An Extension of Buchberger's Algorithm and Calculations in Enveloping Fields of Lie Algebras†

J. APEL AND W. LASSNER

Naturwiss.-Theoretisches Zentrum und Sektion Mathematik, Karl-Marx-Universität, DDR-7010 Leipzig

(Received 10 April 1986; revised 5 December 1986)

The powerful concept of Gröbner bases and an extension of the Buchberger algorithm for their computation have been generalised to enveloping algebras of Lie algebras. Algorithms for the computation of syzygies by use of Gröbner bases are given. This is the first method which allows the transformation of right fractions into left fractions in the Lie field of any finite dimensional Lie algebra. That enables CAS calculations in Lie fields. An AMP program LIEFIELD has been written for this purpose. Another AMP program SYZYGY produces a generating set of the syzygy module of any finite subset of an enveloping algebra. Examples for both programs are presented for the Weyl algebra and the so(3).

1. Introduction

Extending the Buchberger (1965) algorithm to certain types of non-commutative algebras we present an algorithm for CAS calculations in enveloping fields of Lie algebras, i.e. in "rational functions" of generators of Lie algebras.

The main difficulty of calculations in these non-commutative fields of fractions consists in transforming right fractions into left fractions. The algorithm presented solves this non-trivial task together with a mathematically more fundamental problem in abstract algebra—the calculation of the module of syzygies (Gröbner, 1949).

This result is not only of principal interest for algebraists. It also supports constructive ways in representation theory of Lie algebras (Kirillov, 1972; Božek, Havlíček & Navrátil, 1985). The algorithm is of interest for physicists in connection with spectrum generating algebra methods (Cordero & Chirardi, 1972).

We present two algorithms and corresponding AMP (Drouffe, 1981) programs LIEFIELD and SYZYGY. The first one is thought for computer calculations in enveloping fields. SYZYGY calculates not only one syzygy but a generating set of the module of syzygies. We underline that the algorithm presented allows calculations in the enveloping field of any finite dimensional Lie algebra.

So the algorithm covers more than only the Weyl algebra for which also other algorithms are known (Lassner, 1980; Galigo, 1985) and more than the calculation of syzygies of only linear elements from enveloping algebras (Beckmann, 1984).

† This is a revised version of a contribution to the International Conference on Computer Algebra and its Applications in Theoretical Physics, Dubna, 17–20 September 1985.
Let $L$ be a finite dimensional Lie algebra over a field $K$. We recall that the tensor algebra $T$ of $L$ is $T = \bigotimes_{n=1}^{\infty} L \otimes \ldots \otimes L$, in particular, $T^1 = \mathbb{K} \cdot 1$ and $T^1 = L$. Let $I$ be the two-sided ideal of $T$ generated by the tensors $x \otimes y - y \otimes x - [x, y]$, where $x, y \in L$. The associative algebra $T/I$ is called the enveloping algebra of $L$ and denoted by $U(L)$ (Dixmier, 1974). The composition of the canonical mappings $L \rightarrow T \rightarrow U(L)$ is called canonical mapping $\delta$ of $L$ into $U(L)$. We have

$$\delta(x)\delta(y) - \delta(y)\delta(x) = \delta([x, y])$$

for all $x, y \in L$. We denote the canonical image of $T^0 \oplus T^1 \oplus \ldots \oplus T^q$ in $U(L)$ by $U_q(L)$, i.e. $\text{deg}(f) \leq q$ for $f \in U_q(L)$.

**Lemma 1** (Dixmier, 1974). Let $a_1, \ldots, a_p \in L$, $\sigma$ the canonical mapping of $L$ into $U(L)$, and $\pi$ be a permutation of $\{1, \ldots, p\}$. Then

$$\sigma(a_1) \ldots \sigma(a_p) - \sigma(a_{\pi(1)}) \ldots \sigma(a_{\pi(p)}) \in U_{p - 1}(L).$$

From now we denote the canonical image of $x \in L$ in $U(L)$ by the same letter $x$. The Poincaré–Birkhoff–Witt theorem ensures the existence of the following basis in $U(L)$. Let $(x_1, \ldots, x_n)$ be a basis of the vector space $L$. Then the $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, where $i_1, \ldots, i_n \in \mathbb{N} \cup \{0\}$, form a basis of $U(L)$. We denote this basis by $B$ and we assume the elements of $U(L)$ always to be represented with respect to this basis. We denote the coefficient of $t \in B$ in $f \in U(L)$ by $c(f, t)$. Now we sketch the definition of the enveloping field (or Lie field) $D(L)$ (Kirillov, 1972; Dixmier, 1974). Consider the set of formal expressions of the forms $xy^{-1}$ and $y^{-1}x$, where $x, y \in U(L)$ and $y \neq 0$. A left fraction $y^{-1}x_1$ is defined to be equivalent to a right fraction $x_2y_2^{-1}$ if $x_1y_2 = x_2y_1$. Two left (right) fractions are defined to be equivalent if they are equivalent to one and the same right (left) fraction. The enveloping field is defined to be the set of classes of equivalent fractions equipped with the following operations. Consider two fractions $y_1^{-1}x_1$ and $y_2^{-1}x_2$ which represent the classes $a_1$ and $a_2$. In $U(L)$ there always exists a common left multiple, i.e. for given $y_1$ and $y_2$ there exist two elements $z_1$ and $z_2$ such that $z_1y_1 = z_2y_2$ (Ore condition).

Clearly, $y_1^{-1}x_1$ is equivalent to $(z_1 y_1)^{-1}(z_1 x_1)$. The sum $a_1 + a_2$ is the equivalence class of $(z_1 y_1)^{-1}(z_1 x_1 + z_2 x_2)$. The class of the quotient $a_1^{i_1} a_2^{i_2}$ is the class of $(z_1 x_1)^{-i_1}(z_2 x_2)^{i_2}$. The remaining arithmetic operations are defined through

$$a_1 - a_2 = a_1 + (-1)a_2$$

and

$$a_1 a_2 = (a_1^{-1})^{-1}a_2.$$ 

In order to represent a product of two left fractions $a^{-1}b$ and $c^{-1}d$ again by a left fraction $f^{-1}g = a^{-1}b c^{-1}d$ one has to find a left fraction $c^{-1}b'$ equivalent to the occurring right fraction $bc^{-1}$ such that $bc^{-1} = c^{-1}b'$, i.e. $f^{-1}g = (b'a)^{-1}(c'd)$.

**Problem 1.a.** Given a right fraction $ab^{-1}$. Find a left fraction $c^{-1}d$ such that $c^{-1}d = ab^{-1}$.

Note that in general a solution of problem 1a needs more than some commutations according to rules of the type $[u, v^{-1}] = v^{-1}[v, u]v^{-1}$ etc. One has to solve the following task.

**Problem 1.b.** Given $a, b \in U(L)$. Find a (non-zero) solution $(c, d)$ such that $c, d \in U(L)$ and $ca - db = 0$.

This is a special case ($m = 2$) of the following problem.
PROBLEM 1. Given \( m \) elements \( g_1, \ldots, g_m \) of \( U(L) \). Find a (non-zero) syzygy \((h_1, \ldots, h_m)\) of 
\[
 g_1, \ldots, g_m, \text{ i.e. a solution of the equation }
\]
\[
 h_1 g_1 + \ldots + h_m g_m = 0, \quad h_1, \ldots, h_m \in U(L). \tag{1}
\]
While finding only one syzygy of a finite set is trivial in the commutative case, this is in
general a hard problem in the non-commutative case. We attack problem 1 inside a larger
problem.

PROBLEM 2. Given a finite basis \((g_1, \ldots, g_m)\) of a left ideal of \( U(L) \). Find a finite set
\[
 \{(h_{11}, \ldots, h_{1m}), \ldots, (h_{s1}, \ldots, h_{sm})\}, \quad h_{ij} \in U(L), \ 1 \leq i \leq s, \ 1 \leq j \leq m,
\]
which generates the \( U(L) \)-module of the syzygies of \( g_1, \ldots, g_m \), i.e.
\[
 \sum_{j=1}^{m} h_{ij} g_j = 0, \quad 1 \leq i \leq s,
\]
and any syzygy \((h_1, \ldots, h_m)\) is an \( U(L) \)-combination
\[
 (h_1, \ldots, h_m) = \sum_{i=1}^{s} k_i (h_{i1}, \ldots, h_{im}), k_1, \ldots, k_s \in U(L). \tag{2}
\]

3. Extended Buchberger Algorithm

Starting from the notions and results for the commutative case as first introduced in
Buchberger (1965) and tutorially described in Buchberger's summarising paper (1985) we
present a generalisation of Gröbner bases and the Buchberger algorithm to enveloping
algebras of Lie algebras. The class considered contains the commutative ring
\( K[x_1, \ldots, x_n] \) as special case, where the given algorithm specialises to the Buchberger
algorithm, i.e. in its present version to that for non-reduced Gröbner bases.

The extension to enveloping algebras includes some new notions. The theoretical
foundation is given in a series of lemmata. Since the complete proofs are rather long they
are given in details in a forthcoming paper. Though our lemmata are proven for a rich
class of non-commutative algebras the proofs benefit from the basic ideas in the
commutative case.

Due to the non-commutativity various notions require the distinction between left-,
right-, or two-sided ones. Since we consider only left ideals the attribute “left-” occurring
in the definitions will be dropped if no confusion is possible.

For a special class of rings \( A \) the following lemma 2 originates from Zacharias (1978).

Lemmata 2. Let \( A \) a ring with unit element, \( F = (f_1, \ldots, f_m) \) and \( G = (g_1, \ldots, g_2) \) two bases of
the left ideal \( I \subset A \), \( X \) and \( Y \) transformation matrices such that \( G^T = XF^T \) and \( F^T = YG^T \),
and \( R \) be a matrix whose rows generate the syzygy module of \( G \). Then the rows of
\[
 Q = \begin{pmatrix}
 I_m - YX \\
 RX 
\end{pmatrix}
\]
generate the module of syzygies of \( F \); \( I_m \) is the \((m, m)\)-unit matrix.

Proof. (1) The \( Q \)-rows are syzygies
\[
 QF^T = \begin{pmatrix}
 I_m - YX \\
 RX 
\end{pmatrix} F^T = \begin{pmatrix}
 F^T - YXF^T \\
 RXF^T 
\end{pmatrix} = \begin{pmatrix}
 F^T - YG^T \\
 RG^T 
\end{pmatrix} = \begin{pmatrix}
 F^T - F^T \\
 0 
\end{pmatrix} = 0.
\]
(2) (Any syzygy is an $A$-combination of $Q$-rows). Assume $h$ is a syzygy of $F$, i.e. $hF^T = 0$. Because of $F^T = YG^T$ this means $hY$ is syzygy of $G$, i.e. $hY$ is $A$-combination of $R$-rows $hY = kR$ with coefficients $k_i \in A$. So it follows $hYX = kRX$, $h(I_m - I_n + YX) = kRX$, and finally $h = kRX + h(I_m - YX)$, i.e. $h$ is an $A$-combination of $Q$-rows.

As in commutative polynomial rings our extended Buchberger algorithm is a suitable tool for computing a basis $G$, matrices $X$, $Y$, $R$, and the syzygies of the given $(f_1, \ldots, f_m) = F$.

We define an ordering in the basis $B$ of $U(L)$ by

$$x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} < x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

iff the first non-zero component of

$$\left( \sum_{k=1}^{n} (i_k - j_k), i_1 - j_1, \ldots, i_n - j_n \right)$$

is negative.

We introduce the following notations with respect to $<$ for elements $f$ of $U(L)$.

$LBE(f)$: (leading basis element of $f$) the maximal (w.r.t. $<$) basis element $t$ such that $c(f, t) \neq 0$.

$LC(f)$: (leading coefficient of $f$) $LC(f) = c(f, LBE(f))$.

Note some properties of $<$ which are fundamental for the proofs:

(i) $1 = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} < u$ for all $u \in B \setminus \{1\}$.

(ii) Any sequence $u_1, u_2, \ldots, u_i, \ldots$ such that $u_{i+1} < u_i$ for all $i \geq 1$ is finite. ($<$ is a Noetherian ordering.)

(iii) For all $t \in B: u < v$ iff $LBE(tu) < LBE(tv)$.

Furthermore, we define a special "multiple property" for basis elements of $U(L)$.

DEFINITION 1. $u \in B$ is called left top multiple (LTM) of $v \in B$ if there exists a $t \in B$ such that $LBE(tv) = u$. $t \in B$ is called common left top multiple (CLTM) of $u \in B$ and $v \in B$ if there exist $t_1, t_2 \in B$ such that $LBE(t_1 u) = LBE(t_2 v) = t$. The minimal (w.r.t. $<$) CLTM of $u \in B$ and $v \in B$ is called least common left top multiple and denoted by $LCLTM(u, v)$.

Note the analogy of the property

$$LCLTM(x_1^{i_1} \ldots x_n^{i_n}, x_1^{j_1} \ldots x_n^{j_n}) = x_1^{\max(i_1, j_1)} \ldots x_n^{\max(i_n, j_n)}$$

to that of $LCM$ in $K[x_1, \ldots, x_n]$.

A first concept of Gröbner bases for a rich class of non-commutative algebras was developed by Mora (1985). This class is different from our one. While Mora saved the property that the basis elements form a free semigroup, we save Dickson's lemma. The existence of Gröbner bases for any finite generated left ideal is ensured and a constructive way for finding it is given for our class.

LEMMA 3. (Analogue to Dickson's lemma.) Let $t_1, t_2, \ldots, t_i, \ldots$ be a sequence of elements of $B$ such that $t_i$ is not a LTM of $t_j$ for $i > 1$ and $j < i$. Then this sequence is finite.

The proof of Dickson (1913) can be used nearly without changes.

Let us deal now with the reduction of elements of $U(L)$ with respect to a finite subset of $U(L) \setminus \{0\}$.
DEFINITION 2. Let $F = \{f_1, \ldots, f_m\}$ be a finite subset of $U(L) \setminus \{0\}$. Let $g$ and $h$ be elements of $U(L)$. $g$ is called left reducing to $h$ modulo $F$ (write $g \rightarrow_F h$) if there exist $f_i \in F$, $u \in B$, and $a \in K$ such that $c(g, LBE(u f_i)) \neq 0$, $a = c(g, LBE(u f_i))/LC(u f_i)$ and $h = g - a u f_i$. 

$$\sum_{i=1}^{m} h_i f_i + h$$ is called a left normal representation of $g$ modulo $F$ if $g = \sum_{i=1}^{m} h_i f_i + h$, there is no $h'$ such that $h \rightarrow_F h'$, and $LBE(h f_i) < LBE(g)$, $h$ is called a left irreducible part of $g$ modulo $F$.

LEMMA 4. Let $F = \{f_1, \ldots, f_m\}$ be a finite subset of $U(L) \setminus \{0\}$. Then there does not exist any infinite sequence $g_1, g_2, \ldots, g_i, \ldots$ such that $g_i \rightarrow_F g_{i+1}$ for all $i \geq 1$.

The proof of the lemma goes by induction according to $LBE(g_i)$.

PROBLEM 3. Given a set $F = \{f_1, \ldots, f_m\} \subset U(L) \setminus \{0\}$ and an element $g$ of $U(L)$, compute a left normal representation of $g$ modulo $F$.

ALGORITHM 1. $LNR(F, g; h, h_1, h_2, \ldots, h_m)$
1. $h := g$, $h_i := 0$ (1 $\leq i \leq m$)
2. while exist $f_j \in F$ and $t \in B$ such that $c(h, t) \neq 0$ and $t$ is $LTM$ of $LBE(f_j)$ do
2.1. choose a pair $(f_j, t)$ where $t$ is maximal (w.r.t. $<$) among all these pairs $(f_j, t)$
2.2. compute $u$ and $a$ such that $LBE(u f_j) = t$ and $a = c(h, t)/LC(f_j)$
2.3. $h := h - a u f_j$
2.5. $h_j := h_j + a u$.

PROOF OF CORRECTNESS. Obviously, all steps are computable. After each execution of loop 2 the equation

$$\sum_{i=1}^{m} h_i f_i + h = g$$

is satisfied. $LBE(h f_i) < LBE(g)$ holds in any step. After termination $h$ is a left irreducible part of $g$ modulo $F$.

PROOF OF TERMINATION. Let $g_k$ be the value of $h$ before the $k$th execution of loop 2. The sequence $g_1, g_2, \ldots, g_k, \ldots$ is finite according to lemma 4.

Now we transfer the ideas of "S-polynomials" (Buchberger, 1965) and Gröbner bases to enveloping algebras of Lie algebras.

DEFINITION 3. The element $SE(f_1, f_2) := c_2 u_1 f_1 - c_1 u_2 f_2$ of $U(L)$, where $u_i \in B$, $c_i = LC(f_i)$, and $LBE(u_i f_i) = LCLTM(LBE(f_i), LBE(f_j))$, $i = 1, 2$ is called the left $S$-element corresponding to the elements $f_1$ and $f_2$ of $U(L) \setminus \{0\}$.

DEFINITION 4. A finite subset $F = \{f_1, \ldots, f_m\}$ of $U(L) \setminus \{0\}$ is called left Gröbner basis of the left ideal $J \subset U(L)$ if $F$ generates $J$ and zero is a left irreducible part modulo $F$ of any left $S$-element $SE(f_1, f_j)$ corresponding to two elements $f_i$ and $f_j$ of $F$.

Note that the so-defined Gröbner bases are just those finite subsets $G$ of $U(L) \setminus \{0\}$ for which the left irreducible part of any $g \in U(L)$ modulo $G$ is uniquely determined.
Remember that the syzygies of an arbitrary finite set \( F \) could be found according to lemma 2 if the module of syzygies of \( G \) would be given (by \( R \)). For a Gröbner basis \( G \) this gap will be closed by lemma 5.

**Lemma 5.** Let \( G = (g_1, \ldots, g_m) \) be a Gröbner basis and \( \text{LC}(g_k) = 1, i \leq k \leq m \). For any pair \( (g_i, g_j) \) where \( 1 \leq i < j \leq m \) let \( u_i^j \) and \( u_j^i \) be basis elements of \( U(L) \) such that

\[
\text{LCLTM}(\text{LBE}(g_i), \text{LBE}(g_j)) = \text{LBE}(u_i^j g_i) = \text{LBE}(u_j^i g_j),
\]

and let \( h_k^i \) be elements of \( U(L) \) such that \( \text{LBE}(h_k^i g_k) \leq \text{LBE}(\text{SE}(g_i, g_j)) \) and

\[
\sum_{i = 1}^{m} h_k^i g_k - (u_i^j g_i - u_j^i g_j) = 0. \tag{4}
\]

Then the \( m \)-tuples

\[
r_i^j = (h_1^i, \ldots, h_{i-1}^i, h_i^j - u_i^j, h_{i+1}^j, \ldots, h_{j-1}^j, h_j^j + u_j^j, h_{j+1}^j, \ldots, h_m^j), \quad 1 \leq i < j \leq m \tag{5}
\]
generate the module of syzygies of \( g_1, \ldots, g_m \).

**Proof idea.** That the \( r_i^j \) are syzygies of \( g_1, \ldots, g_m \) follows by (4). The proof that any syzygy \( s = (s_1, \ldots, s_m) \) of \( g_1, \ldots, g_m \) in \( U(L) \)-combination of the \( r_i^j \) can be performed by induction according to the maximal (w.r.t. \(<\)) element among all \( \text{LBE}(s_k g_k) (1 \leq k \leq m) \).

This connection between Gröbner bases and syzygies in the commutative case can be found already in the thesis of Zacharias (1978). Later it was described and generalised by certain authors, for example by Moeller & Mora (1986).

Now we are ready to present the main algorithm which could be characterised as an extension of the Buchberger algorithm to enveloping algebras. In the present version the extension corresponds to non-reduced Gröbner bases. Since the elements of the finite set \( F \) appear as the first elements (up to a factor from \( K \)) in \( G \), the first rows \( I_0 = YX \) of \( Q \) described in lemma 2 are zero. Hence, they can be dropped, i.e. \( Q = RX \) may be used. Due to the lemmata 2 and 5 the central problem 2 goes over in the following one.

**Problem 4.** Given a finite set \( F = (f_1, \ldots, f_m) \), where \( f_i \neq 0 \). Compute a left Gröbner basis \( G = (g_1, \ldots, g_l) \) such that \( F \) and \( G \) generate the same left ideal in \( U(L) \), \( \text{LC}(g_l) = 1 \) \((1 \leq i \leq l)\), and \( f_i = \text{LC}(f_i) g_i \) \((1 \leq i \leq m)\). Furthermore, compute matrices \( X \), \( R \), and \( Q \) such that \( G^T = X F^T \) and the rows of \( R \) and \( Q \) generate the modules of the syzygies of \( G \) and \( F \), respectively.

Problem 4 will be solved by the following algorithm.

**Algorithm 2. SYZYGY(F; G, X, R, Q)**

1. \( l := m \)
2. \( R := (0, 0, \ldots, 0), \ Q := (0, 0, \ldots, 0) \) (rows of length \( m \))
3. \( c_k := \text{LC}(f_k) \) \((1 \leq k \leq m)\)
4. \( g_k := f_k/c_k \) \((1 \leq k \leq m)\)
5. \( X := \begin{pmatrix} 1/c_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1/c_m \end{pmatrix} \)
6. \[ G := (g_1, \ldots, g_m) \]
7. \[ P := \{(g_i, g_j) | 1 \leq i < j \leq m\} \]
8. while \( P \neq \emptyset \) do
8.1. take \((g_i, g_j) \in P\)
8.2. \[ P := P \setminus \{(g_i, g_j)\} \]
8.3. \[ h' := SE(g_i, g_j) \]
8.4. \[ h_i := h - u_1^i \]
8.5. \[ h_i := h_i + u_2^i (u_1^i \text{ and } u_2^i \text{ such that } SE(g_i, g_j) = u_1^i g_i - u_2^j g_j) \]
8.6. \[ H := (h_1, \ldots, h_l) \]
8.7. if \( h = 0 \)
8.7.1. then \[ R := \begin{pmatrix} R \\ H \end{pmatrix} \]
8.7.2. else
8.7.2.1. R := \[
\begin{pmatrix}
R \\
H
\end{pmatrix}
\]
8.7.2.2. H := \(-1/\text{LC}(h) \cdot H\)
8.7.2.3. X := \[
\begin{pmatrix}
X \\
HX
\end{pmatrix}
\]
8.7.2.4. \[ g_{i+1} := h/\text{LC}(h) \]
8.7.2.5. \[ G := (g_1, \ldots, g_i, g_{i+1}) \]
8.7.2.6. \[ P := P \cup \{(g_k, g_{i+1}) | 1 \leq k \leq l\} \]
8.7.2.7. \[ l := l + 1 \]
8.8. \[ Q := \begin{pmatrix} Q \\ R_L \end{pmatrix} \] (R_L is the last row of R).

PROOF OF CORRECTNESS. Obviously all steps are computable. If \( P = \emptyset \) then any \( S \)-element corresponding to two elements of \( G \) has 0 as a left irreducible part modulo \( G \), hence \( G \) is a left Gröbner basis by definition 4. After each execution of loop 8 \( G^T = XF^T \) and \( RG^T = 0 \) are satisfied. After termination the rows of \( R \) are tuples (5) of lemma 5. Therefore, they generate the syzygy module of \( G \). That the \( Q \)-rows generate the module of syzygies of \( F \) follows from lemma 2.

PROOF OF TERMINATION. The only step which is of interest for the termination is loop 8. Let us consider the sequence \( LBE(g_1), LBE(g_2), \ldots, LBE(g_k), \ldots \). Since the \( g_k \) \((k > m)\) are left irreducible parts modulo \((g_1, \ldots, g_{k-1})\), there is no \( 1 \leq k' < k \) such that \( LBE(g_k) \) is \( LTM \) of \( LBE(g_{k'}) \). According to lemma 3 such a sequence must be finite. Therefore, only a finite number of pairs \((g_i, g_j)\) must be treated.

REMARK. It is possible to avoid the initialisation of \( R \) and \( Q \) to abundant trivial syzygies \((0, 0, \ldots, 0)\) in step 2. It could be used as initialisation according to loop 8.

Of course, algorithm 2 solves not only problem 2 but also the subproblem 1. But a slight change makes the algorithm more efficient for this purpose. Since \( G^T = XF^T \) and \( RG^T = 0 \) are satisfied after each execution of the loop 8 the equation \( QF^T = RXF^T = 0 \) is
satisfied, too. This means, whenever $Q$ is not a zero matrix in step 8, problem 1 is already solved. Therefore, we change step 8 into

8. while $P \neq \emptyset$ and $Q = 0$ do

In this form the algorithm is called algorithm 2a. It is used for calculations in Lie fields, i.e. for transforming right fractions into left fractions.

Clearly, algorithm 2a is much more time efficient than algorithm 2. In order to calculate only one non-zero syzygy also only a part of the Gröbner basis must be generated in most cases.

4. Implementation

The algorithms 2 and 2a have been realised in the computer algebra system AMP (version 6.4) (Drouffe, 1981). The programs SYZYGY (algorithm 2) and LIEFIELD (algorithm 2a) have been tested on an ESER computer EC 1040.

5. Examples

Let $x_1, x_2, x_3$ be the generators of the Lie algebra $so(3)$, with commutation rules

$$[x_1, x_2] = x_3, \quad [x_2, x_3] = x_1, \quad [x_1, x_3] = -x_2.$$ 

**Example 1.** Consider the right fraction $(x_1 x_2) x_1^{-1}$. We start with $F = (x_1 x_2, x_1)$. SYZYGY computes the Gröbner basis $G = (x_1 x_2, x_1, x_3, x_2)$, the transformation matrix $X$ ($G^T = X F^T$)

$$X = \begin{pmatrix}
1 & 0 \\
0 & 1 \\
1 & -x_2 \\
-x_1 & x_1 x_2 + x_3
\end{pmatrix},$$

the matrix $R$ the rows of which generate the module of syzygies of the Gröbner basis $G$

$$R = \begin{pmatrix}
1 & -x_2 & -1 & 0 \\
0 & x_3 & -x_1 & -1 \\
0 & -1 & x_2 & -x_3 \\
0 & x_2 & 1 & -x_1 \\
1 & 0 & 0 & -x_1 \\
x_3 & x_1 & -x_1 x_2 & -x_2
\end{pmatrix},$$

and the matrix $Q$ whose rows generate the module of syzygies of $F$

$$Q = \begin{pmatrix}
0 & 0 \\
0 & 0 \\
-x_1 x_2 x_3 + x_2^2 - 2x_1^2 - x_1^2 - 1 \\
x_1^2 + 1 & -x_1 x_2 - x_1 x_3 \\
x_1^2 + 1 & -x_2 x_2 - x_1 x_3 \\
0 & 0
\end{pmatrix}.$$
Therefore, the left fraction equivalent to the right fraction above has the following form:
\[
\left( a_1(x_1 x_3 + 2x_2) + a_2(x_1^2 + 1) \right)^{-1} \left( a_1(x_1 x_3 - x_1^2 + 2x_2^2 + x_3^2 + 1) + a_2(x_1^2 x_3 + x_1 x_3) \right),
\]
where \( a_1 \) and \( a_2 \) are arbitrary elements of \( U(\text{so}(3)) \) such that the denominator is not zero.

Note that this is a general solution of the problem, but in the practical use for calculations in Lie fields it is enough to have one non-zero syzygy.

LIEFIELD gives:
\[
(x_1 x_3 + 2x_2)^{-1} (x_1 x_3 - x_1^2 + 2x_2^2 + x_3^2 + 1) = (x_1 x_3 x_1)^{-1}.
\]

Consider the Weyl algebra \( A_2 \) with the basis elements \( q_1, q_2, p_1, p_2 \) and the only non-vanishing commutators \([p_i, q_j] = 1\) between the generators \( q_i, p_i, 1 \) (\( i = 1, 2 \)).

**Example 2.** Consider the right fraction \( (3p_1 - p_0)(1/23q_2 p_1 + p_2) \). The input is
\[
F = (3p_1^2 - p_1, 1/23q_2 p_1 + p_2).
\]
SYZYGY computes the left Gröbner basis
\[
G = (p_1^3 - 1/3p_1, q_2 p_1 + 23p_2, p_1 p_2, p_1^2, p_1 p_2, p_2^2 + 1/23p_1, p_1, p_2).
\]
The matrix \( Q \) contains 28 rows where 22 among them are non-zero. The degree of the first component of the non-trivial syzygies is in the range from 5 up to 9. LIEFIELD gives only the shorter basis
\[
G = (p_1^3 - 1/3p_1, q_2 p_1 + 23p_2, p_1 p_2, p_2^2, p_2^2)
\]
(not yet a left Gröbner basis). The first non-zero syzygy is the third computed one. The returned left fraction is
\[
(1/3q_2 p_1^3 + 23/3p_2 + 2p_1 p_2^2 - 1/9q_2 p_1^2 - 23/9q_1 p_2)^{-1} (23p_1^2 - 46/3p_1 p_2^3 + 23/9p_1^2)
= (3p_2 p_1)(1/23q_2 p_1 + p_2)^{-1}.
\]

In the first example the relation between the running times of SYZYGY and LIEFIELD is 19.5 sec : 10.3 sec. In the second example it is 61 sec : 12 sec. We presented examples from computation in Lie fields. Therefore, \( F \) had had only two elements. Of course, SYZYGY computes the module of the syzygies of \( f_1, \ldots, f_m \) also for \( m > 2 \).

Due to the excessive use of non-commutative multiplications the running time strongly depends on a fast multiplication procedure. The multiplication is realised using LET-commands suitable for any enveloping algebra. For the Weyl algebra twisted products (Lassner, 1980) are three times faster.

6. **Concluding Remarks**

The algorithm presented is especially aimed to calculations in Lie fields. Instead of left ideals, left Gröbner bases etc., we could consider right ones. In this paper we did not deal with two-sided ideals, since they are not interesting for the computation of syzygies. Further extensions analogously to the commutative case are imaginable. It is possible to introduce reduced Gröbner bases (Buchberger, 1985) and to extend the method to left vector modules (Moeller & Mora, 1986) over enveloping algebras. That makes it possible to compute free resolutions of left (right) ideals in enveloping algebras. Note, however, that not everything transfers from the commutative to the considered non-commutative case, as the following examples show.

— The "purely lexicographical ordering" (Buchberger, 1985) cannot be used in \( U(L) \) since property (iii) does not hold.
Criterion 2 (Buchberger, 1985) does not hold. For instance, \( F = (p, q) \subseteq A_1 \) would be a left Gröbner basis according to such a criterion, but this is wrong since \( SE(p, q) = -1 \) does not have zero as left irreducible part.

We would like to thank Professor B. Buchberger from the Johannes Kepler University, Linz for valuable discussions and hints about his algorithm.

References


