COMPUTING THE GRÖBNER BASIS OF AN IDEAL IN POLYNOMIAL RINGS OVER THE INTEGERS

Abdelilah Kandri-Rody
Dept. of Mathematical Sciences
Rensselaer Polytechnic Institute
Troy, New York 12181
and University Mohammed – V
Rabat, Morocco

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

ABSTRACT

An algorithm is developed for computing a Gröbner basis of an ideal in polynomial rings over integers. The algorithm is a natural extension of Buchberger's algorithm for computing a Gröbner basis of an ideal in polynomial rings over a field. The algorithm is implemented in ALDES and LISP and the implementation is discussed with a number of examples given. The uniqueness of the Gröbner basis of a polynomial ideal over the integers is shown.

1. INTRODUCTION

Buchberger [1,3,4] developed an algorithm for computing the Gröbner Basis of an ideal in polynomial rings over a field. This algorithm takes an ideal specified by a finite set of polynomials as its input and produces another finite basis of the ideal which can be used to simplify polynomials such that every polynomial in the ideal simplifies to 0 and every polynomial in the polynomial ring simplifies to a unique normal form. The algorithm has been found useful in algebraic simplification [5].

In this paper, we develop an algorithm to compute the Gröbner basis of an ideal in polynomial rings over the integers. The algorithm is a natural extension of Buchberger's algorithm. New polynomials to complete the basis are computed between pairs of polynomials in the basis, the reduction process is simple and, the minimal Gröbner basis thus obtained is unique. An implementation of an efficient version of this algorithm in ALDES and LISP, patterned after Huet's version [7] of the Knuth-Bendix completion procedure, is also discussed.

* Partially supported by NSF grant MCS-82-11621.
1.1 Related Work

According to Lauer [19], Szekeres [22] showed the existence of a canonical basis for ideals over a Euclidean ring and Shitokhamer developed a generalization of the construction suggested by Szekeres to define a canonical basis over a principal ideal domain. Schaller [21] proposed an algorithm to compute a Gröbner basis of an ideal over polynomials over a principal ideal domain; at the same time, Zacharias [24] developed a similar algorithm for an ideal in a polynomial ring in which the ideal membership and basis problems for homogeneous linear equations are solvable. In both Schaller’s and Zacharias’s approaches, new polynomials needed for a complete basis must be computed for every finite set of polynomials in the input basis; this computation needs solving homogeneous linear equations. The reduction process in their approach needs a computation of extended greatest common divisor over many lead-coefficients in the basis; their algorithm gives a Gröbner basis which is not necessarily unique. In contrast, our approach is simpler: the rewriting relation induced by a polynomial is defined in a natural way.

2. WELL-FOUNDED ORDERING ON POLYNOMIALS

Let \( Z \{X_1, \ldots, X_n\} \) be the ring of polynomials with indeterminates \( X_1, \ldots, X_n \) over the ring of integers \( Z \); it is assumed that \( X_1 < X_2 < \cdots < X_n \). A term is any product \( \prod_{i=1}^{n} x_i^{k_i} \), where \( k_i \geq 0 \); the degree of a term is \( \sum_{i=1}^{n} k_i \). A monomial is a term multiplied by a nonzero coefficient from \( Z \). A polynomial is a sum of monomials; such a polynomial is said to be in sum of products form, abbreviated as SPF (this form of polynomials has also been called distributive normal form in the literature). If no term appears more than once in a polynomial in SPF, it is said to be in simplified sum of products form, abbreviated as SSSP. An arbitrary polynomial which is not in SSSF can be transformed into an equivalent polynomial in SSSF using the rules of the polynomial ring. Henceforth, we will assume polynomials to be in SSSF.

The ordering on terms is defined using the degree of a term and terms of the same degree are ordered lexicographically (this ordering is the same as the one used by Buchberger in [1,3]). Terms \( t_1 = \prod_{i=1}^{n} x_i^{k_i} < t_2 = \prod_{i=1}^{n} x_i^{j_i} \) if and only if (1) the degree of \( t_1 < \) the degree of \( t_2 \), or (2) the degree of \( t_1 = \) degree of \( t_2 \) and there exists an \( i \geq 1 \), such that \( k_i < j_i \) and for each \( 1 \leq i' < i \), \( k_{i'} = j_{i'} \). This ordering is a total ordering and is well-founded. Another total well-founded ordering, for example, is the pure lexicographic ordering on terms based on a total ordering on indeterminates in which the degree of terms is not considered. The results of the paper hold for this total ordering also.

Let \( c \) and \( c' \) be two integers. We say that \( c \) is less than \( c' \), written as \( c << c' \), if and only if \( |c| < |c'| \) or \( (|c| = |c'|, c \) is positive and \( c' \) is negative). For example, \( 2 << -2, 2 << 3, 2 << -3, \) as well as \( -2 << -3 \). The ordering \( << \) on \( Z \) is total and well-founded.

Monomials are ordered using their terms and coefficients: Given two monomials \( m_1 = c_1 t_1 \) and \( m_2 = c_2 t_2, m_1 << m_2 \) if and only if \( t_1 < t_2 \), or \( (t_1 = t_2 \) and \( c_1 << c_2 \)). It is easy to see that the ordering \( << \) on monomials is total and well-founded.

Let \( p = m + r \) be a polynomial in SSSF such that the term of the monomial \( m \) is greater than those within \( r \), then \( m \) is called the head-monomial of \( p \), the term of \( m \) is called the head-term of \( p \) and the coefficient of \( m \) is called the head-coefficient of \( p \). We will call \( r \) the reductum of \( p \). The ordering \( << \) on monomials can be used to define a ordering \( << \) on polynomials in
the following way: polynomials \( p_1 \ll p_2 \) if and only if either (1) \( m_1 \ll m_2 \), or (2) \( m_1 = m_2 \) and \( r_1 \ll r_2 \), where \( m_i \) and \( r_i \) are, respectively, the head-monomial and reduct of \( p_i \), \( i = 1, 2 \). It is easy to see that the ordering \( \ll \) on polynomials in \( \mathbb{Z}[x_1, \ldots, x_n] \) is total and well-founded.

3. GRÖBNER BASIS OF AN IDEAL

Informally, a finite set \( B \) of polynomials, say \( \{p_1, \ldots, p_k\} \), in \( \mathbb{Z}[x_1, \ldots, x_n] \) is called a Gröbner basis for an ideal \( \mathfrak{i} \) generated by \( B \) if for any polynomial \( q \), 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 \([1,3]\). An equivalent definition is that for any polynomial \( p \) in the ideal \( \mathfrak{i} \) generated by \( B \), \( p \rightarrow 0 \). The Gröbner 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 examples, consider the ideal \( \mathfrak{i} \) generated by \( B = \{X^2 + 1, Y^2 + 1\} \) in \( \mathbb{Z}[X, Y] \); \( Y - X^2 \) is in \( \mathfrak{i} \) but does not reduce to 0, so \( B \) is not a Gröbner basis. However, \( B' = \{X^2 + 1, Y^2 + X, x^3 - Y\} \) is a Gröbner basis.

In order to precisely define a Gröbner basis of an ideal \( \mathfrak{i} \), it is necessary to define the rewriting relation induced by a polynomial.

3.1 Polynomials as Reduction Rules

Consider a polynomial \( P = m_1 + m_2 + \ldots + m_k \) in \( \mathbb{Z}[x_1, \ldots, x_n] \) in SSPF such that \( m_1 \) is the head-monomial of \( P \). Further, assume that its head term \( t_1 \) has a positive coefficient \( c_1 \) (i.e., \( m_1 = c_1 t_1 \)). Then the rewrite rule corresponding to \( P \) is as follows:

\[
c_1 t_1 \rightarrow - m_2 + \ldots + m_k
\]

In case the coefficient \( c_1 \) of the head term \( t_1 \) in \( P \) is negative, \( P \) is multiplied by \(-1\) and the result is used as a rewrite rule. In contrast to the rewrite rule for a polynomial over a field, where both the sides of the rule are divided by the head coefficient \( c_1 \) as division is defined on coefficients, the whole monomial is the left-hand-side (lhs). For example, the rewrite rule corresponding to \( 2x^2 y - y \) is \( 2x^2 y - y \).

A rule \( L \rightarrow R \), where \( L = c_1 t_1 \) and \( c_1 > 0 \) rewrites a monomial \( c t \) to \( (c - \epsilon c_1) t + \epsilon \sigma R \) where \( \epsilon = 1 \) if \( c > 0 \), \( \epsilon = -1 \) if \( c < 0 \), if and only if (1) there exists a term \( \sigma \) such that \( \epsilon t = \sigma t_1 \) and (2) either \( c > (c_1 / 2) \) or \( c < -(c_1 - 1) / 2 \). If \( -(c_1 - 1) / 2 \leq c \leq (c_1 / 2) \) or there does not exist any \( \sigma \) such that \( \epsilon t = \sigma t_1 \), then the monomial \( c t \) cannot be rewritten.

A polynomial \( Q \) is rewritten to \( Q' \) using the rule \( L \rightarrow R \) if and only if (1) \( Q = Q_1 + c t \) and \( c t \) is the largest monomial in \( Q \) which can be rewritten using the rule, and (2) \( Q' = Q_1 + (c - \epsilon c_1) t + \epsilon \sigma R \), where \( \epsilon = 1 \) if \( c > 0 \), \( \epsilon = -1 \) otherwise. If there is no monomial in \( Q \) which can be rewritten using the rule, then \( Q \) is irreducible or in normal form with respect to the rule. For example, using the rule \( 2x^2 y - y \), the polynomial

\[
4x^3 y + 5x^2 y^2 - 3x^2 y - 2x^3 y + xy + 5x y^2 - 3x^2 y - 2x y + 5x y^2 - 3x^2 y
\]

The result can be further reduced as the monomial \( -3x^2 y \) is reducible:

\[
-2x y + 5x y^2 - x^2 y - y - 2x y + 5x y^2 + x^2 y - 2y
\]

We assume that after rewriting by a polynomial, polynomials are always brought back to SSPF, i.e., indeterminates in terms are ordered using the prespecified ordering on indeterminates, equal terms are combined, and terms with zero coefficients are omitted (see also [3]).
Let $T = \{ L_1 \rightarrow R_1, \ldots, L_k \rightarrow R_k \}$ be the rule set corresponding to a basis $B = \{ p_1, \ldots, p_k \}$ of an ideal $I$ such that $\{ L_i \rightarrow R_i \}$ be the rule corresponding to $p_i$. Let $\rightarrow$ denote the rewriting relation defined by $T$.

### 3.2 Properties of Reduction Relations

We define properties of $\rightarrow$ which are needed for defining a Gröbner basis (an interested reader may want to refer to [5,6] for more details). Let $\rightarrow^*$ be the reflexive and transitive closure of $\rightarrow$ and $\rightarrow^+$ be the transitive closure of $\rightarrow$.

**Definition:** A relation $\rightarrow$ is Noetherian if and only if there does not exist any infinite sequence $x_0 \rightarrow x_1 \rightarrow x_2 \rightarrow \cdots$.

**Definition:** Two elements $x$ and $y$ are said to be joinable if and only if there exists $u$ such that $x \rightarrow^* u$ and $y \rightarrow^* u$.

**Definition:** A relation $\rightarrow$ is confluent if and only if for all $x$, $y$, $z$, such that $x \rightarrow^* y$ and $x \rightarrow^* z$, $y$ and $z$ are joinable.

**Definition:** A relation $\rightarrow$ is canonical if and only if $\rightarrow$ is Noetherian and confluent.

If the relation $\rightarrow$ is Noetherian, then the test for confluence reduces to a simple local test, called local confluence.

**Definition:** A relation $\rightarrow$ is locally confluent if and only if for each $x$, $y$, $z$, such that $x \rightarrow y$ and $x \rightarrow z$, $y$ and $z$ are joinable.

**Theorem 3.1 [Newman]:** A Noetherian relation $\rightarrow$ is confluent if and only if $\rightarrow$ is locally confluent.


### 3.3 Definition of Gröbner Basis

The Gröbner basis can be defined by requiring that the rewriting relation defined by a basis satisfies certain conditions. It is sufficient to require of a Gröbner basis $B$ that the relation $\rightarrow$ induced by $B$ is confluent. Since we are interested in developing algorithms, we put an additional requirement that $\rightarrow$ be Noetherian.

**Definition:** A basis $B$ is a Gröbner basis if the rewriting relation $\rightarrow$ induced by $B$ is canonical.

In order to develop a Gröbner basis test for polynomial ideals over $\mathbb{Z}$, we first show that $\rightarrow$ is Noetherian using the total well-founded ordering defined on polynomials in Section 2. Then, we develop a test for local confluence and use the above theorem to check whether a basis is a Gröbner basis.

**Lemma 3.2:** The rewriting relation $\rightarrow$ induced by any finite basis over $\mathbb{Z}[X_1, \ldots, X_n]$ is Noetherian.

**Proof:** Follows from the fact that for any polynomials $Q$, $Q'$, such that $Q \rightarrow Q'$, $Q' \ll Q$. $\Box$

The test for local confluence is developed in a way similar to the approach developed by Buchberger for polynomial ideals over a field [1,3,4,5]. We define critical pairs for a pair of polynomials in a basis. Then it is shown that if these critical pairs are trivial, $\rightarrow$ is locally-confluent.
3.4 Critical Pairs

Given two rules \( L_1 \rightarrow R_1 \) and \( L_2 \rightarrow R_2 \), where \( L_1 = c_1 t_1 \) and \( L_2 = c_2 t_2 \), such that \( c_1 \geq c_2 > 0 \). Its critical pair \(<p, q>\) is defined as: \( p = (c_1 - c_2) \lcm(t_1, t_2) + f_1 \ast R_2 \), and \( q = f_1 \ast R_1 \), where \( f_1 \ast t_1 = f_2 \ast t_2 = \lcm(t_1, t_2) \). Polynomials \( p \) and \( q \) are obtained from the superposition \( c_1 \lcm(t_1, t_2) \) by applying \( L_2 \rightarrow R_2 \) and \( L_1 \rightarrow R_1 \), respectively.

The above definition of critical pairs is a generalization of the definition used by Buchberger [1,3,4] for a field. In that case, since \( c_1 \) and \( c_2 \) are 1, the above definition reduces to taking the \( \lcm \) of the left-hand sides. As in the case of polynomials over rationals, for any pair of polynomials, there is exactly one critical pair.

**Example:** in \( \mathbb{Z}[X, Y] \), consider the basis \( B_1 = \{ 3X^2 Y - Y, 10X Y^2 - X \} \). The superposition of the two polynomials is \( 10X^2 Y^2 \), and the critical pair is \(<7X^2 Y^2 + Y^2, X^2>\).

It is easy to see that for the critical pair \(<p, q>\) of 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.

The **S-Polynomial** corresponding to a critical pair \(<p, q>\) is the polynomial \( p - q \).

**Definition:** A critical pair \(<p, q>\) is **trivial** if and only if its S-polynomial \( p - q \) can be reduced to 0 by applying at each step, among all applicable rules, a rule whose left-hand-side has the least coefficient.

The above restriction is necessary because of the way the rewriting relation is defined above. If we do not have this restriction, then there are bases for which all critical pairs are trivial but the bases are not Gröbner bases. For example, consider the basis \( B_2 = \{ 1, 6X^2 Y - Y, 2X Y^2 - X \} \). Its critical pair is \(<4X^2 Y^2 + X^2, Y^2>\), and the two polynomials are joinable if we apply rule 1 first and then rule 2 on the first polynomial.

3.5 Gröbner Basis Test

To test whether a given basis is a Gröbner basis, (1) get the rule set corresponding to the basis, and (2) check whether for each pair of distinct rules, the critical pair \(<p, q>\) is trivial. For example, the basis \( B_1 \) in the above example is not a Gröbner basis because the two polynomials in the critical pair \(<7X^2 Y^2 + Y^2, X^2>\) do not reduce to the same polynomial. The following theorem serves as the basis of this test.

**Theorem 3.3:** A basis \( B \) of polynomials in \( \mathbb{Z}[X_1, \ldots, X_n] \) is a Gröbner basis if and only if for every pair of polynomials in \( B \), the critical pair \(<p, q>\) is trivial.

**Proof:** By Lemma 3.2 above, \( - \) is Noetherian, so it is sufficient to show that the relation \(-\) induced by \( B \) is locally confluent if and only if the critical pairs are trivial.

Explanation of “only if”: Since \( - \) is both locally confluent and Noetherian, \( - \) is confluent. For every pair \( L_1 \rightarrow R_1 \) and \( L_2 \rightarrow R_2 \), where \( L_i = c_i t_i \), \( i = 1, 2 \), and \( c_1 \geq c_2 \), consider a polynomial \( p = c_1 t - f_1 R_1 \), where \( t = \lcm(t_1, t_2) = f_1 R_1 = f_2 R_2 \). Using \( L_1 \rightarrow R_1 \), \( p \) reduces to 0, whereas using \( L_2 \rightarrow R_2 \), \( p \) reduces to \((c_1 - c_2) t + f_2 R_2 - f_1 R_1 \). By confluence of \(-\), we have \((c_1 - c_2) t + f_2 R_2 - f_1 R_1 \) reduce to 0 no matter how it is rewritten. Hence, the critical pair of these rules is trivial.

Explanation of “if”: Consider a polynomial \( p \) which is rewritten in two different ways to \( q_1 \) and \( q_2 \). Let \( t' \) be the term of the largest monomial being rewritten and \( c \) be its coefficient in \( p \) (this is so, since the rewriting relation is defined to be rewriting the largest monomial, so the case when two different terms are being rewritten does not arise); let \( p = p' + ct' \). Let
Let $L_1 \rightarrow R_1$ and $L_2 \rightarrow R_2$ be the two rules being used to rewrite the monomial $c \ i'$; these rules must be distinct as otherwise we have $q_1 = q_2$. Without any loss of generality, we can assume that $c_1 \geq c_2$; let $t = \text{lcm}(t_1, t_2) = f_1 \ R_1 = f_2 \ R_2$, and $t' = \sigma \ t$. Then

\[ q_1 = p' + (c - c_1) \ t' + \epsilon \ \sigma \ \pi_1 \ R_1, \]  
\[ q_2 = p' + (c - c_2) \ t' + \epsilon \ \sigma \ \pi_2 \ R_2, \]

where $\epsilon = 1$ if $c > 0$, and -1 otherwise.

Since the S-polynomial $SP = (c_1 - c_2) \ t + f_2 \ R_2 - f_1 \ R_1$, corresponding to the critical pair of the two rules is trivial, $q_1$ and $q_2$ are joinable using Lemma 3.4 proved below. This is so because if $\epsilon = 1$, then $q_2 - q_1 = \sigma \ \pi \ SP$, whereas if $\epsilon = -1$, then $q_1 - q_2 = \sigma \ \pi \ SP$. □

**Lemma 3.4:** For any two polynomials $p$ and $q$, if $p - q \rightarrow^* 0$, then $p$ and $q$ are joinable.

The relation $\rightarrow^*$ is a subset of the relation $\rightarrow$ and is defined as: A monomial $c \ i \rightarrow q'$ if and only if $c \ i \rightarrow q$ 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 $c \ i$ and $c_1 < c_2$. A polynomial $P \rightarrow Q$ if and only if $Q$ is obtained from $P$ by rewriting the largest monomial under $\rightarrow^*$. The definition of a critical pair being trivial uses the rewriting relation $\rightarrow^*$.

Before we give a proof of the above lemma, we show the following property of $\rightarrow^*$, which is used in the proof of the above lemma.

**Lemma 3.5:** For any two polynomials $p$, $q$ such that $p - q \rightarrow^* h$ and $h \rightarrow^* 0$, there exist $p'$, $q'$, such that $h = p' - q'$ and $p \rightarrow^* p'$ and $q \rightarrow^* q'$.

**Proof:** Suppose that $p - q$ is reduced to $h$ by a rule $c \ i \rightarrow R$. Let $p = R_p + d_p \ t'$, $q = R_q + d_q \ t'$, $d = d_p - d_q$. Then $h = (R_p - R_q) + (d_p - d_q - c) \ t' + \epsilon \ \sigma \ R$, where $t' = \sigma \ t$. There are two cases: (1) $d > c/2$ and (2) $d < -(c - 1)/2$.

**Case 1:** $d > c/2$: This implies $d_p > d_q - c/2$ and $h = (R_p - R_q) + (d_p - d_q - c) \ t' + \sigma \ R$. There are two subcases:

Subcase 1: $d_q \geq 0$, which implies $d_p > c/2$, hence $d_q$ is not a remainder of $c$. So, we reduce $p$ to $p' = R_p + (d_p - c) \ t' + \sigma \ R$. We take $q' = q$.

Subcase 2: $d_q < 0$: If $d_q < -(c - 1)/2$ then we reduce $q$ to $q' = R_q + (d_q + c) \ t' + \sigma \ R$ and we take $p' = p$.

If $0 > d_q \geq -(c - 1)/2$, then $d_p > 0$. If $d_p > c/2$ then we take $p' = R_p + (d_p - c) \ t' + \sigma \ R$ and $q' = q$. If $d_p \leq c/2$ then $c/2 < (d_p - d_q) \leq (c/2 + (c - 1)/2)$ and $d_p - d_q - c$ is a remainder of $c$. This implies that $h$ cannot be reduced to 0 since in $\rightarrow^*$, we require that the rewriting be done using a rule with the smallest head-coefficient. This is a contradiction.

**Case 2:** $d < -(c - 1)/2$: This implies $d_p > d_q + (c - 1)/2$ and $h = (R_p - R_q) + (d_p - d_q + c) \ t' + \sigma \ R$. There are two subcases:

Subcase 1: $d_q > 0$, which implies $d_q > c/2$, hence $d_q$ is not a remainder of $c$. So, we reduce $q$ to $q' = R_q + (d_q - c) \ t' + \sigma \ R$. We take $p' = p$.

Subcase 2: $d_q \leq 0$: If $d_p < -(c - 1)/2$ then we reduce $p$ to $p' = R_p + (d_p + c) \ t' + \sigma \ R$ and we take $q' = q$.

If $0 \geq d_q \geq -(c - 1)/2$, then $d_q \geq 0$. If $d_q > c/2$ then we take $q' = R_q + (d_q - c) \ t' + \sigma \ R$ and $p' = p$. If $d_q \leq c/2$ then $(c - 1)/2 < (d_p - d_q) \leq (c/2 + (c - 1)/2)$ and $d_p - d_q + c$ is a remainder of $c$. This implies that $h$ cannot be reduced to 0 since in $\rightarrow^*$, we require that the rewriting be done using a rule with the smallest head-coefficient. This is a contradiction. □

We now give the proof of Lemma 3.4.
Proof: Let $p - q \rightarrow^n 0$. The proof is by induction on $n$. The basis step of $n = 0$ is trivial, as in that case, $p = q$.

Inductive Step: Assume for $n' < n$, to show for $n$.

Let $p - q \rightarrow^0 h \rightarrow^0 0$. By the above lemma, there exists $p'$ and $q'$ such that $h = p' - q'$, $p \rightarrow p'$ and $q \rightarrow q'$. By inductive hypothesis on $h$, $p'$ and $q'$ are joinable. So, $p$ and $q$ are joinable. $\Box$

Another way of showing the correctness of the Gröbner basis test is to use the approach developed in [10] to show the relationship between Buchberger’s Gröbner basis algorithm for polynomial ideals over a field and the Knuth-Bendix completion procedure. The polynomial simplification process is decomposed into two parts: reduction relation and simplification relation. The rules corresponding to the polynomials in the basis are in the reduction relation, whereas $x + 0 = 0$ and $x + x = x$ are the only axioms in the simplification relation. In [10], it is shown that the canonicalization of a polynomial obtained after combining reduction and simplification such that simplification is performed before each step of reduction (as is done in Buchberger’s Gröbner basis algorithm as well as in the implementation of our Gröbner basis algorithm over $\mathbb{Z}$) is the same as the canonicalization obtained if reduction is completely performed first, followed by simplification at the end. Using this approach, the correctness of the Gröbner basis test is shown by proving a theorem similar to Theorem 4.12 in [10]; an interested reader may look at [9] for details.

4. GRÖBNER BASIS ALGORITHM

If a basis is not a Gröbner basis, it can be completed to get a Gröbner basis. The completion procedure is very much like the Knuth-Bendix completion procedure for term rewriting systems. For every non-trivial critical pair $<p, q>$, add a new rule corresponding to a normal form of the polynomial $p - q$ using the relation $\rightarrow^*$, thus generating a new basis for the same ideal. This step is repeated until for each pair of polynomials in the basis, the critical pair is trivial.

Example: In $\mathbb{Z}[X, Y]$, consider the basis $B = \{1, 2X^2Y - Y, 2, 3X, Y^2 - X\}$, we first add the rule obtained by critical pair of rules 1 and 2: i.e., $3$. $X^2Y^2 \rightarrow - Y^2 + X^2$. From rules 1 and 3, we get the critical pair $<X^2Y^2 - Y^2 + X^2, Y^2>$ which gives an additional rule: $4$. $3Y^2 \rightarrow 2X^2$.

Using rule 4, rule 2 can be reduced to $2'$. $2X^2 - X$.

The above 4 rules constitute a Gröbner basis because every critical pair is trivial. There is no need to reduce rule 2 using rule 4, however, doing so turns out to be more efficient and also results in a unique Gröbner basis subject to an ordering on indeterminates. This will be discussed later in the paper.

One may think that the Gröbner basis of an ideal $I$ in $\mathbb{Z}[X_1, \ldots, X_n]$ could be obtained by first (1) generating the Gröbner basis $B$ of $I$ using Buchberger’s algorithm over rationals and then (2) clearing the denominators of each polynomial in $B$ to get the corresponding polynomials in $\mathbb{Z}[X_1, \ldots, X_n]$.

This construction does not work. As illustrated by the above example, using this construction, we get

$$B' = \{1, 2X^2Y - Y, 2', 2X^3 - X, 4, 3Y^2 - 2X^2\}$$

which is not a Gröbner basis.
The Gröbner basis algorithm for polynomial ideals over \( Z \) is given below. It is patterned after Huet’s version [7] of the Knuth-Bendix completion procedure. Note that the basis being used for reduction is always kept in reduced form.

**ALGORITHM:**

Given \( F \), a finite set of polynomials in \( Z[x_1, \ldots, x_n] \),

find \( G \) such that \( \text{ideal}(F) = \text{ideal}(G) \) and \( G \) is a Gröbner basis.

Initialization: \( T_0 := F ; \ G_0 := \emptyset ; \ i := 0 ; \ m := 0 ; \)

**LOOP**

\[
\text{WHILE} \ T_i \neq \emptyset \ \text{DO}
\]

\[
\begin{align*}
\text{reduce polynomial: select polynomial } P \text{ in } T_i \\
\text{hm and red are head monomial and reductum of normalized } P, \text{ respectively.}
\end{align*}
\]

\[
\text{IF } \text{hm} = 0 \ \text{THEN} \ \{ \ T_{i+1} := T_i - \{ P \} ; \ G_{i+1} := G_i ; \ i := i + 1 ; \} \\
\text{ELSE} \ \{ \ \text{Add new polynomial: let } K \text{ be the set of labels } k \text{ of polynomials of } G_i \\
\text{whose head term } \text{hm}_k \text{ is reducible by (hm, red);} \\
T_{i+1} := (T_i - \{ P \}) \cup \{ (\text{hm}_k, \text{red}_k), \ k \text{ belongs to } K \}; \\
m := m + 1; \\
G_{i+1} := \{ j : (\text{hm}_j, \text{red}_j) \mid j : (\text{hm}_j, \text{red}_j) \text{ in } G_i \text{ and } j \notin K \} \cup \{ n : (\text{hm}, \text{red}) \}; \\
\text{normalize}(G_i \cup \{ m : (\text{hm}, \text{red}) \}, \text{red}_j) \\
\text{the new polynomial } m : (\text{hm}, \text{red}) \text{ is unmarked; } \\
i := i + 1 \}
\]

**ENDWHILE**;

compute critical pairs: IF all polynomials in \( G_i \) are marked

THEN EXITLOOP (\( G \), canonical);

ELSE \{ \ select an unmarked polynomial in \( G_i \), say with label \( k \); \\
\( T_{i+1} := \) the set of all critical pairs computed between polynomial \( k \) and \nany polynomial of \( G_i \) of label not greater than \( k \); \\
\( G_{i+1} := G_i \), except that polynomial \( k \) is now marked; \\
i := i + 1 \}

**ENDLOOP.**

\( G := G_i. \)

Since \( Z[x_1, \ldots, x_n] \) is a Noetherian ring, the termination of the process of generating critical pairs and augmenting the basis is guaranteed because of the finite ascending chain condition of properly contained ideals over a Noetherian ring as shown below. The following theorem establishes that a version of the algorithm in which \( G_i \) and \( T_i \) are not separated and \( T_i \) is reduced immediately using \( G_i \), will terminate (in the proof below, \( G_i \cup T_i = TG_i. \)). The proof that the above algorithm terminates is a special case of the following proof because the loop for \( T_i \) is always guaranteed to terminate.

**Theorem 4.1:** The Gröbner Basis Completion Algorithm always terminates.

**Proof:** Let \( TG_i = (B_1^i, \ldots, B_n^i) \) be the basis at the \( i \)-th iteration of the Gröbner basis algorithm. Let \( M_j = C_j H_j \) be the head-monomial of the polynomial \( B_j \) in the basis \( TG_i \), where \( C_j \) and \( H_j \) are the head-coefficient and head-term of \( B_j \), respectively. Let \( B_{i+1}^{n+1} \) be the polynomial corresponding to the nontrivial critical pair, if any, generated in the \( i \)-th iteration to get \( TG_{i+1} \) from \( TG_i. \)
From $TG_1$, we construct another basis $S$, made only of the head-terms of the polynomials in $TG_1$, i.e., $S = (H^1, \ldots, H^k)$.

We first show that the ideal of $S$ is a subset of the ideal of $S_{i+1}$, written as $S \subseteq S_{i+1}$.

If in the $i$-th iteration, no nontrivial critical pair is generated, then $TG_{i+1} = TG_i$, so $S_{i+1} = S_i$. Consider the case when a nontrivial critical pair is generated in the $i$-th iteration. There are two cases:

1. $B_{i+1}^{j-1}$ does not reduce the head-monomial of any polynomial in $TG_i$: then $S_{i+1} = S_i \cup \{H^{j-1}_{i+1}\}$, implying that $S_i \subseteq S_{i+1}$.

2. $B_{i+1}^{j+1}$ reduces the head-monomial of some polynomials in $TG_i$. So there exist $1 \leq j \leq k_i$ (could be more than one $j$) and a term $\sigma$, $H^j = \sigma H^{j-1}_{i+1}$. In that case, $S_i$ is a subset of $S_{i+1}$ even though $H^j$ may not be in the basis of $S_{i+1}$.

Further, for any $i$, since $TG_i$ is finite, it is only possible to add finitely many polynomials (bound by the largest head-coefficient in $TG_i$) to $TG_i$ so that the corresponding $S_i$ remains invariant. This is so because in order to have $S_i = S_{i+1}$, we must have $H^{j-1}_{i+1}$ so that there exist $j$, $\sigma$, $H^{j+1}_{i+1} = \sigma H^j$ and for $B_{i+1}^{j+1}$ to be irreducible with respect to $TG_i$, $-(Cj - 1)/2 \leq C^{j+1}_{i+1} \leq Cj/2$ for all such $j$.

(As if, there does not exist $j$, $\sigma$, such that $H^{j+1}_{i+1} = \sigma H^j$, then $H^{j+1}_{i+1}$ is not in $S_i$, so $S_i$ is a proper subset of $S_{i+1}$.)

However, if the process of generating new rules does not terminate, then there is an infinite sequence of ideals $S_1 \subseteq S_2 \subseteq \cdots \subseteq S_i \ldots$ such that there does not exist any $s$ for which $S_s = S_{i-1} = S_{i-2} = \ldots$. This leads to a contradiction because for a Noetherian ring of polynomials, such an infinite ascending chain of ideals does not exist (van der Waerden, Vol. II, p. 117, second formulation). □

Note that if we had assumed that when a new rule is added to $TG_i$, it is not used to simplify $TG_i$ (as in another version of the Gröbner basis algorithm given in the Appendix, which is patterned after Buchberger’s algorithm for polynomial ideals over a field), then $TG_{i+1} = TG_i \cup \{B_{i+1}^{j+1}\}$, then the above proof simplifies because in that case, there is no need to consider case (2) above.

The above algorithm has been implemented in ALDES (Algorithm Description Language developed by Collins and Loos) as well as in LISP with various strategies for normalizing a polynomial and choosing a polynomial from $T_i$. We found it is better to choose the smallest polynomial $P$ in $T_i$. The normalization of $P$ with respect to a basis $G_i$ is done step by step starting with the head-monomial of $P$, reducing it with respect to $G_i$, taking the second highest monomial, reducing it and so on.

We also found that for many examples, a reduction check starting with the largest rule in $G_i$ first was more efficient than that starting with the smallest rule. To generate the critical pairs we can choose an unmarked polynomial whose superposition with all the marked one’s is the smallest one. If we compute all critical pairs and we reduce the basis at the end, we may run out of all available storage before finding the Gröbner basis. However, if we reduce the basis each time we add a new critical pair, the algorithm works much better. The above implementation takes care of these two problems, i.e., space and time. Different strategies for generating critical pairs discussed in [13] can also be implemented. The next section contains some examples which were run on this implementation.
5. EXAMPLES

We have run many examples (some of which were provided by Lankford) in the ALDES implementation. Some of these examples and their Gröbner bases are reproduced below.

**Example 1:** In $\mathbb{Z}[X, Y, W]$, $X < Y < W$, consider the ideal generated by

1. $-W + X Y^2 + 4 X^2 + 1$
2. $Y^2 W + 2X + 1$
3. $-X^2 W + Y^2 + X$

The canonical Gröbner basis is

1. $W^2 - W - 4 Y^2 + 2 X^2 - 3 X$
2. $- W + X Y^2 + 4 X^2 + 1$
3. $X^2 W - Y^2 - X$
4. $Y^2 W + 2 X + 1$
5. $-3 X W - Y^2 + 2 X^4 + 13 X^3 + X - 1$
6. $W + Y^4 + 2 X^3 - 3 X^2 - 1$

**Example 2:** In $\mathbb{Z}[X, Y, W]$, $X < Y < W$, consider the ideal generated by

1. $2 X^3 Y^3 W^5 + 5 X Y^2 + X W - 6 Y$
2. $X^2 + 2 X + 1$
3. $X^2 Y^2 - 1$
4. $8 X Y W - 8$
5. $6 X + 3 Y + 2 W$

The canonical Gröbner basis is 1.

**Example 3:** In $\mathbb{Z}[X, Y]$, $X < Y$, consider an ideal $I$ generated by:

1. $Y^6 + X^4 Y^4 - X^2 Y^4 - Y^4 - X^4 Y^2 + 2 X^2 Y^2 + X^6 - X^4$
2. $2 X^3 Y^3 - X Y^2 - 2 X^3 Y^2 + 2 X Y^3 + 3 X^5 - 2 X^3$
3. $3 Y^5 + 2 X^4 Y^3 - 2 X Y^3 - 2 Y^3 - X^4 Y + 2 X^2 Y$

The canonical Gröbner basis is:

1. $4 Y^4 + 4 X^4 Y^2 - 8 X^2 Y^2 - 4 X^6 + 4 X^4$
2. $X^2 Y^4 + 2 Y^4 + 2 X^4 Y^2 - 6 X^2 Y^2 - 3 X^6 + 4 X^4$
3. $4 X Y^5 - 8 X Y^3 - 4 X^3 Y + 8 X^3 Y$
4. $Y^6 + X^4 Y^2 - 2 X^2 Y^2 - 2 X^6 + 2 X^4$
5. $-X Y^4 + 2 X^3 Y^2 + 2 X Y^2 + 2 X^7 - X^6 - 2 X^3$
6. $2 Y^5 + 4 X^2 Y^3 - 4 Y^3 + 4 X^6 Y - 6 X^4 Y + 4 X^2 Y$
(7) \(3 \, x^5 + 2 \, x^4 \, y^3 - 2 \, x^2 \, y^3 - 2 \, y^3 - x^4 \, y + 2 \, x^2 \, y\)
(8) \(3 \, x^4 + 2 \, x^6 \, y^2 + 2 \, x^4 \, y^2 - 2 \, x^2 \, y^2 + x^8 - 2 \, x^6 - x^4\)
(9) \(2 \, x^5 \, y^2 + 2 \, x^2 \, y^2 + x^9 - 2 \, x^3\)
(10) \(4 \, x^2 \, y^3 - 2 \, y^3 + x^8 \, y + 2 \, x^6 \, y - 4 \, x^2 \, y + 2 \, x^2 \, y\)

6. OPTIMIZATION

Using the definition of critical pairs given in Section 3 (henceforth called definition CP1), many intermediate rules are generated which later get simplified and thus do not appear in the Gröbner basis as illustrated by the following example:

The basis \(B = \{1, \, 13 \, x^2 \, y - y, \, 2, \, 8 \, x \, y^2 - x\}\)

Using definition CP1, we get from the superposition of rules 1 and 2, \(<5 \, x^2 \, y^2 + x^2, \, y^2>\) as the critical pair, which gives a rule:

3. \(3 \, x^2 \, y^2 - y^2 + 2 \, x^2\).

Rules 2 and 3 give a critical pair \(<5 \, x^2 \, y^2 - y^2 + 2 \, x^2, \, x^2>\), which gives the rule:

4. \(x^2 \, y^2 - 3 \, y^2 + 5 \, x^2\),

Rule 4 simplifies 3 to:

3'. \(8 \, y^2 - 13 \, x^2\).

Rule 3' simplifies rule 2 above to:

2'. \(13 \, x^3 - x\).

Rules 1, 2', 3' and 4 constitute a Gröbner basis.

The above computation can be optimized using the following definition of critical pairs:

**Definition CP2**: The critical pair for two rules \(c_1 \, t_1 - R_1\) and \(c_2 \, t_2 - R_2\), where \(c_1 \geq c_2\) is: let \(t = \text{lcm} (t_1, t_2) = f_1 \, t_1 = f_2 \, t_2\) and \(c_1 = a \, c_2 + b\), \(-\left(\frac{c_2 - 1}{2}\right) \leq b \leq \frac{c_2}{2}\), then the superposition of the two left-hand-sides is the monomial \(c_1 \, t\) from which by applying the two rules, we obtain the critical pair \(<p, \, q>\), \(p = b \, t + a \, f_2 \ast R_2\) and \(q = f_1 \ast R_1\).

It is again easy to see that the polynomial \(p - q\) obtained from the critical pair \(<p, \, q>\) as defined above is still in the ideal.

As should be evident from the above discussion, rule 4 can be obtained directly from rules 1 and 2 by the greatest common divisor computation on the coefficients. This suggests a further optimization of definition CP2 using the gcd computation on the coefficients of the left-hand-sides of rules.
Definition CP3: The critical pair for two rules $c_1 t_1 \rightarrow R_1$ and $c_2 t_2 \rightarrow R_2$, where $c_1 > c_2$ or $c_1 = c_2$ is defined as follows:

1. if $c_2$ divides $c_1$, we generate the critical pair using the lcm of $c_1 t_1$ and $c_2 t_2$ as the superposition and we obtain $p$ and $q$ by applying the given rules respectively. This case is the same as Definition CP2. Since lcm of $c_1$ and $c_2$ is $c_1$, suppose $c_1 = k c_2$, then, $p = f_1 R_1$ and $q = k f_2 R_2$; otherwise.

2. if $c_2$ does not divide $c_1$, we generate the critical pair using the gcd. Let $c$ be the extended gcd of $c_1$ and $c_2$; there exist $a$ and $b$ such that $c = a c_1 + b c_2$. Then the superposition of the two rules is $a c_1 f_1 t_1 + b c_2 f_2 t_2$, and the critical pair $<p,q>$ is: $p = c \text{lcm}(t_1, t_2)$ and $q = a f_1 R_1 + b f_2 R_2$.

Note that $<p,q>$ can be derived using the definition CP2 of critical pairs from the rules $c_1 t_1 \rightarrow R_1$ and $c_2 t_2 \rightarrow R_2$ by mimicking the gcd computation of $c_1$ and $c_2$.

We will now illustrate definition CP3 on the above example. The extended gcd of 13 and 8, the coefficients of the left-hand-sides of rules 1 and 2, respectively, is 1 such that $1 = (-3)^* 13 + (5)^* 8$. So, the critical pair of rules 1 and 2 using definition CP3 is $<X^2 Y^2, -3 Y^2 + 5 X^2>$, which directly gives rule 4. From rules 1 and 4, we get another rule:

$$6. \quad 40 Y^2 = 65 X^2,$$

and from rules 2 and 4, we get another rule:

$$7. \quad 24 Y^2 = 39 X^2.$$

Definition CP3 on rules 6 and 7 produces rule 3' using which we get the Gröbner basis. As should be evident from this example, although definition CP3 using the extended gcd computation helps in directly generating certain rules (e.g., 4) without having to go through intermediate rules (e.g., 3), yet in order to generate other rules (e.g., 3'), it ends up generating other intermediate rules (e.g., 6 and 7). So, for some cases, definition CP3 works better than definition CP2 while in other cases, definition CP2 works better than definition CP3.

7. UNIQUENESS OF MINIMAL GRÖBNER BASIS

Definition: A Gröbner basis $B = (b_1, ..., b_m)$ is minimal (or reduced) if and only if for each $i$, $1 \leq i \leq m$, the head-coefficient of $b_i$ is positive and $p_i$ cannot be rewritten by any other polynomial in $B$ when viewed as a rewrite rule.

Theorem 7.1: Let $B = (b_1, \cdots, b_m)$ be a basis of an ideal $I$ in $\mathbb{Z}[X_1, \cdots, X_n]$. Then, a minimal Gröbner basis of $I$ is unique subject to a total ordering on indeterminates $X_1, ..., X_n$.

Proof: By contradiction. Assume that $I$ has two minimal Gröbner bases $B = (b_1, \cdots, b_u)$ and $B' = (b'_1, \cdots, b'_v)$. Let $L_1 \rightarrow R_1$ be the rule for $b_1$ and $L'_1 \rightarrow R'_1$ be the rule for $b'_1$. Assume also that the rules are ordered corresponding to their polynomials in both bases, i.e., $L_1 \rightarrow R_1 < \cdots < L_u \rightarrow R_u$ and $L'_1 \rightarrow R'_1 < \cdots < L'_v \rightarrow R'_v$.

Let $i$, $1 \leq i \leq u$, be the smallest rule number where the two bases differ. That is, $b_i$ and $b'_i$ are not identical, and for all $j \geq 1$ and $j < i$, if any, $b_j = b'_j$. There are two possibilities because of the same ordering being used on indeterminates $X_1, ..., X_n$ for both bases: (1) $L_i \neq L'_i$, or (2) $L_i = L'_i$, but $R_i \neq R'_i$.

Case (1): $L_i \neq L'_i$. Without any loss of generality we can assume that $L_i < L'_i$ since monomials are totally ordered.
The polynomial $b_i$ is in $I$, and since $B'$ is a Gröbner basis, $b_i$ must reduce to 0 using polynomials in $B'$. But only rules corresponding to $b'_j$, for $j \geq 1$ and $j < i$, if any, can be applied on $b_i$, which means that $i > 1$, as otherwise $b_1$ is not in $I$, which is a contradiction. The above also implies that $b_i$ can also be reduced by polynomials in $B$, since for all $1 \leq j < i$, $b_i = b'_j$, which is a contradiction as $B$ is a reduced basis.

Case (2): \( L = L_j' \) but \( R_i \neq R_i' \). This implies that \( p = R_i - R_i' \) must reduce to 0. Let \( i_k \) be the head-term of \( p \) with a non-zero coefficient \( d \) (such a \( i_k \) must exist as otherwise \( R_i = R_i' \)). Let \( d \) and \( d'_j \) be the coefficients of \( i_k \) in \( R_i \) and \( R_i' \), respectively, so \( d = d - d'_j \). For \( R_i - R_i' \) to reduce to 0 there must be a rule \( L_j - R_j \), \( 1 \leq j < i \) (because \( i_k \) is the head-term of \( L_i \)), in both \( B \) and \( B' \) which reduces \( i_k \). Consider a rule whose left-hand-side has the least coefficient; say, that rule is \( L_j - R_j \), where \( L_j = c \, i_j \). Since \( B \) and \( B' \) are reduced, \( d \) and \( d'_j \) such that \( -\frac{(c - 1)}{2} \leq d \neq d'_j \leq \frac{c}{2} \). There does not exist any \( k \) such that \( d = k \, c \), which implies that \( R_i - R_i' \) cannot be reduced to 0 either using \( B \) or using \( B' \), since \( c \) is the smallest coefficient of the left-hand-sides of all the rules that can be applied to \( i_k \). Hence, \( R_i \neq R_i' \). (In a reduced basis, there cannot be two polynomials with the same head-term.)

So, there is no \( i \) such that \( b_i \) is different from \( b_i' \). To show that \( u = v \) implying that \( B = B' \), assume \( v > u \), in which case \( b'_v \) is in \( I \) such that \( b'_v \) reduces to 0 using \( B \). But then, \( b'_v \) reduces using \( \{b_j', \cdots, b_i'\} \) in \( B' \), which is a contradiction since \( B' \) is reduced. Hence the proof. \( \square \)

Similar results about the uniqueness of a reduced canonical system have been reported in [12] for Thue systems and [15] for term rewriting systems; see also [16].

8. CONCLUSION

We have developed a Gröbner basis algorithm for polynomial ideals over \( \mathbb{Z} \). Similar argument can be used to get a Gröbner basis algorithm for finitely presented abelian groups. Implementations of these algorithms have been done in ALDES and LISP. Lauer [19] showed that the Gröbner basis can be used to construct canonical representatives for ideal residue classes. Since our algorithm computes a unique Gröbner basis of an ideal, in presence of such a basis, every polynomial in the polynomial ring has a canonical form. Moreover, the unique Gröbner basis of an ideal gives us insight into the structure of the ideal under consideration, such as its dimension, maximality, primality, etc., especially when the pure lexicographic ordering on monomials is used to compute the Gröbner basis, see [9] for more details.

Lankford [personal communication, Sept. 1983] suggested that there might be a relationship between the Gröbner basis computation and word problems over finitely presented algebras. It turns out that computing the Gröbner basis of a polynomial ideal over \( \mathbb{Z} \) solves the uniform word problem (for elementary terms) over a finitely presented commutative ring with unity. The generators of the finitely presented commutative ring play the same role as the indeterminates of the polynomial ring over \( \mathbb{Z} \). The Gröbner basis is the canonical system for the finitely presented commutative ring. Further, a set of polynomials of the form \( t_1 - t_2 \), where \( t_i, i = 1, 2, \), is a term, can be treated as a presentation of a finitely presented commutative semi-group, so computing the Gröbner basis of the ideal generated by this set of polynomials also solves the word problem (for elementary terms) of the corresponding commutative semi-group (see [2] for an alternative but related approach). In a similar way, if the definition of critical pairs given in Section 3.4 is changed slightly so as not to consider the * operation of the polynomial ring, the Gröbner basis computation solves the uniform word
problem (for elementary terms) for finitely presented abelian groups. See [18] where an approach using a commutative-associative completion procedure is discussed for solving the uniform word problem for finitely presented abelian groups. The Gröbner basis approach for solving the uniform word problem for finitely presented abelian groups can also be used to solve the abelian group unification problem for elementary terms (see [17] for a different approach for solving this problem).

By adding additional polynomials (namely, $2 = 0$ and for each indeterminate $x_i$, $x_i \cdot x_i = x_i$) into a basis over $Z[x_1, \ldots, x_n]$, we can simulate polynomial ideals over a boolean ring. Thus, the Gröbner basis algorithm over $Z$ can be used as a way to prove theorems in propositional calculus by showing the unsatisfiability of a formula in conjunctive normal form; this method is closely related to Hsiang’s approach [8]. The Gröbner basis approach also solves the uniform word problem (for elementary terms) for finitely presented boolean rings.

ACKNOWLEDGMENTS:

We thank Paliath Narendran for his helpful comments and suggestions on various drafts of this paper. Richard Harris implemented the algorithm in LISP on Symbolics 3600.

9. REFERENCES


APPENDIX

G := F
k := size(G)
i := 1
while i ≤ size(G) do
j := 1
while 1 ≤ j < i do
<p, q> := critical_pair(G[j], G[i]);
<hm, red> := normalize (G, S-polynomial (p,q));
if hm ≠ 0 then { G[k+1] := hm + red;
                 k := k + 1 };

j := j + 1;
endwhile
i := i + 1;
endwhile