ t_1 \rightarrow -\ rest(p).$$

If p is a monomial, the right-hand side of its rule is 0; if p is an element, say c, of E, even then the rule is $c \rightarrow 0$. We will assume, henceforth, that the rule corresponding to p is: $c_1\ t_1 \rightarrow R_1$, where t_1 is a term (possibly 1) and R_1 is a polynomial (possibly 0) whose head-term is smaller than t_1.

This rule corresponding to p is used to rewrite polynomials as follows: Let m be a monomial, where $m = c\ t$ and $c \neq 0$. If the quotient obtained by dividing c by c_1 is 0 or there does not exist a term σ such that $t = \sigma\ t_1$, then m cannot be rewritten by the rule $c_1\ t_1 \rightarrow R_1$. Otherwise, if $t = \sigma\ t_1$, then

$$m \rightarrow b\ t + a\ \sigma\ R_1,$$

where $c = a\ c_1 + b$, and a and b are respectively, the quotient and remainder obtained by dividing c by c_1 using a division algorithm on E. Let $q = q_1 + c\ t$ be a polynomial such that $c\ t$ is the largest monomial in q that can be rewritten using the rule corresponding to p. Then,

$$q \rightarrow q_1 + b\ t + a\ \sigma\ R_1.$$

For example, in the case of $Z[x, y]$, the rewrite rule corresponding to $3\ x\ y^2 - x$ is $3\ x\ y^2 \rightarrow x$. Using this rule, the polynomial

$$10\ x\ y^3 - 4\ x\ y^2 + 5\ x^2\ y \rightarrow x\ y^3 + 3\ x\ y - 4\ x\ y^2 + 5\ x^2\ y;$$

the monomial $10\ x\ y^3$ is being rewritten using the above rule since 10 can be divided by 3 giving the quotient 3 and the remainder 1. The above result can be further reduced as the monomial $-4\ x\ y^2$ is reducible since -4 can also be divided by 3,

$\rightarrow x\ y^3 + 3\ x\ y\ -\ x\ y^2 - x\ + 5\ x^2\ y.$

The rewriting relation induced by a finite set of polynomials is the *union* over the rewriting relations induced by the polynomials in the set. For definitions, details and motivation for the rewriting approach, an interested reader may wish to refer to (Huet and Oppen, 1980; Musser and Kapur, 1982; Buchberger and Loos, 1982). Henceforth, we assume familiarity with definitions of Noetherian (finitely terminating), confluent, locally-confluent, canonical, complete reduction relations, as well as with the definitions of normal form, canonical form, etc.

Since a division algorithm over E always produces a remainder smaller than the element being divided when the quotient is non-zero, using the well-founded ordering defined on polynomials in Section 2, we have

Theorem 3.1: Given any finite basis B of polynomials in $E[x_1, \ldots, x_n]$, the rewriting relation $\rightarrow$ induced by B is Noetherian.

We should emphasize here that the rewriting (reduction) relation defined above involves the use of a single polynomial at a time for reduction and depends upon a division algorithm over E. Different division algorithms will lead to different rewriting relations.

The definitions of reduction relations given in (Shtokhamer, 1976; Trinks, 1978; Zacharias, 1978; Schaller, 1979) are, on the other hand, quite different; as stated in Subsection 1.1 on related work, for reducing a monomial with respect to a basis in these approaches, all polynomials in the basis whose head-terms divide the monomial, must be considered and a non-homogeneous equation over E must be solved.

For example, to reduce xy with respect to the basis $\{2x, 3y\}$, both the polynomials will be used and xy reduces to 0 using them as there exist a, b, and c such that $1 - c = 2a + 3b$ and $c < 1$ (in particular, $a = -1$, $b = 1$ and $c = 0$).

Using our definition of rewriting, xy cannot be rewritten by any of the two polynomials. We think that our definition of rewriting is simpler than those proposed in (Shtokhamer, 1976; Trinks, 1978; Zacharias, 1978; Schaller, 1979).

3.1 Rewriting Relation and Ideal Congruence

It must be shown that the rewriting relation as defined above is strong enough to capture the ideal congruence relation, i.e., the reflexive, symmetric and transitive closure of the relation $\rightarrow$ for a finite set of polynomials $\{b_1, \cdots, b_k\}$, denoted as $\leftrightarrow^*$, is indeed the ideal congruence relation $=_I$, where $I = (b_1, \ldots, b_k)$, and $p =_I q$ if and only if $p = q + \sum_{i=1}^{k} q_i\ b_i$ from some $q_1, \ldots, q_k \in E[x_1, \ldots, x_n]$. In order to prove this, we require that a division algorithm on E has the unique remainder property as defined in Section 2.1; it states that for any non-zero divisor d of a Euclidean domain, the difference of any two distinct remainders resulting from division by d is not a multiple of d.

Theorem 3.2: $\leftrightarrow^* = =_I$.

Proof: (1) $\leftrightarrow^* \subseteq =_I$: It is trivial to show this by induction that for every k, $\leftrightarrow^k \subseteq =_I$.

(2) $=_I \subseteq \leftrightarrow^*$: $p =_I q$ implies $p = q + \sum_{i=1}^{k} q_i\, b_i = q + \sum_{j=1}^{m} a_j\, s_j\, b_{i_j}$, where $a_j \in E$, s_j is a term and $b_{i_j} \in (b_1, \cdots, b_k)$. We show that $p \leftrightarrow^* q$ by induction on m.

Basis: $m = 0$: obvious.

Inductive step: $p = q + a_{m+1}\, s_{m+1}\, b_{i_{m+1}} + \sum_{j=1}^{m} a_j\, s_j\, b_{i_j}$.

By induction hypothesis, $p \leftrightarrow^* q + a_{m+1}\, s_{m+1}\, b_{i_{m+1}}$.
Let $q' = q + a_{m+1}\, s_{m+1}\, b_{i_{m+1}}$ and the rule corresponding to $b_{i_{m+1}}$ be $L \rightarrow R$. Let t and c be the head-term and head-coefficient, respectively, of $a_{m+1}\, s_{m+1}\, b_{i_{m+1}}$. Let t' be the term of the largest monomial in q which can be rewritten using the rule $L \rightarrow R$.

Case 1: $t' \leq t$: Let $q \rightarrow^* q_1$ using $L \rightarrow R$ such that the monomial with terms $\geq t$ in q_1 cannot be rewritten any further using $L \rightarrow R$. Similarly, let $q' \rightarrow^* q_1'$ using $L \rightarrow R$ such that the monomial with terms $\geq t$ in q_1' cannot be rewritten any further using $L \rightarrow R$. Since $q' - q = a_{m+1}\, s_{m+1}\, b_{i_{m+1}}$, $q_1 = q_1'$ because of the unique remainder property of division algorithm (the difference of any two distinct remainders obtained after dividing by a non-zero divisor d is not a multiple of d). So $q \leftrightarrow^* q'$. Thus, $p \leftrightarrow^* q' \leftrightarrow^* q$.

Case 2: $t' > t$: Let $q \rightarrow^* q_1$ by applying $L \rightarrow R$ such that monomials with terms $\geq t$ in q_1 cannot be rewritten using $L \rightarrow R$. Apply the same reductions on q' as much as possible, and let the result be q_1'. Since all terms $> t$ have the same coefficient in q and q', either $q_1' = q_1 + a_{m+1}\, s_{m+1}\, b_{i_{m+1}}$ or $q_1' = q_1$.
This is case 1 from which we have q_1 and q_1' are joinable. So $q_1 \leftrightarrow^* q_1'$.
Thus $q \leftrightarrow^* q'$ from which $p \leftrightarrow^* q$. □

4. Gröbner basis of a polynomial ideal

Following Buchberger, a finite set B of polynomials, say $\{b_1, \cdots, b_k\}$, in $E[x_1, \ldots, x_n]$ is defined as a *Gröbner basis* of the ideal $(b_1, \cdots, b_k)$ if and only if for any polynomial q in $E[x_1, \ldots, x_n]$, no matter how q is rewritten using the rules corresponding to polynomials in B, the result is always the same, i.e., it is unique. It can be easily shown that this definition implies that for any polynomial p in the ideal I generated by B, $p \rightarrow^* 0$. A Gröbner basis of an ideal generated by a finite set of polynomials is thus like a complete (canonical) rewriting system for an equational theory generated by a finite set of axioms; it generates canonical forms for residue classes induced by its ideal on $E[x_1, \ldots, x_n]$.

For examples, consider the ideal I generated by $B = \{x\, y + 1,\ y^2 + x\}$ in $Z[x, y]$; $y - x^2$ is in I but does not reduce to 0, so B is not a Gröbner basis. However, $B' = \{x\, y + 1,\ y^2 + x,\ x^2 - y\}$ is a Gröbner basis. Similarly, the basis $\{(5 + 3i)\, x^2\, y - y,\ (3 + 2i)\, x\, y^2 - x\}$ in $Z[i][x, y]$ is not a Gröbner basis, where $Z[i]$ is the ring of Gaussian integers and $i^2 = -1$.

Let $F = \{L_1 \rightarrow R_1, \cdots, L_k \rightarrow R_k\}$ be the rule set corresponding to a finite basis $(b_1, \cdots, b_k)$ of an ideal I such that $\{L_i \rightarrow R_i\}$ be the rule corresponding to

b_i. We will also call F a basis of I.

Definition: A basis F is a Gröbner basis of (F) if the Noetherian relation $\rightarrow$ induced by F is confluent, i.e., for any polynomial p, for all p_1, p_2 such that $p \rightarrow^* p_1$ and $p \rightarrow^* p_2$, there is a q such that $p_1 \rightarrow^* q$ and $p_2 \rightarrow^* q$.

Definition: A Gröbner basis F is *reduced* (or *minimal*) if and only if for each i, $1 \leq i \leq k$, neither L_i nor R_i can be reduced by any other rule in F.

4.1 Test for a Gröbner Basis

The confluence test for $\rightarrow$ is developed in a way similar to that developed by Buchberger (1976, 1980, 1984) for polynomial ideals over a field. We define a *critical pair* for a pair of polynomials in a basis. Then we show that if these critical pairs are *quasi-joinable* (called trivial in (Kandri-Rody and Kapur, 1984c)) in the sense that the corresponding S-polynomials reduce to 0, $\rightarrow$ is confluent.

4.1.1 Critical Pairs

The critical pairs to check whether the basis F of an ideal I is a Gröbner basis, are defined as:

Definition CP1: Given two rules $L_i \rightarrow R_i$ and $L_j \rightarrow R_j$, where $L_i = c_i\ t_i$ and $L_j = c_j\ t_j$, $c_i \geq c_j$, the *superposition* is $c_i\ lcm(t_i, t_j)$ and the *critical pair* $<p, q>$ is:

$p = a\ f_j\ R_j + b\ lcm(t_i, t_j)$, and

$q = f_i\ R_i$

where $f_i\ t_i = f_j\ t_j = lcm(t_i, t_j)$, standing for the least-common-multiple (lcm) of terms t_i and t_j, and $c_i = a\ c_j + b$, where a and b are respectively, the quotient and remainder obtained by dividing c_i by c_j. Polynomials p and q are obtained from the superposition $c_i\ lcm(t_i, t_j)$ by applying $L_j \rightarrow R_j$ and $L_i \rightarrow R_i$, respectively. Note that there is exactly one critical pair for a pair of rules.

The above definition of critical pairs is a generalization of the definition used in Buchberger(1976) where the coefficients of terms in polynomials are from a field as well as the definition used in (Kandri-Rody and Kapur, 1984a; 1984b) for the case where the coefficients are integers, Gaussian integers, or univariate polynomials over a field.

It is easy to see that for each critical pair $<p, q>$ of any two polynomials in an ideal, the polynomial $p - q$ is also in the ideal. So, adding the polynomial $p - q$ to the ideal does not change the ideal.

Definition: The *S-Polynomial* corresponding to a critical pair $<p, q>$ is the polynomial $p - q$.

Definition: A critical pair $<p, q>$ is *quasi-joinable* if and only if its S-polynomial $p - q$ can be reduced to 0 by applying at every step, among all applicable rules, a rule whose left-hand-side has a minimal coefficient with respect to $<$ on E.

As Theorem 4.1 below implies, to test whether a given basis F is a Gröbner basis, one needs to check whether for each pair of distinct rules in F, its critical pair $<p, q>$ is quasi-joinable.

The above definition of an S-polynomial is different and much simpler from those used by Shtokhamer, Trinks, Zacharias and Schaller; they compute S-polynomials using syzygies by solving linear homogeneous equations. Since reduction relations used in their approaches are quite strong because, in general, more than one polynomial is used for reduction, a Gröbner basis of an ideal by their approaches is usually a proper subset of a Gröbner basis as defined above.

As stated in the related work subsection 1.1, the basis $\{2x\ ,\ 3y\ \}$ is a Gröbner basis according to the approaches proposed by Shtokhamer, Trinks, Zacharias, as well as Schaller, whereas $\{2x\ ,\ 3y\ \}$ is not a Gröbner basis by the above definition. This is so because in our approach, the polynomial xy which is in the ideal $(2x\ ,\ 3y\ )$, cannot be reduced to 0; in fact, xy cannot be reduced by either of the two polynomials in the basis. The above critical pair test detects this when the rules corresponding to these two polynomials are superposed: the superposition is $3xy$, the critical pair is $<xy\ ,\ 0>$, and the S-polynomial xy cannot be reduced to 0.

In contrast, the polynomial xy can be reduced to 0 using the reduction relations used by Shtokhamer, Trinks, Zacharias, as well as Schaller, because both the polynomials $2x$ and $3y$ are used together to reduce xy; see the discussion following Theorem 3.1 in Section 3. S-polynomials in those approaches are computed as follows: (i) for every subset S (of size > 1) of polynomials in a basis, compute the least-common-multiple (lcm), say t, of the head-terms of these polynomials in S; (ii) for each such t, consider the set of all polynomials in the basis whose head-terms divide t and call it S'; solve a homogeneous equation over the head-coefficients of polynomials in S'; (iii) each element in a basis for the solutions of this homogeneous equation gives an S-polynomial for the subset S' of polynomials in the basis; the head-term of each such S-polynomial is smaller than the lcm t.

For the basis $\{2x\ ,\ 3y\ \}$, the lcm of the head-terms of its two polynomials is xy; the homogeneous equation that needs to be solved is:

$$2a\ +\ 3b\ =0,$$

where $a\ ,\ b$ are solutions of the equation. Then, a S-polynomial for $2x$ and $3y$ is:

$$a\ \ y\ \ (2x\ )\ +\ b\ \ x\ \ (3y\ ).$$

This is obtained by adding the result of multiplying the polynomial $2x$ by ay, where y is the term obtained by dividing the lcm xy by the head-term of $2x$, to the result of multiplying the polynomial $3y$ by bx, where, similarly, $x\ =xy\ /y$. For the above homogeneous equation, any multiple of the pair $<-3,\ 2>$ is a solution, which gives the value of the S-polynomial to be 0, thus declaring $\{2x\ ,\ 3y\ \}$ to be a Gröbner basis. A relationship between critical pairs defined using syzygies and our definition of critical pairs is discussed in (Kapur and Narendran, 1985c).

Theorem 4.1: A basis B of polynomials in $E\left[x_{1,}\ \cdots\ ,\ x_n\right]$ is a Gröbner basis of $(B\ )$ if and only if for every pair of polynomials in B, the critical pair $<p\ ,\ q\ >$ as defined using definition **CP1** is quasi-joinable.

The proof of this theorem has a structure similar to the proof of an analogous theorem in (Bachmair and Buchberger, 1980) when E is a field. There are two major differences. Firstly, the definition of a quasi-joinable critical pair uses a subset of $\rightarrow$, denoted by $\rightarrow'$, which is defined as follows: A monomial $c\ \ t\ \rightarrow'\ q'$ if and only if $c\ \ t\ \rightarrow\ q'$ using a rule $c_1\ t_1\ \rightarrow R_1$ in B such that there does not exist any other rule $c_2\ t_2\ \rightarrow R_2$ in B which can be applied on $c\ \ t$ and $c_2 < c_1$.

Secondly, the proof uses the following lemma: if every pair of polynomials in a basis B has a quasi-joinable critical pair, then for any two rules $c_i\ t_i \rightarrow R_i$ and $c_j\ t_j \rightarrow R_j$, there is a rule $d\ t' \rightarrow R'$ in B such that d divides the gcd (greatest common divisor) of c_i and c_j and there is a term σ, $\sigma\ t' = lcm\ (t_i\ ,\ t_j) = t$ (Lemma 5.7 in (Kandri-Rody and Kapur, 1984c)). For details of the proof, the reader may consult (Kandri-Rody and Kapur, 1984c).

The proof of the above theorem also depends upon the unique remainder property of a division algorithm on E.

Note that if a weak notion of a Gröbner basis was considered which only required that every polynomial in an ideal reduces to 0 with respect to its Gröbner basis (called a *weak* Gröbner basis in (Kapur and Narendran, 1985c)) and did not require that every polynomial in a polynomial ring has a unique normal form with respect to a Gröbner basis, then the unique remainder property of a division algorithm on a Euclidean domain is not needed for the proof of Theorem 4.1. Pan (1985) discussed such bases for polynomial ideals.

5. A Gröbner basis algorithm

If a given basis of an ideal is not a Gröbner basis, it can be *completed* to get a Gröbner basis of its ideal. For every critical pair $< p\ ,\ q >$ such that normal forms of p and q do not simplify to the same polynomial, we add a new rule corresponding to a normal form of the S-polynomial $p - q$, thus generating a new basis for the same ideal. This step is repeated until the critical pair $< p\ ,\ q >$ of each pair of rules in the basis is quasi-joinable. The termination of this process is guaranteed because of the finite ascending chain condition of properly contained ideals over a Noetherian ring (since $E\ [x_1, \cdots, x_n]$ is a Noetherian ring); for a detailed proof of termination, the reader may consult (Kandri-Rody and Kapur, 1984c).

Example: Consider an example of a polynomial ideal over $Z\ [x\ ,\ y\ ]$ taken from (Möller, 1985) with the total degree ordering induced by $y > x$.

$B = \{1.\ 7\ x^2\ y \rightarrow 3x\ ,\ \ 2.\ 4\ x\ y^2 \rightarrow xy\ ,\ \ 3.\ 3y^3 \rightarrow 0\}$.

We use the minimal remainder division algorithm on integers for defining the reduction relation. It is easy to see that B is not a Gröbner basis. To obtain a Gröbner basis, we first add the rule obtained by the critical pair of rules 1 and 2:

4. $x^2\ y^2 \rightarrow 2x^2y\ - 3xy.$

From rules 2 and 4, we get the critical pair $< x^2y\ ,\ 8\ x^2y\ - 12\ xy >$ which gives an additional rule:

5. $12\ xy \rightarrow 3\ x.$

Rule 1 can be reduced using rule 5 as xy divides x^2y and the minimal remainder division algorithm on 7 divided by 12 gives 1 as quotient and -5 as remainder.

1'. $5\ x^2y \rightarrow 3x^2 - 3x.$

The critical pair between rules 3 and 5 gives a new rule:

6. $xy^2 \rightarrow xy\ ,$

which simplifies rule 2 to:

2'. $3xy \rightarrow 0.$

This simplifies rule 5 to give:

$5'.\ 3x \rightarrow 0,$

which simplifies rules $1'$ to:

$1''.\ x^2y \rightarrow 0.$

Rules $1''$, 3, $5'$, and 6 delete other rules. The polynomials $\{ 3x, x^2y, xy^2 - xy, 3y^3 \}$ corresponding to rules $1''$, 3, $5'$ and 6 constitute a Gröbner basis as the critical pair for each pair of these polynomials is quasi-joinable.

We now give a simple algorithm patterned after a Gröbner basis algorithm in (Buchberger, 1985).

ALGORITHM: Given F, a finite set of polynomials in $E[x_1, \cdots, x_n]$, find G such that ideal (F) = ideal (G) and G is a Gröbner basis.

```
S := F; G := { };
loop until has-unit (G) or (empty (pairs) and empty (S))
  loop until empty (S)
    q := remove (S);
    (G , S , pairs) := addrule (q , G , S , pairs)
  end loop;
(p 1, p 2) := next-pair (pairs);
(G , S , pairs) := addrule (S-poly (p 1, p 2), G , S , pairs)
end loop;
return G .
```

```
addrule (q , G , S , pairs) returns (G , S , pairs)

new := normal-form (q , G );
G' := { p | p in G and hm (p ) can be reduced by new };
G := G - G';
S := S ∪ G';
pairs := pairs ∪ { (p , new) | p in G };
G := reduced (G ∪ { new });
return (G , S , pairs)
```

In the above algorithm, the predicate *has-unit* (G) tests whether G includes a unit in E, in which case that unit by itself is a Gröbner basis; the predicate *empty* (S) tests whether a set is empty or not. The function *remove* takes out an element from a non-empty set with a side-effect on the set. The function *next-pair* picks the next pair of polynomials in G whose critical pair is to be considered next. Both of these functions can take as parameter a strategy to be used for picking the next element in a set. The function *next-pair* considers only those pairs in which both polynomials are in G and discards other pairs. Criteria for discarding unnecessary critical pairs can also be included to decide whether the S-polynomial of a pair of polynomials should be computed. The function *normal-form* computes a normal form of a polynomial with respect to a finite set of polynomials; it can also be parameterized to specify different normalization strategies. The function *S-poly* computes the S-polynomial of a pair of

polynomials. The function *reduced* reduces the righ-hand-sides of the rules with respect to each other, and generates a reduced basis; even if the expression "*reduced* $(G \cup \{ new \})$" in the function *addrule* is replaced by "$G \cup \{ new \}$," the result of the modified algorithm will still be a Gröbner basis which is not necessarily reduced.

The correctness of the above algorithm can be established using arguments similar to those given in (Buchberger, 1984; Buchberger, 1985).

An instance of the above algorithm for polynomial ideals over the ring of integers has been implemented in ALDES as well as in LISP, and has been experimented with; an interested reader may refer to (Kandri-Rody and Kapur, 1984b) and (Kandri-Rody, Kapur and Narendran, 1985) for examples.

5.1 Optimization

The above process of generating critical pairs (using definition CP1) can be replaced by another construction that explicitly uses the gcd computation on the elements of a Euclidean domain.

Definition CP2: The critical pair for two rules $c_1\, t_1 \rightarrow R_1$ and $c_2\, t_2 \rightarrow R_2$, where $c_2 \geq c_1$ is defined as follows: Let c be the extended *gcd* of c_1 and c_2, i.e., there is an a and b such that $c = a\ \ c_1 + b\ \ c_2$; further, $c_1 = k_1\, c$ and $c_2 = k_2\, c$. Let $t = lcm\,(t_1, t_2) = f_1\, t_1 = f_2\, t_2$.

(a) One critical pair $< p\ ,\ q >$ is: $p = c\ \ lcm\,(t_1, t_2)$ and $q = a\ \ f_1 R_1 + b\ \ f_2 R_2$.

(b) Another critical pair $< p\ ,\ q >$ is obtained from the superposition $k_1\, k_2\, c\ \ lcm\,(t_1, t_2)$ by applying the two rules: $p = k_2\, f_1\, R_1$ and $q = k_1\, f_2\, R_2$.

If c_1 divides c_2, then $c = c_1$, $k_1 = 1$, $a = 1$ and $b = 0$. Then, there is only one critical pair due to case (b).

This definition is closely related to the one proposed by Lauer (1976b) for obtaining a Gröbner basis. The critical pair construction (a) is not considered in the methods of Shtokhamer, Trinks, Zacharias, as well as Schaller. It is needed in our algorithm because of the simple reduction relation defined using one polynomial at a time. The critical pair construction (a) above leads to additional polynomials in Gröbner bases generated by our algorithm in contrast to Gröbner bases obtained from algorithms of Shtokhamer, Trinks, Zacharias, and Schaller.

The following result was jointly proved by Paliath Narendran and the second author. Since it does not appear in (Kandri-Rody and Kapur, 1984c), its proof is included below.

Theorem 5.1: A basis B of polynomials in $E[x_1, \cdots, x_n]$ is a Gröbner basis of (B) if and only if for every pair of polynomials in B, the critical pairs defined by the definition **CP2** are quasi-joinable.

Proof: It is shown that if for every pair of polynomials in B, the critical pairs defined by CP2 are quasi-joinable, then the critical pair defined by CP1 is also quasi-joinable.

Consider two rules $c_1\, t_1 \rightarrow R_1$ and $c_2\, t_2 \rightarrow R_2$ such that $c_2 \geq c_1$, as stated above in the definition CP2. There are two cases:

(i) $c_2 = dc_1$; the critical pair using CP1 is the critical pair using CP2.

(ii) $c_2 = d\ c_1 + r$, where $r < c_1$. There exists a k such that $r = k\ c$ which is
$= k\ a\ c_1 + k\ b\ c_2 = k\ a\ c_1 + (k\ b - 1)\ c_2 + d\ c_1 + r$;
so we have $(k\ a + d)\ c_1 + (k\ b - 1)\ c_2 = 0$. Since $c_1 = k_1\ c$ and $c_2 = k_2\ c$, we have $(k\ a + d)\ k_1\ c + (k\ b - 1)\ k_2\ c = 0$, from which we have $(k\ a + d)\ k_1 = -(k\ b - 1)k_2$. Since k_1 and k_2 do not have a common factor, there exists an α such that $k\ a + d = k_2\ \alpha$ and $(k\ b - 1) = -k_1\ \alpha$.

The S-polynomial using definition CP1 is $r\ t + d\ f_1 R_1 - f_2 R_2$. Using CP2, we have $c\ t - a\ f_1 R_1 - b\ f_2 R_2 \rightarrow'^* 0$ as well as $k_1\ f_2 R_2 - k_2\ f_1 R_1 \rightarrow'^* 0$. By Lemma 5.6 in (Kandri-Rody and Kapur, 1984c),

$k\ c\ t - k\ a\ f_1 R_1 - k\ b\ f_2 R_2 \rightarrow'^* 0$ and $\alpha k_1\ f_2 R_2 - \alpha\ k_2\ f_1 R_1 \rightarrow'^* 0$.

Using the property that for any two polynomials $p \rightarrow'^* 0$ and $q \rightarrow'^* 0$ implies $p - q \rightarrow'^* 0$,

$k\ c\ t - (k\ a - \alpha\ k_2)\ f_1 R_1 - (k\ b + \alpha\ k_1) f_2 R_2$
$= k\ c\ t + d\ f_1 R_1 - f_2 R_2 \rightarrow'^* 0$.

This implies that the S-polynomial from definition CP1 reduces to 0 also. □

Another proof of the above theorem was independently obtained by the first author with D. Lazard.

For the example discussed above, using CP2, we will obtain a Gröbner basis as follows: From rules 2 and 3, we get two rules:

4. $3xy^2 \rightarrow 0$.

5. $xy^3 \rightarrow xy^2$.

Rule 4 simplifies rule 2 to give:

2′. $xy^2 \rightarrow xy$.

Rule 2′ deletes rule 5 and simplifies rule 4 to:

4′. $3xy \rightarrow 0$.

Rule 4′ simplifies rule 1 to give:

1′. $x^2y \rightarrow 3x$.

Rules 1′ and 2′ give a new rule:

6. $3x \rightarrow 0$,

which simplifies rule 1′ to:

1″. $x^2y \rightarrow 0$.

Rule 6 deletes rule 4′. The polynomials corresponding to rules 1″, 2′, 3 and 6 constitute a Gröbner basis.

The above method was implemented for polynomial ideals over the integers and compared with the method using CP1. For some examples, the method using CP2 is better than the method using CP1 in overall performance while for some other examples, the method using CP1 turns out to be better than the method using CP2.

6. Examples

In Section 5, we discussed an example of an ideal over $Z[x, y]$. Here, we discuss an example from $Z[i][x, y]$, where $i^2 = -1$ and another from $Q[s][x, y]$.

Afterwards, we discuss examples of polynomial ideals over algebraic integers in $Q[\sqrt{-3}]$ and $Q[\sqrt{2}]$. In each case, we assume the total degree ordering induced by $y > x$. These examples are illustrated using definition CP1.

We use a division algorithm over $Z[i]$ as given in (van der Waerden, 1966, p. 56). Consider the basis:

1. $(5 + 3i)\, x^2\, y \rightarrow y$ and 2. $(3 + 2i)\, x\, y^2 \rightarrow x$.

From rules 1 and 2, we get the superposition $(5 + 3i)\, x^2\, y^2$ and the critical pair $<y^2,\ 2x^2 - (1 + i)\, x^2\, y^2>$, which gives the following rule:

3. $(1 + i)\, x^2\, y^2 \rightarrow 2x^2 - y^2$.

From rules 2 and 3, the superposition is $(3 + 2i)\, x^2\, y^2$, which gives the following rule:

4. $x^2\, y^2 \rightarrow 2\, y^2 - 3\, x^2$.

Rule 3 now reduces to: $3'$ $(3 + 2i)\, y^2 \rightarrow (5 + 3i)\, x^2$.
Rule 2 now simplifies to: $2'$ $(5 + 3i)\, x^3 \rightarrow x$.
The basis consisting of polynomials corresponding to rules 1, 2′, 3′, and 4 is a Gröbner basis.

If a Gröbner basis algorithm over $Z[i, x, y]$ is used to compute a Gröbner basis of a polynomial ideal over $Z[i][x, y]$ by augmenting its basis over $Z[i][x, y]$ with the polynomial $i^2 + 1$, we obtain a very different basis after considerably more steps. For the above example, the following Gröbner basis is obtained:

$\{\ i^2 + 1,\ 34x^3 + (-5+3i)x,\ (13+i)x^3 + (-2+i)x,\ 34x^2y + (-5+3i)y,$
$(13+i)x^2y + (-2+i)y,\ 13y^2 + (-21+i)x^2,\ (-5+i)y^2 + (8-2i)x^2$
$x^2y^2 - 2y^2 + 3x^2\ \}$.

This is so because of the different ordering used in a Gröbner basis algorithm over $Z[i, x, y]$:

$a + bi > c + di$ if $b > d$ or $(b = d$ and $a > c)$.

Consider now an example over $Q[s][x, y]$. The division algorithm used is the standard division over univariate polynomials. The basis is:

1. $(s^2 - 1)\, x^2\, y \rightarrow y$

2. $(s + 1)\, x\, y^2 \rightarrow x$.

From rules 1 and 2, the superposition is $(s^2 - 1)\, x^2\, y^2$ and we get the following rule:

3. $y^2 \rightarrow (s - 1)\, x^2$.

Rule 3 can be used to reduce rule 2 to:

$2'$. $(s^2 - 1)\, x^3 \rightarrow x$.

Rules 1, 2′ and 3 constitute the Gröbner basis of $Q[s][x, y]$.

Consider a more complex example over $Q[s][x, y]$. The basis is:

1. $(s^2 + 2/5\ s - 1/5)\, x^2\, y \rightarrow 1/5\ y$

2. $(s - 1/3)\, x\, y^2 \rightarrow 1/3\ x$.

From rules 1 and 2, we get the rule: 3. $x^2\, y^2 \rightarrow 9/2\ y^2 - (15/2\ s + 11/2)\, x^2$.
From rules 2 and 3, we get the rule: 4. $(s - 1/3)\, y^2 \rightarrow (5/3\ s^2 + 2/3\ s - 1/3)\, x^2$.
Rule 2 can now be reduced using rule 4 to: $2'$. $(s^2 + 2/5\ s - 1/5)\, x^3 \rightarrow 1/5\ x$.

Rules 1, 2', 3, and 4 constitute a Gröbner basis of the above ideal.

Since $Q[s][x, y] = Q[s, x, y]$, the Gröbner basis algorithm over rationals can also be used to obtain a Gröbner basis over $Q[s, x, y]$. The computation steps in the above algorithm are however different from the computation steps in a Gröbner basis algorithm over $Q[s, x, y]$. In the above algorithm, coefficients of monomials are univariate polynomials because of which multiple steps of a Gröbner basis algorithm over $Q[s, x, y]$ may correspond to a single step of a Gröbner basis algorithm over $Q[s][x, y]$. If a lexicographic ordering on terms is used in which s is the smallest indeterminate, a reduced Gröbner basis obtained by running the above algorithm over $Q[s][x, y]$ will be the same as a reduced Gröbner basis obtained by running the algorithm over $Q[s, x, y]$. A reduced Gröbner basis obtained by running the above algorithm over $Q[s][x, y]$ using the total degree ordering on terms can also be obtained by running the above algorithm over $Q[s, x, y]$ only if a mixed ordering on terms is used with the following properties: (i) s is the smallest indeterminate, and (ii) terms are compared first by comparing the total degrees of indeterminates x and y in the total degree ordering, and comparing the degrees of s only if the total degrees of x and y in the two terms being compared are equal.

Now, we consider examples in which coefficients of monomials are taken from rings of algebraic integers in algebraic number fields which admit Euclid's division algorithm (Hardy and Wright, 1938; Oppenheim, 1934). As a first example, consider the ring of integers in the algebraic number field $Q[\sqrt{-3}]$; note that this ring has units 1, -1, and $(1 + \sqrt{-3})/2$, $(1 - \sqrt{-3})/2$, $(-1 + \sqrt{-3})/2$ and $(-1 - \sqrt{-3})/2$. Consider a basis

1. $(1 + 3j)/2\ x^2 y \rightarrow y$ and 2. $(4 + j)\ x\ y^2 \rightarrow x$,

where $j = \sqrt{-3}$. The norm function defined on integers in $Q[\sqrt{-3}]$ is $g(a + b\sqrt{-3}) = a^2 + 3b^2$. The division algorithm discussed in (Hardy and Wright, 1938, p. 212) is used. From rules 1 and 2, we get the superposition $(4 + j)\ x^2 y^2$ and the critical pair $\langle x^2, (1 - j)\ y^2 - x^2 y^2 \rangle$, which gives the following rule:

3. $x^2 y^2 \rightarrow -x^2 + (1 - j)\ y^2$.

From rules 1 and 3, the superposition is $(1 + 3j)/2\ x^2 y^2$, which gives the following rule:

4. $(4 + j)\ y^2 \rightarrow (1 + 3j)/2\ x^2$.

This rule simplifies rule 2 to: $2'\ (1 + 3j)/2\ x^3 \rightarrow x$.
The basis consisting of polynomials corresponding to rules 1, 2', 3, and 4 is a Gröbner basis.

Now consider the ring of algebraic integers in the algebraic number field $Q[\sqrt{2}]$ with infinitely many units (Hardy and Wright, 1938). Consider a basis

1. $(5 + 3k)\ x^2 y \rightarrow y$ and 2. $(3 + 2k)\ x\ y^2 \rightarrow x$,

where $k = \sqrt{2}$. The norm function defined on integers in $Q[\sqrt{2}]$ is $g(a + b\sqrt{2}) = |a^2 - 2b^2|$. Again the division algorithm discussed in (Hardy and Wright, 1938; p. 214) is used. From rules 1 and 2, we get the superposition $(5 + 3k)\ x^2 y^2$ and the critical pair $\langle y^2, (3 - k)\ x^2 \rangle$, which gives the following rule:

3. $y^2 \rightarrow (3 - k)\ x^2$.

Rule 3 now reduces rule 2 to: $2'\ (5 + 3k)\ x^3 \rightarrow x$.
The basis consisting of polynomials corresponding to rules 1, 2', and 3 is a Gröbner basis.

7. Extension to other Structures

We have so far discussed how to compute a Gröbner basis of a polynomial ideal over a Euclidean domain; however, a method for computing a Gröbner basis of an ideal over a Euclidean domain which is not necessarily a polynomial ring, is subsumed in our approach since rules corresponding to the elements of E are also allowed.

Consider, for example, an ideal over the ring of integers, specified by a basis $B = (c_1, \ldots, c_k)$. Its Gröbner basis can be constructed using the algorithm discussed above. Corresponding to every element $c_i \in B$, there is a rule $c_i \rightarrow 0$. In this case, for computing a Gröbner basis, we do not have to compute even the critical pairs because after rewriting the rules, we will eventually get a single rule in the basis, which is the greatest-common-divisor (gcd) of c_i's. This single rule constitutes a Gröbner basis of the ideal specified by the input basis consisting of integers. Note that computing a Gröbner basis in this way is the same as applying Euclid's algorithm for computing the *gcd* of a finite set of integers. This is also analogous to computing a Gröbner basis of an ideal of univariate polynomials over a field using Buchberger's algorithm. Similarly, for $Z[i]$ or any Euclidean domain, we can compute a Gröbner basis of an ideal over it using our algorithm; this Gröbner basis consists of the element obtained by computing the gcd of the elements in the basis.

Note also that we can use our algorithm to compute a Gröbner basis of an ideal over Z mod p also, where p is an arbitrary integer. Z mod p can be a ring with zero divisors depending upon the value of p. Given an ideal over Z mod p specified by a basis, we augment the basis with p and compute a Gröbner basis of the ideal specified by the augmented basis over Z using our algorithm; the result after taking out the rule $p \rightarrow 0$ from it is a Gröbner basis of the ideal specified over Z mod p. A Gröbner basis of a polynomial ideal over Z mod p can also be computed in the same way by augmenting the basis with an additional element p and computing a Gröbner basis from the augmented basis. In fact, this is the approach adopted in computing a Gröbner basis of a polynomial ideal over a boolean ring in (Kapur and Narendran, 1985b). Our algorithm can thus be used for computing Gröbner bases of polynomial ideals over a Euclidean ring with zero divisors insofar as the Euclidean ring is presented as a quotient structure defined by an ideal over a Euclidean domain.

Based on (Kandri-Rody and Kapur, 1984c), Pan (1985) showed that the critical pair definition CP2 is adequate to compute weak Gröbner bases (called D-bases by Pan) for polynomial ideals over a principal ideal domain using which ideal membership can be decided, i.e., every polynomial in an ideal reduces to 0 using a D-basis of the ideal; see also (Kapur and Narendran, 1985c).

8. Uniqueness of a reduced Gröbner basis

In general, a Gröbner basis of a polynomial ideal need not be unique. A reduced Gröbner basis (see the definition in Section 4) of a polynomial ideal need not be unique either, even up to an admissible total ordering on terms. As the reduction relation is defined using a division algorithm over E, different division algorithms can result in different Gröbner bases for the same ideal. For a given division algorithm over E and a given admissible total ordering on terms, a reduced Gröbner basis for a polynomial ideal may still not be unique because of multiple units in E. Given a reduced Gröbner basis, it is possible to get another reduced Gröbner basis from it by

multiplying its elements by appropriate units.

As in the case of polynomial ideals over a field, we can "canonicalize" the head-coefficient of every polynomial in the basis. For the case when the ground ring is a field, every non-zero element is a unit; but, 1 is picked as a canonical element and it is required that the head-coefficient of every element in a reduced basis be that canonical element. Similarly as shown in (Kandri-Rody and Kapur, 1984b), if the ground ring is the ring of integers, the head-coefficient of each element in a reduced basis can be made positive. For a Euclidean domain, assume that it is possible to pick a canonical element from every equivalence class of associate elements; the function *canon* in (Kandri-Rody and Kapur, 1984c) is introduced to do this picking. In fact, there can be infinitely many ways to define a *canon* function. Assuming a *canon* function, it is easy to canonicalize head-coefficients of each polynomial in a reduced Gröbner basis by multiplying with appropriate units. Then, we get the following result:

Theorem 8.1: A reduced Gröbner basis of an ideal I in $E[x_1, \cdots, x_n]$ is unique subject to a division algorithm over E, an admissible ordering on terms and the selection of a *canon* function on E.

See (Kandri-Rody and Kapur, 1984c) for a proof. Similar results about the uniqueness of a reduced complete system have been reported in (Buchberger, 1976b) for polynomial ideals over a field, in (Kapur and Narendran, 1985a) for Thue systems and in (Lankford and Ballantyne, 1984) and (Metevier, 1984) for term rewriting systems.

9. Conclusion

We have developed a general Gröbner basis algorithm for polynomial ideals over a Euclidean domain based on a natural definition of reduction of polynomials using a single polynomial at a time and Euclid's division algorithm. There are many applications of the Gröbner basis computation; for details, see (Buchberger and Loos, 1982; Buchberger, 1985). Lauer (1976) showed that a Gröbner basis can be used to construct canonical forms for residue classes defined by a polynomial ideal over a polynomial ring. The unique reduced Gröbner basis of an ideal (subject to an admissible ordering and other conditions stated above) is useful in computing other structural properties of the ideal under consideration, such as its dimension, maximality, primality, primary decomposition of ideals, etc., especially when a lexicographic ordering on terms is used to compute a Gröbner basis, see (Kandri-Rody, 1984; Kandri-Rody and Saunders, 1984) for more details. The Gröbner basis computation is also related to solving uniform word problem over finitely presented commutative algebras whose generators play the same role as of indeterminates of the polynomial ring; see (Le-Chenadec, 1984; Buchberger, 1985; Kandri-Rody, Kapur, and Narendran, 1985) for details.

Hsiang (1985) developed a term rewriting approach to first-order theorem proving using the representation of first-order formulae in terms of the boolean connectives 'exclusive-or' and 'and.' Using this representation of first-order formulae, Kapur and Narendran (1985b) extended the concept of a Gröbner basis to theorem proving in first-order predicate calculus. The notions of a first-order ring on infinitely many indeterminates and a first-order ideal are introduced. It is shown how a first-order formula serves as a finite basis of a first-order ideal. Using Hilbert's Nullstellensatz, proving whether a first-order formula is unsatisfiable is equivalent to checking if the

ideal specified by the first-order formula is the whole first-order ring.

Recently Gröbner basis computations have been used for theorem proving in algebraic geometry; for further details and papers on this application, the reader may consult the proceedings of the SYMSAC-86 conference.

ACKNOWLEDGMENT: We thank Paliath Narendran and Bruno Buchberger for valuable suggestions and comments during the course of this research, Klaus Madlener and Jürgen Avenhaus for translating Trinks' paper as well as portions of Lauer's thesis, and Ron Book for encouragement. We also thank Bruno Buchberger and the referees for suggestions which led to improvements in the presentation.

References

Ayoub, C.W. (1983). On constructing bases for ideals in polynomial rings over the integers. *J. of Number Theory*, 17, 204-225.

Bachmair, L. and Buchberger, B. (1980). A simplified proof of the characterization theorem for Gröbner bases. *ACM-SIGSAM Bulletin*, 14/4, 29-34.

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

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

Buchberger, B. (1976b). Some properties of Gröbner bases for polynomial ideals. *ACM-SIGSAM Bulletin, 10/4*, 40, 19-24.

Buchberger, B. (1984). A critical-pair/completion algorithm in reduction rings. In: (E. Borger, G. Hasenjaeger, D. Rodding, eds.) *Proc. Logic and Machines: Decision Problems and Complexity*, Springer LNCS 171, 137-161.

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

Buchberger, B. and Loos, R. (1982). Algebraic simplification. In: (B. Buchberger, G.E. Collins, and R. Loos, eds.) *Computer Algebra: Symbolic and Algebraic Computation* Computing Suppl. 4, Springer Verlag, 11-43.

Collins, G.E. (1968). *The SAC-1 polynomial system.* University of Wisconsin, Madison, Computer Science Department, Tech. Report 115.

Hardy, G.H., and Wright, E.M. (1938). *An Introduction of the Theory of Numbers.* Oxford University Press, Oxford, England.

Huet, G. and Oppen, D. (1980). Equations and rewrite rules: A survey. In: (R. Book, ed.) *Formal Languages: Perspectives and Open Problems,* Academic Press, New York.

Kandri-Rody, A. (1984). *Effective methods in the theory of polynomial ideals,* Ph.D. Thesis, RPI, Troy, NY.

Kandri-Rody, A. and Kapur, D. (1983). *On relationship between Buchberger's* Gröbner *basis algorithm and the Knuth-Bendix completion procedure.* TIS Report No. 83CRD286, General Electric Research and Development Center, Schenectady, NY.

Kandri-Rody, A. and Kapur, D. (1984a). Algorithms for computing the Gröbner basis of polynomial ideals over various Euclidean rings. Proceedings of *EUROSAM '84*, Cambridge, England, Springer Verlag LNCS 174, 195-206.

Kandri-Rody, A. and Kapur, D. (1984b). Computing the Gröbner basis of polynomial ideals over the integers. Proceedings of *Third MACSYMA Users' Conference,* Schenectady, NY, 436-451.

Kandri-Rody, A. and Kapur, D. (1984c). *An algorithm for computing the Grö bner basis of a polynomial ideal over a Euclidean ring.* General Electric Corporate Research and Development Report No. 84CRD045, Schenectady, NY. (An expanded version of this paper.)

Kandri-Rody, A., Kapur, D., and Narendran, P. (1985). An ideal-theoretic approach to word problems and

unification problems over finitely presented commutative algebras. Proceedings of *First International Conference on Rewriting Techniques and Applications,* Dijon, France, Springer Verlag LNCS 202, 345-364.

Kandri-Rody, A. and Saunders, B.D. (1984). Primality of ideals in polynomial rings. Proceedings of *Third MACSYMA Users' Conference,* Schenectady, NY, 459-471.

Kapur, D. and Narendran, P. (1985a). The Knuth-Bendix completion procedure and Thue systems. *SIAM J. of Computing,* 14, 1052-1072.

Kapur, D. and Narendran, P. (1985b). An equational approach to theorem proving in first-order predicate calculus. Proc. of the *IJCAI-85,* Los Angeles, 1146-1153.

Kapur, D. and Narendran, P. (1985c). Existence and construction of a Gröbner basis of a polynomial ideal. In: Proceedings of a workshop on *Combinatorial Algorithms in Algebraic Structures,* September 30-October 4, 1985, Europaeische Akademie, Otzenhausen, Fachbereich Informatik Report, Univ. of Kaiserslautern, W. Germany.

Knuth, D.E. and Bendix, P.B. (1970). Simple word problems in universal algebras. In: (J. Leech, ed.) *Computational Problems in Abstract Algebras.* Pergamon Press, 263-297.

Lankford, D.S., and Ballantyne, A.M. (1977). *Decision procedures for simple equational theories with commutative-associative axioms: Complete sets of commutative-associative reductions.* Automatic Theorem Proving Project Report ATP-39, Dept. of Math. and Computer Science, University of Texas at Austin.

Lankford, D.S. and Ballantyne, A.M. (1983). *On uniqueness of term rewriting systems.* Unpublished Manuscript, Louisiana Tech University, Math. Dept.

Lauer, M. (1976a). Canonical representatives for residue classes of a polynomial ideal. *SYMSAC-76.* Yorktown Heights, NY, 339-345.

Lauer, M. (1976b). *Kanonische repraesentanten fuer die restklassen nach einem polynomideal.* Diplomarbeit, Univ. of Kaiserslautern, W. Germany.

Le-Chenadec, P. (1984). Canonical forms in finitely presented algebras. In: Proc. of *7th Intl. Conf. on Automated Deduction* Springer Verlag LNCS 170, NAPA Valley, Calif.

Loos, R. (1974). Towards A formal implementation of computer algebra. *EUROSAM-74,* 9-16.

Metevier, Y. (1983). About the rewriting systems produced by the Knuth-Bendix completion algorithm. *Information Processing Letters,* 16, 31-34.

Möller, H.M. (1985). *On the computation of Grö bner bases in commutative rings.* Unpublished manuscript, Fern University, W. Germany.

Möller, H.M., and Mora, F. (1986). New constructive methods in classical ideal theory. *J. of Algebra,* 100, 138-178.

Musser, D.R., and Kapur, D. (1982). Rewrite rule theory and abstract data type analysis. Proc. *Computer Algebra, EUROCAM, 1982,* Lecture Notes in Computer Science 144 (ed. Calmet), Springer Verlag, 77-90.

Oppenheim, A. (1934). Quadratic fields with and without Euclid's algorithm. *Math. Annalen,* 109, 349-352.

Pan, L. (1985). On the D-bases of ideals in polynomial rings over principal ideal domains. In: Proc. of the workshop *Combinatorial Algorithms in Algebraic Structures* at Europaeische Akademie, Otzenhausen, West Germany, Sept. 30- Oct. 4, 1985.

Peterson, G.L., and Stickel, M.E. (1981). Complete set of reductions for some equational theories. *JACM* 28, 233-264.

Richman, F. (1974). Constructive aspects of Noetherian rings. Proc. *American Math. Society,* 44/4, 436-441.

Schaller, S. (1979). *Algorithmic aspects of polynomial residue class rings.* Ph.D. Thesis, Computer Science Tech., University of Wisconsin, Madison, Rep. 370.

Shtokhamer, R. (1976). *A canonical form of polynomials in the presence of side relations.* Technion Haifa Israel, Tech. Rep. PH-76-25.

Shtokhamer, R. (1986). *Lifting canonical algorithms from a ring R to the ring R[x].* Unpublished Manuscript, Dept. of Computer and Information Sciences, Univ. of Delaware.

Szekeres, G. (1952). A canonical basis for the ideals of a polynomial domain. *American Mathematical*

Monthly, 59/6, 379-386.

Trinks, W. (1978). Ueber B. Buchberger's verfahern systeme algebraischer gleichungen zu loesen. *J. of Number Theory,* 10, 475-488.

van der Waerden, B.L. (1966). *Modern Algebra,* Vols. I and II, New York: Fredrick Ungar Publishing Co.

Zacharias, G. (1978). *Generalized Gröbner bases in commutative polynomial rings.* Bachelor Thesis, Lab. for Computer Science, MIT.