AN IDEAL-THEORETIC APPROACH TO WORD PROBLEMS AND UNIFICATION PROBLEMS OVER FINITELY PRESENTED COMMUTATIVE ALGEBRAS

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

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

ABSTRACT

A new approach based on computing the Gröbner basis of polynomial ideals is developed for solving word problems and unification problems for finitely presented commutative algebras. This approach is simpler and more efficient than the approaches based on generalizations of the Knuth-Bendix completion procedure to handle associative and commutative operators. It is shown that (i) the word problem over a finitely presented commutative ring with unity is equivalent to the polynomial equivalence problem modulo a polynomial ideal over the integers, (ii) the unification problem for linear forms is decidable for finitely presented commutative rings with unity, (iii) the word problem and unification problem for finitely presented boolean polynomial rings are co-NP-complete and co-NP-hard respectively, and (iv) the set of all unifiers of two forms over a finitely presented abelian group can be computed in polynomial time. Examples and results of algorithms based on the Gröbner basis computation are also reported.

Key Words: Word Problem, Unification Problem, Finitely Presented Algebras, Commutative Algebras, Gröbner Basis, Polynomial Ideals, Term Rewriting, Knuth-Bendix Completion Procedure.

† This work was done when Kandri-Rody was a graduate student at Rensselaer Polytechnic Institute, Troy, NY.
* Partially supported by the National Science Foundation grant MCS-82-11621.
1. INTRODUCTION

We present a new approach for developing decision procedures for word problems and unification problems for finitely presented commutative algebraic structures. The approach is based on the Gröbner basis computation developed for polynomial ideals over the ring of integers in [10,12] and is simpler and more efficient for implementation than the approaches based on generalizations of the Knuth-Bendix completion procedure to handle associative and commutative (AC) operators developed in [16,23]. For related approaches for computing a Gröbner basis of a polynomial ideal over the integers, also see [4,20,24,28].

The results reported in this paper are:

1. the word problem over a finitely presented commutative ring with unity is equivalent to the polynomial equivalence problem modulo an ideal over \( Z[X_1,\ldots,X_n] \),

2. the unification problem over a finitely presented commutative ring with unity is the same as finding whether a polynomial has a solution modulo an ideal over \( Z[X_1,\ldots,X_n] \). The unification problem is undecidable as Hilbert's 10th problem is a special case of the unification problem over a free commutative ring with unity,

3. the unification problem over a finitely presented commutative ring with unity is decidable if we restrict ourselves to linear forms,

4. the word problem over a finitely presented boolean (polynomial) ring is co-NP-complete,

5. the unification problem over the boolean ring is NP-complete whereas the unification problem over a finitely presented boolean (polynomial) ring is co-NP-hard,

6. computing a reduced Gröbner basis over linear polynomials is essentially the same as computing the Hermite normal form of an integral matrix, which implies that the uniform word problem for finitely presented abelian groups can be solved in polynomial time, and

7. the set of all unifiers of two forms of a finitely presented abelian group can be computed in polynomial time.

The Gröbner basis approach has been implemented to solve uniform word problems over finitely presented commutative semi-groups, abelian groups, commutative rings with unity, boolean rings etc.. In fact, the same algorithm solves the uniform word problem for finitely presented abelian semi-groups and commutative rings with unity; for solving word problems over finitely presented boolean rings, this algorithm is modified to include, in the presentations, the relation \( a \cdot a = a \) for each generator \( a \), as well as \( 1 + 1 = 0 \). For finitely presented abelian groups, the algorithm for commutative ring is slightly modified so that it does not as-
sume the existence of the multiplication operation of a commutative ring. We also discuss the relation between the Gröbner basis computation and unification (of elementary terms) over finitely presented abelian groups.

For approaches to solve word problems and unification problems based on extensions of the Knuth-Bendix completion procedure for handling AC-operators, see [2,17,18,19,21].

In the next section, we define the word problem and unification problem over finitely presented algebras to avoid any possible confusion due to the terminology used in the paper. Section 3 is a background material on rewriting systems, polynomial ideals and Gröbner basis. Section 4 is a discussion of word problems and unification problems over finitely presented commutative rings with unity; we also establish a relationship between polynomial rings over integers and commutative rings freely generated by a finite set of generators, by showing how each generator serves the role of an indeterminate. Section 5 discusses these problems over finitely presented boolean rings. Section 6 considers these problems over finitely presented abelian groups. In Section 7, we discuss word problems over finitely presented commutative semi-groups.

2. FINITELY PRESENTED ALGEBRAS, WORD PROBLEM, UNIFICATION PROBLEM

Consider a variety (or family) of algebraic structures defined by a collection of axioms, in particular equations (or identities). For example,

\[ x + (-x) = 0 \]
\[ x + y = y + x \]
\[ x + (y + z) = (x + y) + z \]
\[ x + 0 = x \]

defines a variety of abelian groups.

A word problem on a variety \( V \) is to decide, given two words \( w_1 \) and \( w_2 \) constructed from (first-order) variables and operators of the variety, whether \( w_1 \) and \( w_2 \) are equivalent in the variety. This problem is commonly known as the identity problem; however, in this paper we have chosen to follow the terminology of [15].

The unification problem (on elementary terms) on a variety \( V \) is to determine, given two words \( w_1 \) and \( w_2 \) constructed from variables and operators of the variety, whether there exists a substitution \( \sigma \) for variables such that \( \sigma(w_1) \) and \( \sigma(w_2) \) are equivalent in the variety.

If we allow other uninterpreted function symbols (different from the operators of the variety) also for building words, then we refer to those word (unification) problems as general word (unification) problems.

An algebra \( A \) in a variety \( V \) is finitely presented if and only if there exists a finite set of generators \( \{ a_1, \ldots, a_n \} \) and a finite set of equations \( \{ e_{11} = e_{21}, \ldots, e_{1k} = e_{2k} \} \), relating
words constructed using these generators and operators of the variety, which define \( A \). Generators and defining equations relating these generators constitute a finite presentation \( P \) of \( A \).

The word problem over an algebra \( A \) of variety \( V \) with a finite presentation \( P \) is to determine, given two words \( w_1 \) and \( w_2 \) constructed using the generators in \( P \) and the operators of \( V \), whether \( w_1 \) and \( w_2 \) are equivalent in \( A \).

The uniform word problem over a variety \( V \) is to determine, given a finite presentation \( P \) of an algebra \( A \) of variety \( V \) and two words \( w_1 \) and \( w_2 \) of the finitely presented algebra specified by \( P \), whether \( w_1 \) and \( w_2 \) are equivalent in \( A \).

The unification problem (on elementary terms) on an algebra \( A \) of variety \( V \) with a finite presentation \( P \) is to determine, given two words \( w_1 \) and \( w_2 \) constructed from variables, generators of \( A \) and operators of variety \( V \), whether there exists a substitution \( \sigma \) for variables such that \( \sigma(w_1) \) and \( \sigma(w_2) \) are equivalent in \( A \). The unification problem is also often called the word equation problem.

3. BACKGROUND

3.1 Rewrite Relations

Most of this will be familiar to the reader who has some familiarity with the literature on term rewriting systems [9].

Let \( \rightarrow \) be a binary relation on a set \( S \), called a rewriting relation. The reflexive, transitive closure of a rewrite relation \( \rightarrow \) is denoted by \( \rightarrow^* \), is referred to as reduction. An element \( p \) in \( S \) is said to be in normal form if and only if there is no \( q \) such that \( p \rightarrow q \). If \( p \rightarrow^* q \) and \( q \) is in normal form, then \( q \) is said to be a normal form of \( p \).

A rewrite relation \( \rightarrow \) is said to be finitely terminating or Noetherian if and only if there cannot be any infinite sequence of the form \( a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \cdots \). The relation \( \rightarrow \) is

- confluent if and only if for all \( p, q, r \) such that \( p \rightarrow^* q \) and \( p \rightarrow^* r \) there exists \( s \) such that \( q \rightarrow^* s \) and \( r \rightarrow^* s \).

- locally confluent if and only if for all \( p, q, r \) such that \( p \rightarrow q \) and \( p \rightarrow r \) there exists \( s \) such that \( q \rightarrow^* s \) and \( r \rightarrow^* s \).

It can be shown, fairly easily, that if \( \rightarrow \) is both Noetherian and locally confluent then it is confluent. A rewrite relation \( \rightarrow \) that is both Noetherian and confluent is said to be canonical.

3.2 POLYNOMIAL IDEALS

Let \( R [X_1, \ldots, X_n] \) be the ring of polynomials with indeterminates \( X_1, \ldots, X_n \) over \( R \), where \( R \) is a commutative ring with unity. Let us assume a total ordering on indeterminates, in particular, without any loss of generality, \( X_1 < X_2 < \cdots < X_n \). A term is any power 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 (or power product) multiplied by a nonzero coefficient from \( R \). A polynomial is a sum of monomials.
We can define a well-founded total ordering on terms in many ways. In this paper, we use the degree and lexicographic ordering. Terms \( t_1 = \prod_{i=1}^{a} x_i^{k_i} < t_2 = \prod_{i=1}^{a} x_i^{j_i} \) if and only if (1) the degree of \( t_1 \) is less than the degree of \( t_2 \), or (2) the degree of \( t_1 \) is degree of \( t_2 \) and there exists an \( i \geq 1 \), such that \( k_i = j_i \), and for each \( 1 \leq i' < i \), \( k_i' = j_i' \).

When \( R \) is \( Z \), then monomials are ordered using their terms and coefficients. We say that an integer \( c \) is less than another integer \( c' \), written as \( c \ll c' \), if and only if \( |c| < |c'| \) or \( (|c| = |c'|, c \) is positive and \( c' \) is negative); \( |c| \) stands for the absolute value of \( c \). Thus, \( 0 \ll 1 \ll -1 \ll 2 \ll -2 \ll \ldots \) The ordering \( \ll \) on \( Z \) is total and well-founded. Given two monomials \( m_1 = c_1 t_1 \) and \( m_2 = c_2 t_2 \), \( m_1 \ll m_2 \) if and only if \( t_1 < t_2 \), or \( (t_1 = t_2 \) and \( c_1 \ll c_2 \)). It is easy to see that the ordering \( \ll \) on monomials is total and well-founded.

Consider a polynomial \( p = m + r \) 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 \( p \), the coefficient of \( m \) is called the head-coefficient of \( p \), and \( r \) is called the reductum of \( p \). The ordering \( \ll \) on monomials can be used to define a ordering \( \ll \) on polynomials as: 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 the head-monomial and reductum of \( p_i \), \( i = 1, 2 \). It is easy to see that the ordering \( \ll \) on polynomials in \( Z [X_1, \ldots, X_a] \) is total and well-founded.

Given a set \( B \) of polynomials, the ideal \( I \) generated by \( B \) is the set of all polynomials which can be expressed as a linear combination of the elements in the basis. That is,
\[
I = \{ p \mid p = \sum a_i b_i \}
\]
where \( a_i \) is any polynomial and \( b_i \) is an element of \( B \). This is often expressed in this paper as \( I = (b_1, \ldots, b_b) \). (Note the distinction between the use of braces and that of parentheses; \( \{b_1, \ldots, b_b\} \) stands for a set of polynomials whereas \( (b_1, \ldots, b_b) \) denotes the ideal generated by them.) An ideal is said to be trivial if and only if it is the entire ring, and non-trivial otherwise. If \( R \) is a Noetherian ring, then by Hilbert's theorem [27], every ideal of \( R [X_1, \ldots, X_a] \) is finitely generated. All of the rings that are considered in this paper are Noetherian.

Let \( I \) be an ideal over \( R [X_1, \ldots, X_a] \) specified by a finite basis \( B = \{b_1, \ldots, b_b\} \). The ideal membership problem is to determine, given a polynomial \( p \) and a basis \( B \), whether \( p \) is in the ideal \( I \) generated by \( B \). The polynomial equivalence problem modulo an ideal is to determine, given two polynomials \( p \) and \( q \) and a basis \( B = \{b_1, \ldots, b_b\} \), whether there exist polynomials \( q_i \) such that
\[
p = q + \sum q_i b_i
\]
The polynomial equivalence problem can be reduced to the ideal membership problem by asking whether \( p - q \) is in the ideal \( I = (b_1, \ldots, b_b) \).

The triviality problem is to determine, given a set \( B \) of polynomials, whether the ideal generated by \( B \) is trivial.
A polynomial $p$ has a solution in $R$ if and only if there exist elements of $R$ such that when these are substituted for indeterminates in $p$, $p$ evaluates to 0.

Let a form be defined as a polynomial which besides using indeterminates, also involves (first-order) variables. An equation $t_1 = t_2$, where $t_1$ and $t_2$ are forms, has a solution modulo an ideal $I$ if and only if there exist polynomials which can be substituted for variables in $t_1$ and $t_2$ such that the polynomials $q_1$ and $q_2$ obtained after this substitution are equivalent modulo $I$.

### 3.3 Grobner Bases

A basis $B$ is called a Gröbner basis for an ideal $I$ if for any polynomial $q$, no matter how $q$ is reduced using polynomials in $B$, the result is always the same, i.e., it is unique [3,5]. An equivalent definition is that for any polynomial $p$ in $I$, $p$ reduces to 0 using the polynomials in $B$. To precisely define a Gröbner basis of an ideal over $\mathbb{Z}[x_1,\ldots,x_n]$, it is necessary to define how polynomials are used as rewrite rules, or, in other words, how a polynomial reduces another polynomial. We give below some definitions; an interested reader may wish to consult [10,11,12] for more details.

Consider a polynomial $P = m_1 + r_1$ where $m_1$ and $r_1$ are, respectively, the head-monomial and reductum of $P$. Let $m_1 = c_1 t_1$, where $c_1$ and $t_1$ are respectively the head-coefficient and head-term of $m_1$. Then the rewrite rule corresponding to $P$ is: $c_1 t_1 \rightarrow -r_1$. In case the head-coefficient $c_1$ of $P$ is negative, $P$ is multiplied by -1 and the result is used as a rewrite rule. For example, the rewrite rule corresponding to $2x_1^2 x_2 - x_2$ is $2x_1^2 x_2 \rightarrow x_2$. 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 $t = \sigma t_1$ and (2) either $c > (c_1 / 2)$ or $c < - (c_1 / 2)$. If $-(c_1 / 2) \leq c \leq (c_1 / 2)$ or there does not exist any $\sigma$ such that $t = \sigma t_1$, 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 $Q$ that can be rewritten using the rule, and (2) $Q' = Q_1 + (c - \epsilon c_1) t + \epsilon \sigma R$, where $\epsilon = 1$ if $c > 0$ and $\epsilon = -1$ otherwise. If there is no monomial in $Q$ which can be rewritten using the rule, then $Q$ is in normal form with respect to the rule. For example, using the rule $2x_1^2 x_2 \rightarrow x_2$, the polynomial

$$4x_1^3 x_2 + 5x_1 x_2^2 - 3x_1^2 x_2 \rightarrow 2x_1^3 x_2 + x_1 x_2 + 5x_1 x_2^2 - 3x_1^2 x_2$$

$$\rightarrow 2x_1 x_2 + 5x_1 x_2^2 - 3x_1^2 x_2.$$

The result can be further reduced as the monomial $-3x_1^2 x_2$ is reducible:

$$2x_1 x_2 + 5x_1 x_2^2 - 3x_1^2 x_2 \rightarrow 2x_1 x_2 + 5x_1 x_2^2 - x_1^2 x_2 - x_2$$

$$\rightarrow 2x_1 x_2 + 5x_1 x_2^2 + x_1^2 x_2 - 2x_2.$$

We assume that after rewriting by a polynomial, indeterminates in terms are ordered using the prespecified ordering on indeterminates, monomials whose terms (power products) are equal are
combined, and terms with zero coefficients are omitted.\footnote{We could as well have defined the rewriting relation induced by a polynomial using a division algorithm on integer coefficients that produces the least remainder; an interested reader may wish to refer to \cite{12} for such a definition of the rewriting relation induced by a polynomial. We have used the definition given in \cite{10} which uses repeated subtraction on integer coefficients as this definition is simpler to understand.}

Let \( T = \{ L_1 \rightarrow R_1, \ldots, L_k \rightarrow R_k \} \) be the set of rules corresponding to a basis \( B = \{ b_1, \ldots, b_k \} \) of an ideal \( I \) such that \( L_i \rightarrow R_i \) is the rule corresponding to \( b_i \). Let \( \rightarrow \) denote the rewriting relation defined by \( T \), i.e., a polynomial \( Q \rightarrow Q' \) if and only if \( Q \) rewrites to \( Q' \) using some rule \( L_i \rightarrow R_i \) in \( T \). It is easy to see (using the ordering defined on polynomials earlier) that \( \rightarrow \) is Noetherian.

A basis \( B \) is a Gröbner basis if and only if the rewriting relation \( \rightarrow \) defined by \( B \) is canonical.

In \cite{10}, we discuss an algorithm for generating the Gröbner basis of a polynomial ideal over \( Z[X_1, \ldots, X_n] \). (See \cite{4} for a similar algorithm independently developed by Buchberger.) The algorithm is similar to the Knuth-Bendix completion procedure. It accepts a finite basis of an ideal and an ordering on indeterminates and generates a Gröbner basis for the ideal generated by the input basis which is unique up to the ordering on the indeterminates. In \cite{12}, we have generalized this algorithm so that it works on polynomial rings over an arbitrary Euclidean ring.

The ideal membership problem (and hence the polynomial equivalence problem modulo an ideal) can be easily solved using the Gröbner basis of an ideal. To check whether a polynomial \( p \) is in an ideal \( I \) generated by a basis \( B \) or not, generate the Gröbner basis \( GB \) of \( I \) from \( B \) using some ordering on indeterminates; then reduce \( p \) using \( GB \); if the result is 0, then \( p \) is in \( I \) and otherwise it is not in \( I \). Thus to test for equivalence of \( p \) and \( q \), it is enough to reduce \( p \) and \( q \) using \( GB \) and check whether their normal forms are the same or not. Note that this is similar to proving that an equation is in an equational theory by generating a canonical system for the equational theory.

Our approach for solving word problems and unification problems over commutative algebras uses the above results about polynomial ideals and their Gröbner bases. In the next section, we establish a relationship between polynomial rings over integers and commutative rings freely generated by a finite set of generators, by showing how each generator serves the role of an indeterminate.

4. COMMUTATIVE RINGS WITH UNITY

The word problem or the identity problem over a free commutative ring with unity is known to be decidable; see \cite{16,23} for a canonical term rewriting system which can be used to
generate canonical forms of words, thus giving us a decision procedure for the word problem. The unification problem over a free commutative ring is discussed later after we establish the relationship between a free commutative ring generated by a finite set of generators and the polynomial ring over the integers.

4.1 Word Problem over Finitely Presented Commutative Rings with Unity

Let \( A \) be a finitely presented ring with generators \( a_1, \ldots, a_n \) and the relators (or relations) \( e_{11} = e_{21}, \ldots, e_{1k} = e_{2k} \). As said above, each of \( e_{ij} \) is a word constructed from \( a_1, \ldots, a_n \) and the ring operations. Assuming some ordering on the \( a_i \)'s, say \( a_1 < \cdots < a_n \), we can transform each \( e_{ij} - e_{2j} \) into its canonical sum-of-products form, say \( p_j \), which is a polynomial in \( Z[a_1, \ldots, a_n] \).

**Theorem 1:** The word problem over a finitely presented ring with generators \( a_1, \ldots, a_n \) and relators \( e_{1i} = e_{2i} \), for \( 1 \leq i \leq k \), is the same as the polynomial equivalence problem modulo the ideal \( I \) specified by the basis \( \{p_1, \ldots, p_k\} \) in \( Z[a_1, \ldots, a_n] \), where \( p_i \) is the canonical sum of products form of \( e_{1i} - e_{2i} \).

**Proof:** The polynomial equivalence problem modulo an ideal \( I \) is to check, given two polynomial \( r \) and \( s \), whether there exist some polynomials \( q_i \) such that \( r = s + \sum q_i p_i \). This reduces to asking whether the words \( r \) and \( s \) are equivalent in the equational theory of \( p_i = 0 \), which is also the equational theory of \( e_{1i} = e_{2i} \).

If two words \( w_1 \) and \( w_2 \) are equivalent with respect to relators \( e_{1i} = e_{2i} \), then there exists a sequence of steps involving replacement of \( e_{1i} \) by \( e_{2i} \) or vice versa, using which \( w_1 \) can be transformed to \( w_2 \). Using induction on the number of such steps, it can be shown that \( w_1 = w_2 + \sum q_i (e_{1i} - e_{2i}) \). Hence the result. \( Q.E.D. \)

So, the algorithm for computing the Gröbner basis of a ideal over a polynomial ring of integers discussed in [10] can be used to solve the uniform word problem over a finitely presented commutative ring with unity. (Because of the Hilbert basis theorem [27], the algorithm in [10] is guaranteed to terminate with the Gröbner basis of the ideal specified by the input.) From the presentation of the ring, we can generate its Gröbner basis assuming some total ordering on indeterminates, then compute the normal forms of the words under consideration with respect to this basis and check whether the two normal forms are the same. The Gröbner basis is the canonical basis of the finitely presented commutative ring which is isomorphic to \( Z[a_1, \ldots, a_n]/I \). The Gröbner basis algorithm can also be used for solving the uniform word problem over finitely presented commutative rings with unity of any characteristic; to a presentation of such a ring, we add the relation \( m = 0 \), where \( m \) is the characteristic of the ring, and then apply the Gröbner basis algorithm. Later, we discuss finitely presented boolean rings which are of characteristic 2.

As noted in [10], the ordering on indeterminates considerably affects the performance of the algorithm. We give below some examples run using this algorithm which has been implemented on a VAX/780 in ALDES and Franz Lisp and on the Symbolics 3600 in Zetalisp.

---

2. Hecaseforth, by a commutative ring, we shall mean a commutative ring with unity.
Example 1: Consider the commutative ring generated by generators $X$, $Y$, $W$ with the following presentation:

(1) $-W + X Y^2 + 4 X^2 + 1 = 0$
(2) $Y^2 W + 2X + 1 = 0$
(3) $-X^2 W + Y^2 + X = 0$.

The canonical basis for the commutative ring using the ordering $X < Y < W$ is

(1) $W^2 - W - 4 Y^2 + 2 X^2 - 3 X = 0$
(2) $-W + X Y^2 + 4 X^2 + 1 = 0$
(3) $X^2 W - Y^2 - X = 0$
(4) $Y^2 W + 2X + 1 = 0$
(5) $-3 X W - Y^2 + 2 X^4 + 13 X^3 + X - 1 = 0$
(6) $W + Y^4 + 2 X^3 - 3 X^2 - 1 = 0$

Example 2: The presentation is

(1) $2 X^2 Y^4 W^5 + 5 X Y^2 + X W - 6 Y = 0$
(2) $X^2 + 2 X + 1 = 0$
(3) $X^2 Y^2 - 1 = 0$
(4) $8 X Y W - 8 = 0$
(5) $6 X + 3 Y + 2 W = 0$

The canonical basis of the above presentation generated using the ordering $X < Y < W$ turns out to be $1 = 0$. Thus the ideal is trivial as all words in the ring are equivalent to each other.

Example 3: Consider the presentation [21]

(1) $Y^6 + X^4 Y^4 - X^2 Y^4 - Y^4 - X^4 Y^2 + 2 X^2 Y^2 + X^6 - X^4 = 0$
(2) $2 X^3 Y^4 - X Y^4 - 2 X^3 Y^2 + 2X Y^2 + 3 X^5 - 2 X^3 = 0$
(3) $3 Y^5 + 2 X^4 Y^3 - 2 X^2 Y^3 - 2 Y^3 - X^4 Y + 2 X^2 Y = 0$

The canonical basis obtained using the ordering $X < Y$ is:

(1) $4 Y^4 + 4 X^4 Y^2 - 8 X^2 Y^2 - 4 X^8 + 4 X^4 = 0$
(2) $X^2 Y^4 + 2 Y^4 + 2 X^4 Y^2 - 6 X^2 Y^2 - 3 X^8 + 4 X^4 = 0$
(3) $4 X Y^5 - 8 X Y^3 - 4 X^5 Y + 8 X^3 Y = 0$
(4) \[ Y^6 + X^4 Y^2 - 2 X^2 Y^2 - 2 X^6 + 2 X^4 = 0 \]
(5) \[ -X Y^4 + 2 X^3 Y^2 + 2 X^2 Y^2 + 2 X^7 - X^5 - 2 X^3 = 0 \]
(6) \[ 2 Y^5 + 4 X^2 Y^3 - 4 Y^3 + 4 X^6 Y - 6 X^4 Y + 4 X^2 Y = 0 \]
(7) \[ 3 Y^5 + 2 X^4 Y^3 - 2 X^2 Y^3 - 2 Y^3 - X^4 Y + 2 X^2 Y = 0 \]
(8) \[ 3 Y^4 + 2 X^6 Y^2 + 2 X^4 Y^2 - 2 X^2 Y^2 + X^8 - 2 X^6 - X^4 = 0 \]
(9) \[ 2 X^5 Y^2 + 2 X Y^2 + X^8 - 2 X^2 = 0 \]
(10) \[ 4 X^2 Y^3 - 2 Y^3 + X^8 Y + 2 X^8 Y - 4 X^4 Y + 2 X^2 Y = 0 \]

4.2 The Unification Problem

**Theorem 2:** The unification problem for terms \( t_1 \) and \( t_2 \) involving variables over a finitely presented commutative ring \( A \) generated by \( a_1, \ldots, a_n \), and relations \( e_{1i} = e_{2i}, 1 \leq i \leq k \), is the same as finding whether \( t_1 = t_2 \) have a solution modulo \( I = (p_1, \ldots, p_k) \) in \( Z[a_1, \ldots, a_n] \), where \( p_i \) is the canonical sum of products form of \( e_{1i} - e_{2i} \).

**Proof:** Follows from Theorem 1 in the previous section. Q.E.D.

**Theorem 3:** Hilbert's 10th problem is a special case of the unification problem over free commutative rings with unity.

**Proof:** Integers can be simulated within a free commutative ring with unity with no generators at all. For example, we can simulate any positive integer \( k \) as the summation of \( 1 \) repeated \( k \) times, and any negative integer \(-k\), where \( k \) is positive, as the summation of \(-1\) \( k \) times. If the indeterminates in an instance of Hilbert's 10th problem are replaced by variables, then the problem of unifying the resulting term with zero in the free commutative ring is the same as finding an integer solution of the original polynomial. The term can be unified with 0 if and only if its polynomial has an integer solution. Q.E.D.

The above theorem shows that the unification problem over a free commutative ring is undecidable since Hilbert's 10th problem is undecidable. In the next section we show that a restricted case of this problem - where the polynomials under consideration are linear over the variables - is decidable.

4.2.1 Linear Forms

By a **linear form** we mean an expression of the form \( p_1 y_1 + p_2 y_2 + \cdots + p_m y_m + q \) where \( p_1, \ldots, p_m, q \) are polynomials belonging to \( R[X_1, \ldots, X_n] \) and \( y_1, \ldots, y_m \) are variables. (Non-linear forms can be similarly defined.) A linear form \( p_1 y_1 + p_2 y_2 + \cdots + p_m y_m + q \) has a solution modulo an ideal \( I \) (over \( R[X_1, \ldots, X_n] \)) if and only if there exist polynomials \( r_1, \ldots, r_m \) such that \( p_1 r_1 + p_2 r_2 + \cdots + p_m r_m + q \) belongs to \( I \). The unification problem of linear forms is equivalent to a linear form having a solution.
Lemma 1: Let \( L = p_1 y_1 + p_2 y_2 + \cdots + p_m y_m + q \) be a linear form and \( I = (f_1, \ldots, f_r) \) be an ideal over \( R[X_1, \ldots, X_a] \). Then \( L \) has a solution modulo \( I \) if and only if \( q \) belongs to the ideal \( J = (f_1, \ldots, f_r, p_1, \ldots, p_m) \).

Proof: "If part": Since \( q \) belongs to \( J \), \( q = \sum d_i f_i + \sum b_j p_j \) which implies that \( L \) has a solution modulo \( J \). In particular, the \(-b_j\)'s are the solutions.

"Only if part": If \( L \) has a solution modulo \( I \), say \( y_j = b_j \) for all \( j \), then \( \sum b_j p_j + q = 0 \) which means that \( q \) belongs to the ideal \( J \).

Corollary 1: The following problem is decidable:

**Instance:** A linear form \( L \), a set \( \{X_1, \ldots, X_a\} \) of indeterminates and a polynomial ideal \( I \) over \( Z[X_1, \ldots, X_a] \).

**Question:** Does \( L \) have a solution modulo \( I \)?

However the general problem (of solving non-linear forms) can be shown to be undecidable, again by reducing Hilbert's 10th problem to it.

4.3 Boolean Rings

A boolean ring \( B = \{0, 1\}, +, \cdot \) is a commutative ring where the multiplicative identity 1 has the property \( 1 + 1 = 0 \). In other words, 1 is its own inverse. An alternate way of viewing the boolean ring is in terms of propositional calculus, whereby + stands for 'exclusive-or' and \( \cdot \) for '\( \land \)'. A boolean ring of polynomials is any ring of polynomials with coefficients from \( B \) with the additional property that \( X \cdot X = X \) for every indeterminate \( X \) ("the idempotence law"). The reader can now easily see that this implies \( p \cdot p = p \) for every polynomial \( p \) in the ring. Thus only flat polynomials, i.e. those in which the degree of an indeterminate in a term is always either 0 or 1, need be considered; for instance, \( X^3 + Y \) is equivalent to \( X + Y \) which is flat. Throughout the rest of this section we denote a boolean ring of polynomials with indeterminates \( X_1, \ldots, X_a \) by \( B[X_1, \ldots, X_a] \) (even though this abuses the notation).

The above notion of "boolean ring of polynomials" enables us to express the entire propositional calculus in terms of polynomials, since the operators 'exclusive-or' and \( \land \) are enough to express any propositional formula. (See [8] for methods for converting formulae in terms of \( \land, \lor \) and \( \neg \) into the above-mentioned polynomial form.) This enables us to show [1,10,14] that theorem-proving in propositional calculus can be reduced to testing whether a polynomial ideal over \( B[X_1, \ldots, X_a] \) is trivial. This "ideal-theoretic" approach to theorem-proving has been extended to first-order logic with a few modifications [14].

**Theorem 4:** Given a set of polynomials \( S \) over a boolean polynomial ring, the problem of determining, whether \( I \in (S) \) is co-NP-complete.

Consider a set of boolean polynomials \( S \) and polynomials \( p \) and \( q \). Let \( I \) be the ideal generated by \( S \). Clearly, \( p = q \) if and only if \( p - q \in I \) if and only if \( (p - q)^n \in I \) for some \( n \).

Now it is not hard to show by an argument similar to that used in the proof of Hilbert's Nullstellensatz in [27] that \( (p - q)^n \in I \) for some \( n \) if and only if \( (S, (p - q) \cdot Y + 1) \),
where \( Y \) is a new indeterminate, contains \( 1 \); if \( p - q \) is not in \( I \), then there exists an assignment of \( Y \) such that the polynomial \((p - q) \ast Y + 1\) has a zero common with \( I \). All this leads us to

**Theorem 5:** The word problem for finitely presented boolean polynomial rings is co-NP-complete.

On the other hand,

**Theorem 6:** The unification problem over the boolean ring \( B \) is NP-complete.

The unification problem over the boolean ring \( B \) turns out to be the same as the satisfiability problem. Since the word problem for finitely presented boolean (polynomial) rings is a special case of the unification problem over finitely presented boolean (polynomial) rings, we also have

**Theorem 7:** The unification problem over finitely presented boolean (polynomial) rings is co-NP-hard.

Note that the unification problem is clearly decidable, since the number of flat boolean polynomials over a finite set of indeterminates is finite. It can also be viewed as a special case of the validity problem for quantified boolean formulae; let \( A = \{ a_1, \ldots, a_n \} \) be a set of indeterminates, \( P = \{ p_1 = 0, \ldots, p_k = 0 \} \) be a presentation, \( V = \{ y_1, \ldots, y_m \} \) be a set of variables and \( e \) and \( f \) be two forms built from \( A \) and \( V \) that have to be unified. We can assume without loss of generality that \( f = 0 \). Now it can be shown that \( e \) and \( 0 \) are unifiable if and only if the formula \( \forall a_1 \cdots \forall a_n \exists y_1 \cdots \exists y_m : P \Rightarrow (e = 0) \) is valid, where \( a_i \) and \( y_j \) range over boolean values; thus the problem is complete for the class \( \Pi^P_2 \) in the polynomial hierarchy. (See [7], Section 7.2, for the definitions and further details on the polynomial hierarchy.)

## 5. Finitely Presented Abelian Groups
### 5.1 Word Problem

Let \( G \) be an abelian group with the set of generators \( A = \{ a_1, \ldots, a_n \} \), operator + and a finite set of relations \( F \). Each relation in \( F \) can be viewed as an equation of the form \( c_1 \ast a_1 + \cdots + c_n \ast a_n = 0 \) where the \( c_i \)'s are integers. (The notation \( c \ast a_i \), where \( c \) is an integer, denotes \( a_i + \cdots + a_i \) (\( |c| \) times) if \( c \) is positive and \( -a_i + \cdots + -a_i \) (\( |c| \) times) if \( c \) is negative.) In other words, each relation in \( F \) is a linear polynomial from \( \mathbb{Z}[a_1, \ldots, a_n] \) with a constant term of 0.

Treating every presentation \( F \) as a set of integral polynomials clearly enables us to solve the uniform word problem in the obvious fashion; all that we have to do is to compute the corresponding Gröbner basis. But since every term in a finitely generated abelian group can be represented by a linear integral polynomial, we need to make use of only the linear polynomials in these Gröbner bases. Thus what we have to compute is not the entire Gröbner basis but a modified Gröbner basis, called the Gröbner basis for Abelian Groups (referred to as "AG-Gröbner basis" hereafter), that can be obtained by deleting all the non-linear polynomials from the actual one.
The above-mentioned approach for computing AG-Gröbner bases is clearly inefficient. A better way would be to avoid the generation of non-linear polynomials altogether during the computation. Such an algorithm can be obtained by a slight modification of the algorithm in [10]. A brief description of the algorithm is given below.

Let \( \{a_1, \ldots, a_n\} \) be the set of generators and \( F = \{e_1 = 0, \ldots, e_k = 0\} \) be the set of equations under consideration. The algorithm assumes a total ordering \( > \) on generators. Consider the indeterminate highest in the ordering and not considered so far, say \( a_i \). Take the extended gcd of its non-zero coefficients, say \( c(1,i), \ldots, c(k,i) \), in all equations in the set \( F \) in which \( a_i \) appears. Let the extended gcd give the result \( (d, m_1, \ldots, m_k) \), i.e., \( d = m_1 c(1,i) + \cdots + m_k c(k,i) \). Then \( m_1 e_1 + \cdots + m_k e_k = 0 \) is the equation for \( a_i \) which is included in the canonical basis. Substitute for \( d a_i \) in all equations in \( F \); this reduction would get rid of \( a_i \) in the new equations that we get. Obviously, if the coefficient of \( a_i \) is 1 (or -1) in some equation \( e_j \), then \( e_j \) can be included in the basis straightaway. (We do not have to compute the extended gcd.)

Repeat the above process until all equations are taken care of or all generators are taken care of.

**Definition:** Let \( M \) be an integer matrix. \( M \) is said to be upper triangular if and only if the following conditions hold: (a) \( M_{ij} = 0 \) for all \( 0 < j < i \); (b) \( M_{ii} \neq 0 \) for all \( i \).

Let \( G = \{p_1, \ldots, p_k\} \) be a set of linear polynomials over \( Z[a_1, \ldots, a_n] \) such that

\[
G = C \cdot [a_1, \ldots, a_n]^T
\]

where \( C \) is an \( k \times n \) matrix. (Thus the \( p_i \)'s have no constant terms.)

A rule in a Gröbner basis is redundant if and only if its left-hand side can be reduced using other rules.

**Lemma 2:** \( G \) is an AG-Gröbner basis with respect to the total ordering \( > \) with no redundant rules if and only if \( C \) is in upper triangular form.

**Proof:** "If part": Consider the linear polynomials generated from \( C \cdot [a_1, \ldots, a_n]^T \). Since the left-hand side of the rule corresponding to every polynomial thus obtained is a linear term, i.e., term of degree 1, and each left-hand side involves a distinct indeterminate, all critical pairs are trivial, or, in other words, they do not generate a linear polynomial as a new rule. So, the basis is an AG-Gröbner basis and no rule is redundant because none of the left-hand sides can be simplified using other rules; however the right-hand side of a rule could be reduced.

"Only if part": If \( G \) is an AG-Gröbner basis with no redundant rules, then every left-hand side has a distinct indeterminate and every right-hand side involves indeterminates lower than the indeterminate on the left-hand side. Thus its polynomials can be put into a upper triangular form using the ordering on indeterminates. \( \text{Q.E.D.} \)
Let $L$ be a set of linear polynomials over $\mathbb{Z}[a_1, \ldots, a_n]$ with no constant terms and let $D$ be an integral matrix such that $L = D \ast [a_1, \ldots, a_n]^T$. By the above lemma, computing the AG-Gröbner basis of $L$ is nothing but converting $D$ into upper triangular form. The algorithms presented in [13] (see also [6]) for constructing Hermite Normal Forms of integral matrices enable us to accomplish this in polynomial time. Thus, we have:

**Theorem 8**: The uniform word problem for finitely presented abelian groups can be solved in polynomial time.

The following examples are taken from [21]; the results were obtained by running the AG-Gröbner basis algorithm discussed above.

**Example 4**: The presentation is

\[
\begin{align*}
B - 2E + 3C + 9A - 3D + 8F + 5G &= 0 \\
- B + 6H + 2E + 7A + 8D + 5F + 2G &= 0 \\
- 2B + 4H + 2E + 4C + 5A - D + 6F + 6G &= 0 \\
7B + H - 3E + 6C + 4A + 9D + 7F &= 0 \\
2B - 2H + E - C + 9A + 3D + 4F - 3G &= 0 \\
- 3B + 7H + 8E + 5C + 9A + 8F + G &= 0 \\
3B + 5H + 5E - C - 2A + 3D + F + 9G &= 0 \\
- H + 2E - 2C - 2A + 8D + 3F + 7G &= 0
\end{align*}
\]

Using the total ordering $B > H > E > C > A > D > F > G$ on indeterminates, we obtain the following canonical basis is:

\[
\begin{align*}
B + 5770416G &= 0 \\
H + 4512026G &= 0 \\
E + 5472958G &= 0 \\
C + 652996G &= 0 \\
A + 5287750G &= 0 \\
D + 6588077G &= 0 \\
F + 4856406G &= 0 \\
6634025G &= 0
\end{align*}
\]

**Example 5**: The presentation is:

\[
\begin{align*}
3F + 6E + 8C - 2B - 3A &= 0 \\
- F + 7E + D + 9C - 3B - 3A &= 0 \\
8F + 5E + 6D - 2C - B + 7A &= 0 \\
- 2F + E + 4C + 2B + 6A &= 0 \\
6F + 7E + 2D + 5C - B + 3A &= 0 \\
2F + 7E + 3D + 8C + 4B + 9A &= 0
\end{align*}
\]
If we use the total ordering $F > E > D > C > B > A$ on generators, the canonical basis is:

\[
\begin{align*}
F + B + 728A &= 0 \\
E + 2B + 1090A &= 0 \\
D + 4B + 1435A &= 0 \\
C + 4B + 548A &= 0 \\
7B + 161A &= 0 \\
1498A &= 0
\end{align*}
\]

5.2 Unification Problem over Finitely Presented Abelian Groups

**Lemma 3:** The unification problem is decidable for finitely presented abelian groups.

**Proof:** Let $G$ be an abelian group with the set of generators $A = \{a_1, \ldots, a_n\}$, operator $+$ and a presentation $F$, where each relation in $F$ is represented as a linear polynomial from $Z[a_1, \ldots, a_n]$ with a constant term of 0.

Let $V = \{y_1, \ldots, y_m\}$ be a set of variables and $e_1$ and $e_2$ be two forms involving variables from $V$. Forms $e_1$ and $e_2$ can be thought of as linear polynomials over $V \cup A$ with integer coefficients. Let $e = e_1 - e_2$.

**Claim 1:** Let $L = \{p_1, \ldots, p_m\}$ be a set of linear polynomials in $Z[a_1, \ldots, a_n]$ with the following property: every $p_i$ in $L$ is either a constant (i.e., an integer) or has no constant term at all. Let $I$ be the ideal generated by $L$ and let $p$ be a linear polynomial in $Z[a_1, \ldots, a_n]$. Then $p \in I$ if and only if there exist $q_1, \ldots, q_m$ such that

(a) $p = p_1 q_1 + \cdots + p_m q_m$ and
(b) $p_i q_i$ is linear for all $i$, $1 \leq i \leq m$.

**Proof:** ($\Rightarrow$): Trivial.

($\Rightarrow$): We can assume, without loss of generality, that $L = \{p_1, \ldots, p_m, c\}$ where the $p_i$'s are linear polynomials with no constant term and $c$ is an integer. $p \in I$ implies that there exist polynomials $q_1, \ldots, q_m, r$ such that

$$p = p_1 q_1 + \cdots + p_m q_m + rc.$$

Assume $p \neq 0$, since the result trivially holds true for 0. The following possibilities have to be considered now:

(a) At least one of the $q_i$'s has a constant term.

(b) $r$ has linear terms (i.e., monomials of degree 1) or constant terms.

It should be obvious that either (a) or (b) should hold, because $p$ would not be linear otherwise.

Let us first consider the case when (a) holds. Let $q_j = q_j' + d_j$ for some $j$, $1 \leq j \leq m$ such that $q_j'$ has no constant term. Then $p' = p - d_j p_j$ is a linear polynomial and

$$p' = p_1 q_1' + \cdots + p_j q_j' + \cdots + p_m q_m + rc.$$
Consider (b), i.e., let \( r = r' + w \) where \( w \) is a linear polynomial and \( r' \) has no linear terms. Now \( p' = p - cw \) is a linear polynomial and
\[
p' = p_1 q_1 + \cdots + p_m q_m + r'.
\]

Since the above steps can be repeated, the claim is proved. Q.E.D.

Claim 2: \( e_1 \) is unifiable with \( e_2 \) modulo \( G \) if and only if \( c \), considered as a linear form over \( Z[a_1, \ldots, a_n] \), has a solution modulo the ideal generated by \( F \).

Proof: The 'only if' part is trivial. To prove the 'if' part, first observe that \( c = d_1 y_1 + d_2 y_2 + \cdots + d_m y_m + q \) for some \( d_i \) (1 ≤ i ≤ m) and \( q \), where the \( d_i \)'s are integers and \( q \) is a linear polynomial in \( Z[a_1, \ldots, a_n] \). By Lemma 1, \( c \) has a solution if and only if \( q \) belongs to the ideal \( J = (F, d_1, \ldots, d_m) \) and now Claim 1 enables us to complete the proof. Q.E.D.

Lemma 4: Let \( I \) be an ideal over \( Z[a_1, \ldots, a_n] \) and \( GB = \{p_1, \ldots, p_m\} \) be its Gröbner basis with respect to the degree + lexicographic ordering. Then, for all polynomials \( p \) in \( Z[a_1, \ldots, a_n] \), \( p \in I \) if and only if there exist polynomials \( q_1, \ldots, q_m \) such that
(a) \( p = p_1 q_1 + \cdots + p_m q_m \)
(b) degree(\( p_i, q_i \)) ≤ degree(\( p \)) for all \( i, 1 ≤ i ≤ m \).

Proof: Obvious from the way rewriting with respect to a polynomial is defined and the property that \( p \in I \) if and only if \( p \to^* 0 \), where \( \to^* \) is the rewriting relation induced by \( GB \), since \( GB \) is a Gröbner basis of \( I \). Q.E.D.

Corollary 2: Let \( I \) and \( GB \) be as in Lemma 4 and let \( GB \) consist only of non-constant polynomials. Then, for a linear polynomial \( p \) in \( Z[a_1, \ldots, a_n] \), \( p \in I \) if and only if there exist integers \( e_1, \ldots, e_m \) such that \( p = p_1 e_1 + \cdots + p_m e_m \), where \( p_i \) are linear polynomials in \( GB \).

The above corollary enables us to exhibit yet another decision procedure for the unification problem for finitely presented abelian groups. As in the previous section, let \( AG \) be an abelian group with the set of generators \( A = \{a_1, \ldots, a_n\} \), operator \( + \) and a finite set of relations \( F \).
The presentation \( F \) consists of linear polynomials \( c_{i,1} a_1 + \cdots + c_{i,m} a_m = 0 \) for
\[
1 ≤ i ≤ k = |F|, \text{ where the } c_{i,j}'s \text{ are integers. We can also assume, without loss of generality, that } F \text{ is an AG-Gröbner basis. Let } V = \{y_1, \ldots, y_m\} \text{ be a set of variables and } e_1 \text{ and } e_2 \text{ be two expressions involving variables from } V. \text{ Forms } e_1 \text{ and } e_2 \text{ can be thought of as linear polynomials over } V \cup A \text{ with integer coefficients. Let } c = e_1 - e_2 = d_1 y_1 + d_2 y_2 + \cdots + d_m y_m + q \text{ for some } d_i \text{ (1 ≤ i ≤ m)} \text{ and } q, \text{ where the } d_i \text{'s are integers and } q \text{ is a linear polynomial in } Z[a_1, \ldots, a_n]. \text{ Let } G \text{ be the } k \times n \text{ matrix } [c_{i,j}]. \text{ Thus } F = G \ast [a_1, \ldots, a_n]^T.

Our aim is to find solutions to the \( y_i \)'s in terms of linear expressions over \( a_1, \ldots, a_n \).
Let \( |y_i|_{a_j} \) stand for the coefficient of \( a_j \) in the expression for \( y_i \). Thus
\[
y_i = \sum_{j=1}^{n} |y_i|_{a_j} a_j
\]
Let \( q = Q_1 a_1 + \cdots + Q_n a_n \). By Corollary 2, every linear polynomial in the ideal generated by \( F \) is the sum of integral multiples of polynomials in \( F \). This enables us to write equations of the form

\[
d_1 y_1 a_1 + \cdots + d_m y_m a_i + Q_1 c_{i,1} + K_{2i} c_{2i,1} + \cdots + K_i c_{i,1}
\]

where the \( y_i a_i \)'s and the \( K_i \)'s are variables ranging over the integers. We get \( n \) such equations, since we have to account for the sums of coefficients corresponding to every generator \( a_i \). Note that the linear polynomials appearing on the right-hand sides of the equations can also be expressed as \( C^T \ast [K_1, \ldots, K_n]^T \).

A succinct representation of all possible solutions to a set of linear diophantine equations with integer coefficients can be obtained in polynomial time [6,13]. Together with the results in the previous section, this gives us the following theorem:

**Theorem 9**: The following problem can be solved in polynomial time:

**Instance**: An abelian group \( AG \) with a set of generators \( A \) and a presentation \( F \), and two linear expressions \( \varepsilon_1 \) and \( \varepsilon_2 \) involving \( A \) and a set of variables \( V \).

**Problem**: Find the set of all unifiers of \( \varepsilon_1 \) and \( \varepsilon_2 \). (In other words, find the set of all substitutions \( \theta \) to the variables that occur in \( \varepsilon_1 \) and \( \varepsilon_2 \) such that \( \theta(\varepsilon_1) = \theta(\varepsilon_2) \).)

6. Finitely Presented Commutative Semigroups

A finitely presented commutative semigroup can be presented as a set of equations of the form \( t_1 = t_2 \), where \( t_1 \) and \( t_2 \) are terms in \( Z[a_1, \ldots, a_n] \) (we are using \( * \) as the binary operation of a commutative semigroup). Thus it follows that the uniform word problem over a finitely presented commutative semigroup can be solved as a special case of the uniform word problem over commutative rings with unity; we merely restrict our attention to polynomials of the form \( t_1 - t_2 \). The computation steps turn out to be the same as those in [2].

The following examples of finitely presented commutative semigroups are taken from [2] and run using our algorithm for commutative rings with unity.

**Example 6**:

\[
\begin{align*}
B A^2 &= C \\
C B &= C^2 \\
C^2 B A &= C A
\end{align*}
\]

Assuming the ordering \( A > B > C \) on generators, we get the canonical basis

\[
\begin{align*}
C B &= C^2 \\
C A^2 &= C^3 \\
B A^2 &= C \\
C^4 &= C^2 \\
C^2 A &= C A
\end{align*}
\]
Example 7:

\[
\begin{align*}
D^3 C^5 B^4 A^2 &= D^2 C^2 B^3 A \\
D^4 C^3 B A^8 &= D^2 C^4 B^8 A \\
D^2 C^2 B^2 A^2 &= D C^2 \\
C^2 B^8 A &= D^2 B^2 \\
D^7 A^7 &= C^8
\end{align*}
\]

Let \( A < B < C < D \) be the ordering on the generators. Our program generated a canonical basis different from the one reported in [2]; our result is given below:

\[
\begin{align*}
D^2 C^2 &= D C^2 \\
D C^3 &= D C^2 \\
D C^2 B &= D C^2 \\
D C^2 A &= D C^2 \\
D^4 B^2 &= D C^2 \\
C^{10} &= D C^2 \\
C^8 B^2 &= D C^2 \\
C^3 B^8 A &= D^3 B^2 \\
D^7 A^7 &= C^8
\end{align*}
\]

Later, we discovered that indeed the basis reported by Lankford and Ballantyne is not a canonical basis because, by their basis, the word \( A^2 B^2 C^5 D^2 \) has two distinct normal forms \(- C^5 D \) and \( A B C^2 D \). The presence of a bug in their implementation was later confirmed by Lankford in personal communication.

7. REFERENCES


