J. Symbolic Computation (1990) **9**, 27–38

An Algorithm for the Construction of Matrix Representations for Finitely Presented Non-commutative Algebras*

GILLES LABONTÉ

Department of Mathematics and Computer Science, Royal Military College of Canada, Kingston, Ontario, Canada K7K 5L0

(*Received* 12 *November* 1987)

Let a finite presentation be given for an associative, in general non-commutative algebra E, with identity, over a field. We study an algorithm for the construction, from this presentation, of linear, i.e. matrix, representations of this algebra. A set of vector constraints which is given as part of the initial data determines which particular representation of E is produced.

This construction problem for the algebra is solved through a reduction of it to the much simpler problem of constructing a Gröbner basis for a left module. The price paid for this simplification is that the latter is then infinitely presented.

Convergence of the algorithm is proven for all cases where the representation to be found is finite dimensional; which is always the case, for example, when E is finite. Examples are provided, some of which illustrate the close relationship that exists between this method and the Todd–Coxeter coset-enumeration method for group theory.

1. Introduction

In many practical applications, it is very useful to have available explicit matrix representations for the elements of (generally non-commutative) algebras. Our own initial motivation for this study in fact stems from such an application, made while studying quantum mechanical wave equations which are covariant under the Poincaré group (see Labonté, 1987*a*). It is the purpose of this article to analyse a general method for constructing representations of algebras, when given finite presentations for them.

The field of constructive methods involving ideals of polynomials with commutative variables has been quite active in the past few years. This is due in great part to the introduction of the concepts of Gröbner bases (see, for example, Buchberger, 1965; 1979; 1985) and standard bases (Hironaka, 1964) and of the algorithms involving them.

For structures with non-commutative variables, which concern us more in this article, only constructive group theory has seen a comparable level of activity in the past. A good idea of the achievements in that field can be found in the survey by Neubüser (1983). For rings and algebras, there are relatively few results, given the vastness of the subject, concerning constructive techniques. As in the Abelian case, the formalism of rewriting theory (see, for example, Huet, 1980) has been used with advantage in their description. Noteworthy realisations are Bergman's (1978) discussion of the possibility of establishing a unique canonical form for the elements of algebras, and suggestion of using a completion algorithm of Buchberger or Knuth–Bendix (see Knuth & Bendix, 1970) type to deal with their presentations.

* This Research was supported in part by a grant from the Academic Research Program of the Canadian Department of National Defence.

0747–7171/90/010027+12 $03.00/0

Galligo (1985) has studied Gröbner bases for left ideals in Weyl algebras. Mora (1985) and Kandri-Rody & Weispfenning (1986) have studied Gröbner bases for two-sided ideals of algebras and rings. Apel & Lassner (1986*a*; 1986*b*; 1987) have extended Buchberger's algorithm in order to produce programs to perform calculations in enveloping fields of Lie algebras. Le Chenadec (1986) has discussed the completion of finite presentations corresponding to semi-groups, monoids, modules, groups and rings (see mainly Chapter 4 of his book). He has also produced a LISP system which performs such completions. Particularly worthy of attention also are Mora's studies (1988*a*; 1988*b*) of Gröbner bases and algorithms for their computation, which are done in a very wide algebraic context.

Most recent ventures into the domain of non-commutative algebras rest on generalisations of the Buchberger algorithm for the construction of Gröbner bases or more generally, on Knuth–Bendix completion. There is another very important construction technique which has been used, for an already longer time in the context of group theory: this is the Todd–Coxeter coset enumeration method [see Todd & Coxeter (1936) or Leech (1970)].

The algorithm which we discuss in this paper also corresponds to a somewhat different point of view than that taken in the non-commutative algebra Gröbner basis or completion techniques; it would be more closely related to Dehn's (1910) algorithm for the construction of the Cayley graph of a group (his "Gruppenbild") and coset enumeration. In fact, Labonté (1988) describes the algorithm as the construction of a weighted digraph which corresponds to the representation of the algebra; such digraphs are straightforward generalisations of Cayley graphs. On the other hand, Remarks 4 and 5, at the end of our Section 2, bear on the relationship to coset enumeration while the first examples of Section 4 serve to illustrate these remarks.

Even though the Buchberger algorithm or completion technique and the Todd–Coxeter coset enumeration method are so commonly used, there does not seem to have been studies in which their efficiencies have been systematically compared. Such a comparison of the algorithm, which we discuss in this paper, with the former techniques is of course also imperative; this will constitute the subject of a forthcoming study.

For the moment, we can only recall that the opinion has been expressed [see, for example, at the end of Chapter 6 of Le Chenadec (1986)] that coset enumeration would be more efficient in certain questions pertaining to the representations of groups. As for the algorithm discussed hereafter, it is clear that there are problems, involving the construction of particular representations of algebras, for which it will be more efficient than the Gröbner basis or completion approach. This is a direct consequence of the way such construction problems are posed. Indeed, consider such extreme cases as the following one. For the group G, specified by n generators A_i, $i = 1$ to n, and some relations between them; construct the particular representation for which the vector space is generated by a vector V such that $A_iV = V$ for each $i = 1$ to n. With our algorithm, which then reduces to coset enumeration (since the vector V is in fact a representative of the subgroup G of G), the construction is trivial, and yields immediately $A_i = I$ for $i = 1$ to n. On the other hand, it is clear that the construction of this representation of G would be longer by any method requiring that the presentation of the group be completed first. Example 6 of our Section 4 also correspond to extreme cases which show that the Gröbner basis or completion techniques for the algebra itself are not so well adapted to deal with the construction of particular representations. In these cases, the regular representation is infinite dimensional, and a finite particular representation is to be constructed. The presentations of the algebras involved are trivially completed (in one case there are no equations!) but, still, it is

hard to see how the above-mentioned methods would be of any help in producing the representation sought.

Leaving aside extreme cases, there certainly remain some problems with which the different algorithms could be meaningfully compared. Two important ones among these are the construction of finite dimensional regular representations of algebras, and the construction of Gröbner bases for commutative polynomial ideals. We are presently preparing a commutative version of our algorithm to conduct tests on the latter problem.

As a final remark, we point out the main feature of the algorithm discussed hereafter, which is that the need to deal with Gröbner bases for non-commutative algebras is bypassed, through a reduction of the problem to one dealing only with Gröbner bases for left modules. The theory for these is essentially identical to that of Gröbner bases for left ideals, and, as remarked by Mora (1985) at the end of his article, it is very simple compared to the theory of two sided ideals of algebras. As we will see, however, there is a price to be paid for this simplification in that the module presentations which have to be dealt with are infinite.

Despite this infinity, convergence of the algorithm can be proven, in the sense that whenever the given problem has a solution in the form of a finite representation for the algebra E, it will be finitely constructed. In particular, termination of the computation is always guaranteed when E is finite dimensional. The proof we give is similar in principle to that of Métivier (1983) [see also Proposition 3.8 in Chapter 3 of Le Chenadec's book (1986)] for the termination of the completion algorithm for presentations of finite groups.

2. Statement of the Problem

2.1. NOTATION

K is a field,
$A = \{X_1, X_2, \ldots, X_n\}$ is a finite alphabet,
A^+ is the free semi-group on A with the associative binary operation of concatenation of words, denoted by "conc",
e is the empty word,
$\langle A \rangle$ is the free monoid over A, with unit e,
$|w|$ is the length of the word w; $|e| = 0$,
$P = K\langle A \rangle$ is the free K-algebra on A, i.e. the algebra of polynomials with non-commutative variables in A and coefficients in K,

$GV = \{V_1, V_2, \ldots, V_m\}$ is a finite alphabet,
PV_i is the free cyclic left P-module generated by V_i; it is a linear vector space over K,
$P^m = PGV$ = the internal direct sum of all $PV_i : V_i \in GV$,
$B(\phi) = \{WV_i : W \in A^+, V_i \in GV\}$ is the set of monomials which forms a basis in P^m considered as a linear vector space over K,

LEQS is a finite subset of P, given as initial data,
I is the two-sided ideal of P generated by LEQS,
$I^m = IGV$ is the cyclic left I—module generated by GV,
E is the quotient algebra P/I,
LVEQS is a finite subset of P^m, given as initial data,

V = P LVEQS is the vector space over K defined as the left P—module generated by LVEQS.

2.2. A REPRESENTATION OF E

In the following, the relations $p \sim 0 : p \in$ LVEQS will play the role of constraints, given from the start, to be satisfied in the vector space carrying the representation sought. They effectively serve to specify which particular representation will be constructed. This way of characterising the various representations of E was chosen initially because it corresponded to the physical applications we then had in mind (see Labonté, 1987*a*). It was later kept, as it seemed to be a useful and fairly versatile way of doing so.

Let S be the vector space $V \cup I^m$, $u = \{u_1, u_2, \ldots, u_d\}$ be a basis in the quotient vector space $V_{rep} = P^m/S$, and $\sim$ be the congruence modulo S over the elements of P^m. V_{rep} then carries the linear representation of E described below.

Given that $\forall X_i \in A$ and $u_j \in u$,

$$X_i u_j \sim \sum_{k=1}^{d} c_{ijk} u_k \quad \text{for some} \quad c_{ijk} \in K; \tag{2.1}$$

with each $X_i \in A$ can be associated a linear function $\bar{X}_i : V_{rep} \to V_{rep}$, defined by

$$\bar{X}_i(u_j) = \sum_{k=1}^{d} c_{ijk} u_k. \tag{2.2}$$

With e can be associated the identity function $\bar{e} : \bar{e}(u_j) = (u_j)$. It then naturally follows that with $T = X_i X_j \ldots X_k \in A^+$ is associated $\bar{T}$:

$$\bar{T}(u_l) = \bar{X}_i(\bar{X}_j(\ldots \bar{X}_k(u_l)))$$

and with $P \in K\langle A\rangle$, $\bar{P}$:

$$\bar{P}(u_j) = \sum_i c_i \bar{T}_i(u_j),$$

when $P = \sum_i c_i T_i$, with $c_i \in K$ and $T_i \in \langle A\rangle$.

The elements of $E = P/I$ are equivalence classes denoted here $|[M]| = \{M+R : M \in P, R \in I\}$. If M_1 and M_2 belong to the same class $|[M]|$, then the operators $\bar{M}_1$ and $\bar{M}_2$ are equal. Indeed, $M_1 = M_2 + R$ for some $R \in I$, so that $\forall u_i \in u$:

$$\bar{M}_1(u_i) = \bar{M}_2(u_i) + \bar{R}(u_i) \sim \bar{M}_2(u_i) \text{ since } \bar{R}(u_i) = Ru_i \in I^m \subset S.$$

The class $|[M]|$ is thus represented by a single linear operator $\bar{M}_j$; M_j being any element of $|[M]|$.

2.3. THE PROBLEM SOLVED

The algorithm studied hereafter solves the problem of constructing the representation of E described above. Actually, it produces a basis u for V_{rep} and the set of coefficients $\{c_{ijk} \in K$: Eq. (2.1) holds$\}$ which, we recall, served to define the linear operators representing the generators of E as in Eq. (2.2).

We note that the dimension of V_{rep} is never known from the start: it is known only once the computation terminates. We shall assume hereafter that V_{rep} is finite dimensional. Of course, however, as for the general word problem, it is unknown how to characterise the

initial data: LEQS and LVEQS, for this to be the case. We shall furthermore consider that all calculations in K can be performed.

2.4. REMARKS

1. If LVEQS $= \phi$ then $S = I^m$ and $V_{rep} = P^m/I^m$; these are respectively called S_0 and V_0. The representation $\tilde{R}$, described in Section 2.2 is then equivalent to a direct sum of m times the left regular representation R as $\tilde{R} = R \oplus R \oplus \ldots \oplus R$. One such representation is carried by each vector subspace EV_i of V_0. We recall that the construction of the regular representation of E is equivalent to that of its whole multiplication table.

2. If LVEQS $\neq \phi$ then $S \supset S_0$ and $V_{rep} \subset V_0$. The representation constructed is thus a component of the regular representation $\tilde{R}$; which one it is depends on the actual choice of LVEQS, as remarked at the beginning of Section 2.2.

3. If E if finite, then V_{rep} is finite. Indeed, since $S \supseteq S_0$, $V_{rep} \subseteq V_0$ while the latter is finite.

4. Here is how coset enumeration appears as a particular instance of Problem 2.3. Let $E = KG$ be the group algebra of a group G, and LEQS be the set of binomials $w - w'$: the relation $w \sim w'$ is one in the group presentation. Let $GV = \{V_1\}$ with $V_1 = H =$ a subgroup of G, and $LVEQS = \{(g-1)\}V_1 : g \in H\}$. We note that the relations $p \sim 0$: $p \in$ LVEQS effectively define the "generating vector" $V_1 = H$ since $gH = H \; \forall \; g \in H$.

The algorithm studied then produces a realisation of the representation 2.2 in which the elements of the basis of V_{rep} are the different left cosets $g_iH : i = 1$ to d, of H in G. An arbitrary vector in V_{rep} is a set

$$\sum_{i=1}^{d} c_i g_i H: \; c_i \in K,$$

and vector addition is defined by $c_ig_iH + c_jg_jH = (c_ig_i + c_jg_j)H$. The first example of Section 4 illustrates this construction of the cosets.

5. Let each $V_i \in GV$ be a subset of the ring or algebra E. The representation constructed will then be very similar to that of the preceding case, in that the basis vectors will be sets xV_i: $x \in E$. Coset enumeration as described above is evidently just a particular instance of this more general vector-space construction.

Let each $V_i \in GV$ be an element of E. The vector space V_{rep} carrying the representation is then the union of the principal left ideals of E generated by each V_i. Examples of both these cases are provided in Section 4.

3. A Method of Solution

3.1. PRELIMINARIES

An order relation on $B(\phi)$ is needed. Let $<$ be an arbitrary alphabetical order on $GV \cup A$. We then extend the order relation $<$ to total degree order on $\langle A \rangle$ and on $B(\phi)$, defined by

$$w_1 \langle w_1 \quad \text{if} \quad |w_1| < |w_2|$$

or if $|w_1| = |w_2|$ and $w_1 < w_2$ with respect to the lexicographical order.

We denote as T[B(ϕ)] the graph defined as the union of the m independent trees T[PV_i], which are generated by the elements $V_i \in$ GV, and in which the closest descendants of a particular node W are the nodes $\{X_i\mathrm{W} : X_i \in \mathrm{A}\}$.

REMARK. A property of the total degree order which is crucial for the successful termination of the following algorithm (as will be seen in section 3.3) is that if B_i is the subset of $\mathrm{B}(\phi) = \{w : w \leqq i\text{th element of } \mathrm{B}(\phi)\}$, then

$$\lim_{i\to\infty} B_i = \mathrm{B}(\phi).$$

Pure lexicographical order, for example, does not have this property; since if V = Min(GV) and X = Min(A), then $B_i = \{\mathrm{V}, X\mathrm{V}, X^2\mathrm{V}, \ldots X^{i-1}\mathrm{V}\}$ and

$$\lim_{i\to\infty} B_i$$

exists but is not B(ϕ). Acceptable total-order relations for this algorithm must have the property that, as i increases, the element of $B_{i+1} - B_i$ traces a path, with a countably infinite number of steps, through the graph T[B(ϕ)] such that

$$\lim_{i\to\infty} B_i = \mathrm{B}(\phi).$$

Relations like $p \sim 0 : p \in \mathrm{P}^{\mathrm{m}}$ can always be rewritten as

$$W \sim f, \tag{3.1}$$

with W = lead (p) = the largest monomial of p, and $f \in \mathrm{P}^{\mathrm{m}}$.

The polynomial $W - f$ is then called the normalised form of p. The following concepts are trivial extensions to left modules of similar ones introduced by Buchberger (1965) [for a good introduction, see Buchberger (1985); note in particular Definitions 6.1, 6.2, 6.3 and 6.5], when dealing with commutative polynomials.

Let F be a set of normalised polynomials. For p_1 and $p_2 \in \mathrm{P}^{\mathrm{m}}$, we shall say that $p_1 \to_{\mathrm{F}} p_2$, (i.e. p_1 reduces to p_2 modulo F) if $\exists$ a $(W - f) \in \mathrm{F}$, while p_1 contains a monomial CW for some $C \in \langle \mathrm{A} \rangle$ with non-zero coefficient, and p_2 is obtained by substituting Cf for CW in p_1. p_1 will be said in normal or reduced form modulo F if $\nexists (W - f) \in \mathrm{F}$: $p_1 \to_{\mathrm{F}} p_2$. A Gröbner basis in the left-module P^{m} will be a subset of G of P^{m} such that each $p \in \mathrm{P}^{\mathrm{m}}$ has a unique normal form modulo G. A subset H of P^{m} will be said to be "reduced" if it is such that every $p \in \mathrm{H}$ is in normalised form, and reduced modulo $\mathrm{H} - \{p\}$.

Gröbner bases for left (or right) modules have a certain triviality, as the following theorem [which is a trivial variant of one, given in Section 4 or Mora (1985), for left and right ideals in non-commutative algebras] indicates.

THEOREM. *Any reduced set F is also a reduced Gröbner basis.*

PROOF: Each $p \in \mathrm{P}^{\mathrm{m}}$ has a unique normal form modulo F iff any monomial $X \in \mathrm{B}(\phi)$ has this property. An ambiguity in the reduction of X to a normal form modulo F can only occur as

$$X = C_1 W_1 = C_2 W_2 \tag{3.2}$$

with C_1 and $C_2 \in \langle \mathrm{A} \rangle$, while $(W_1 - f_1)$ and $(W_2 - f_2) \in \mathrm{F}$. However, (3.2) is obviously possible only if one of (W_1, W_2) is a suffix of the other, which cannot be since F is reduced.

Thus all normal forms are unique.

3.2. THE ALGORITHM

For the following algorithm, the important variables will be a finite reduced left module Gröbner basis $G \subset P^m$, and a possibly infinite subset B(G) of $B(\phi)$. The latter will be the ordered list of monomials of $B(\phi)$ which are irreducible modulo G, i.e. $B(G) = B(\phi) - \{W \text{ and all its descendants: } (W-f) \in G\}$. With B(G) can always be associated a graph T[B(G)], which is the union of m distinct trees, each one being a connected subtree of one of the $T[PV_i]$s.

With each $X_i \in A$, will be associated the linear function $\bar{X}_i : P^m \to P^m$, defined such that $\forall\, W \in B(\phi)$:

$$\tilde{X}_i(W) = \begin{cases} f & \text{if } (X_i W - f) \in G, \\ \text{conc}(X_i, W) & \text{if not.} \end{cases} \tag{3.3}$$

Upon defining $\tilde{e} : \tilde{e}(W) = W\ \forall\, W \in B(\phi)$, the definition of $\tilde{T}$ for $T \in \langle A \rangle$, and of $\tilde{P}$ for $P \in K\langle A \rangle$ then naturally follows, as previously for $\bar{T}$ and $\bar{P}$ [see after Eq. (2.2)].

Given initial variables: a finite reduced Gröbner basis $G = G_0$, $B(G_0)$, and a finite list L of polynomials which are reduced modulo G_0, the following procedure will produce the finite reduced Gröbner basis $G = G_f$, obtained through the reduction of $G_0 \cup L$, and the corresponding B(G). Note that the left P-modules $P(G_0 \cup L)$ and PG_f are equal.

```
INCORPORATE (L)
while L ≠ φ do
    remove the first element p of L, and find its normalised form (W−f)
    remove W and all its descendants from B
    substitute f for W in each element of L and G
    replace the modified elements of G by their normalised form.
    while ∃ an element X_i W − g for some i, in G do
        remove it from G
        add [X̃_i(f) − g] at the end of L                                  (3.4)
```

When the initial G and L are finite, the termination of this computation follows straightforwardly from the well-foundedness of the order relation $<$. Note that if initially $G = \phi$, $B = B(\phi)$, then the P-module reduced Gröbner basis G_f, such that $PG_f = PL$ is computed.

Given the initial variables G_0, a finite reduced P-module Gröbner basis, $B_0 = B(G_0)$, and LEQS, a finite subset of P, the following algorithm will compute a reduced P-module Gröbner basis G_∞ such that the P-modules generated by G_∞ and $G_0 \cup [\text{LEQS } B(\phi)]$ are equal. This set LEQS $B(\phi)$ is $\{pW : p \in \text{LEQS}, W \in B(\phi)\}$; the P-module generated by this set is then simply I^m, since $B(\phi)$ is a basis in the vector space P^m. Thus

$$PG_\infty = PG_0 \cup I^m. \tag{3.5}$$

```
SOLUTION
  Z ← the first element of B_0
  B ← B_0 : G ← G_0 : i ← 0
Loop
  for each EQ ∈ LEQS do
    if Z is still in B then
      INCORPORATE ((ẼQ(Z)))
      i ← i+1 : B_i ← B : G_i ← G
```

(1) *if* $\exists\ Y \in B : Y > Z$ *then* $Z \leftarrow$ the smallest such Y : go Loop
else $B_k \leftarrow B\ \forall\ k > i$: *return* "construction completed" (3.6)

The construction problem explained in Section 2.2 is solved as follows. Given LVEQS, use Procedure (3.4) to obtain the reduced P-module Gröbner basis $G_0 : PG_0 =$ PLVEQS $= V$. Then, use this G_0 and $B(G_0)$ as initial data for Algorithm (3.6), so that the resulting reduced Gröbner basis G_∞ is, according to Eq. (3.5), such that

$$PG_\infty = V \cup I^m = S. \tag{3.7}$$

The vector space $V_{rep} = P^m/S$ carries the representation of E sought. The set $[B_\infty] = \{[W] : W \in B_\infty = B(G_\infty)\}$ constitutes a basis in V_{rep}. [Indeed, this situation is quite analogous to that prevailing in the Problem 6.8, discussed by Buchberger (1985).]

3.3. CONVERGENCE

THEOREM. *If the vector space* V_{rep} *is finite dimensional, the computation* (3.6) *will always terminate.*

PROOF. As is evident in the statement (1) of the algorithm, the computation goes on after $i =$ a certain k, only if there is a Y remaining in $B(= B_k)$, the value of which Z has not yet taken. Since the graph T(B) is always connected, as remarked at the beginning of the previous section, the number of elements in B is at least equal to the number of ancestors of Y. Clearly, then, non-termination can occur only when B_∞ is infinite. As noted after Eq. (3.7), the number of elements of $B_\infty = \dim(V_{rep})$; thus, the hypothesis that V_{rep} is finite dimensional ensures termination.

3.4. A SIMPLER REALISATION

We will prefer hereafter to use the following realisation of the representation of E described in Section 2.2, obtained through the isomorphic mapping ϕ:

$$[W] \in [B] \rightarrow W \in B,$$
$$\bar{X}_i \rightarrow \tilde{X}_i.$$

The set B_∞ then becomes the basis for the representation vector space which, from now on, V_{rep} will denote. The defining properties of the linear operators $\{\tilde{X}_i\}$ representing the generators $\{X_i\}$ can be straightforwardly read off the elements of the reduced Gröbner basis G_∞ [according to the definition of Eq. (3.3)]. The elements $|[M]|$ of E are represented by the linear operators $\tilde{p}$; p being any element of the class $|[M]|$.

4. Examples

In most of the following examples, the calculations can be done by hand.

1. This example shows how coset enumeration can be obtained when the algorithm is used with a group presentation. Let

$$A = \{C, D\} \quad \text{and} \quad LEQS = \{(C^4 - 1), (D^2 - 1), [(CD)^2 - 1]\};$$

these define the dihedral group D_4. Let us choose to construct the representation from $GV = \{H\}$ with H the subgroup $\{1, C^2, D, C^2D\}$ of D_4. According to Remark 4 at the end of Section 2, LVEQS would then be taken equal to $\{CCH - H, DH - H\}$.

Upon using Algorithm (3.6) with this data, one obtains as the loop is gone through:

with Z = H: two identities and the addition of $CDCH-H$ to the Gröbner basis G;
with $Z = CH$: two identities and the new element $DDCH-CH$ for G;
with $Z = DCH$: one identity and the new element $DC-C$ for G;

the computation then terminates with $B = \{H, CH\}$ as basis. The linear operators representing the generators C and D are such that

$$\begin{aligned} \tilde{C}(H) &= CH, & \tilde{D}(H) &= H, \\ \tilde{C}(CH) &= H, & \tilde{D}(CH) &= CH. \end{aligned}$$

The basis B corresponds to the list of left cosets of H in D_4.

2. This is an example with a ring, for which the solution appears remarkably similar to that corresponding to coset enumeration for groups. Let us consider the Kemmer (1939) ring, defined by the presentation $A = \{G_0, G_1\}$ and

$$G_\mu G_\rho G_\nu + G_\nu G_\rho G_\mu \sim g_{\mu\rho} G_\nu + G_{\nu\rho} G_\mu, \tag{4.1}$$

in which each index has for possible values (0, 1), and $g_{\mu\nu}$ is the metric tensor: $g_{00} = 1$, $g_{11} = -1$, $g_{01} = g_{10} = 0$.

Since $(G_0)^3 \sim G_0$, $H = \{G_0, G_0^2\}$ is a subring.

If one takes GV = $\{H\}$ with LVEQS = $\{G_0H-H\}$ (since $G_0H = H$) the vectors of V_{rep} will be sets, as in example 1. The loop of (3.6) will produce, apart from identities the following new elements for the Gröbner basis: with $Z = H$: $G_0^2G_1H$, G_0G_1H, $G_1{}^3H+G_1H$, $G_0G_1{}^2H+G_1{}^2H+H$ with $Z = G_1H$ and $G_1{}^2H$: none. The computation then terminates with the basis B being $\{H, G_1H, G_1{}^2H\}$, and the linear operators representing G_0 and G_1 are:

$$\begin{aligned} \tilde{G}_0(\mathrm{H}) &= \mathrm{H}, & \tilde{G}_1(\mathrm{H}) &= \mathrm{G_1H}, \\ \tilde{G}_0(\mathrm{G_1H}) &= 0, & \tilde{G}_1(\mathrm{G_1H}) &= \mathrm{G_1G_1H}, \\ \tilde{G}_0(\mathrm{G_1G_1H}) &= -\mathrm{G_1G_1H-H}, & \tilde{G}_1(\mathrm{G_1G_1H}) &= -\mathrm{G_1H}. \end{aligned}$$

3. When GV is a subset of E, the vector space V_{rep} is the union of the left ideals generated by each $V_i \in$ GV. For example, consider again the Kemmer ring, but this time, take GV = $\{V\}$ with $V = G_1^2+1$, an element of the ring. Since $G_1V \sim 0$, we take LVEQS to be $\{G_1V\}$. The loop of Algorithm (3.6) yields all non-trivial Gröbner basis elements with the first vector $Z = V$; only identities are obtained afterwards. After having dealt with V, G_0V, G_0^2V and G_1G_0V, the computation terminates; these form a basis, and the linear operators $\tilde{G}_0$ and $\tilde{G}_1$ are:

$$\begin{aligned} \tilde{G}_0(V) &= G_0V, & \tilde{G}_1(V) &= 0, \\ \tilde{G}_0(G_0V) &= G_0G_0V, & \tilde{G}_1(G_0V) &= G_1G_0V, \\ \tilde{G}_0(G_0G_0V) &= G_0V, & \tilde{G}_1(G_0G_0V) &= 0, \\ \tilde{G}_0(G_1G_0V) &= 0, & \tilde{G}_1(G_1G_0V) &= -G_0V. \end{aligned}$$

4(a). Let GV = A, i.e. $V_1 = G_0$ and $V_2 = G_1$, and LVEQS correspond to the equations (4.1), interpreted as relations of the type $MV_1+NV_2 \sim 0$ with M and $N \in K\langle A\rangle$. The nine-dimensional left regular representation of the Kemmer ring without unit element is then produced by Algorithm (3.6).

4(b). The Kemmer ring, defined with Lorentz metric for one time and three space dimensions, has a left regular representation which has 126 dimensions. This is straightforwardly constructed from GV = $\{1\}$, 1 being the ring identity, and LVEQS = ϕ.

This case cannot easily be dealt with by hand since there are then forty equations in the presentation (5.1).

5. Abelian rings can obviously be dealt with by adding to their presentation the non-trivial relations expressing the commutativity of the generators. Let us consider the following example given by Winkler *et al.* (1985) to illustrate an application of Buchberger's algorithm:

$$4x^2+xy^2-z+\tfrac{1}{4}=0, \qquad 2x+y^2z+\tfrac{1}{2}=0,$$
$$-x^2z+\tfrac{1}{2}x+y^2=0.$$

To these relations, we add

$$xy-yx=0, \qquad xz-zx=0, \qquad yz-zy=0.$$

Upon taking GV = {1}, LVEQS = ϕ, the 14-dimensional regular representation is produced. The matrix representing z has been given explicitly in Labonté (1987*b*). The 14 possible sets of values for (x, y, z) are the simultaneous eigenvalues, i.e. those corresponding to common eigenvectors, for the three commuting matrices $\tilde{x}$, $\tilde{y}$ and $\tilde{z}$. The possible values of z are thus the roots r of the equation $\det(\tilde{z}-r\tilde{1})=0$, i.e. of

$$(r^7-\tfrac{1}{2}r^6+\tfrac{1}{16}r^5+\tfrac{13}{4}r^4+\tfrac{75}{16}r^3-\tfrac{171}{8}r^2+\tfrac{133}{8}r-\tfrac{15}{4})^2=0.$$

This is the same result as obtained through the use of Buchberger's algorithm.

6. The following two examples are somewhat trivial but illustrate the fact that the construction can terminate even though E is an infinite algebra, provided the "vector constraints" expressed in LVEQS are "strong enough".

(a). Consider A = $\{X_1, X_2\}$, LEQS = ϕ so that E = K⟨A⟩, but take GV = $\{V\}$ with LVEQS = $\{(X_1V-V), (X_1X_2V+X_2V), (X_2X_2V+V)\}$. The representation constructed is then two-dimensional, with basis $\{V, X_2V\}$ and the linear operators representing the generators are:

$$\tilde{X}_1(V)=V, \qquad \tilde{X}_2(V)=X_2V,$$
$$\tilde{X}_1(X_2V)=-X_2V, \quad \tilde{X}_2(X_2V)=-V.$$

(b). The algebra E presented by A = $\{X_1, X_2\}$ and LEQS = $\{(X_1X_2+X_2)\}$ is also infinite. However, with the constraints corresponding to LVEQS = $\{(X_1V-V), (X_2X_2V+V)\}$, a finite dimensional representation, exactly the same representation as in (a) above, is actually obtained.

7. In Labonté (1987) this algorithm has been used for the construction of relativistic quantum mechanical wave equations, i.e. partial differential equations which are covariant under representations of the Poincaré group, which are intended to describe elementary particles. In the example treated in this article, A has 13 elements, LEQS has 11, GV has 3 and LVEQS 5. As mentioned in the introduction, the construction of such equations is the application for which we met the need for the algorithm described in the present work.

5. Concluding Remarks

This algorithm is easily implemented: a LISP version of it already exists [it is described in Labonté (1987, in prep. 1) and (1987, in prep. 2)].

We have no estimate on the intrinsic complexity of the problem solved or of the algorithm. There is no doubt, however, that it is a "hard" problem, since the commutative

version of it is already considered to be such [see, for example, the remark after Method 6.7 in Buchberger (1985)].

This method can be used as well for algebras without an identity. It should only be noted that, in such cases, the left regular representation would be constructed from $GV = A$ [see example 4(a), in Section 4].

Further studies should determine whether it is possible to eliminate some of the many calculations leading to identities in the construction process, as was done for the Buchberger and Knuth–Bendix algorithms (see Buchberger, 1979; Winkler & Buchberger, 1983). It should also be examined how to incorporate, in this algorithm, certain requirements, for example symmetry or hermiticity of matrices, which are not readily expressed in terms of algebraic equations. (The property of inversibility has already been dealt with in the version of the algorithm specialised for groups.) Work is now in progress on a complementary algorithm for the decomposition of the representations of algebras into their irreducible components.

References

Apel, J., Lassner, W. (1986*a*). An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras. *J. Symb. Comp.* **6,** 361–370.

Apel, J., Lassner, W. (1986*b*). Computation of reduced Gröbner bases and syzygies in enveloping fields. *Proc. SYMSAC 86 Conf.*, Waterloo, Canada.

Apel, J., Lassner, W. (1987). Computation and simplification in Lie fields. *Proc. EUROCAL 87,* to be published.

Bergman, G. M. (1978). The diamond lemma for ring theory. *Adv. in Math.* **29,** 178–218.

Buchberger, B. (1965). *An algorithm for finding a basis for a residue class ring of a zero-dimensional polynomial ideal.* (German), Ph.D. Thesis, Mathematics Institute, University of Innsbruck, Austria.

Buchberger, B. (1979). A criterion for detecting unnecessary reductions in the construction of Gröbner bases. *Proc. EUROSAM 79, LNCS 72,* pp. 3–21. New York: Springer.

Buchberger, B. (1985). Gröbner bases: an algorithmic method in polynomial ideal theory. In: (Bose, N. K., ed.). *Multidimensional Systems Theory,* pp. 184–232. Dordrecht: D. Reidel Pub. Co.

Dehn, M. (1910). Über die Topologie das dreidimensionalen Raumes. *Math. Annalen* **69,** 137–168.

Galligo, A. (1985). Some algorithmic questions on ideals of differential operators. *Proc. EUROCAL 85, LNCS 204.* New York: Springer.

Hironaka, H. (1964). Resolution of singularities of an algebraic variety over a field of characteristic zero. *Ann. Math.* **79,** 109–326.

Huet, G. (1980). Confluent reductions: abstract properties and applications to term rewriting systems. *J. ACM* **27,** 797–821.

Kandri-Rody, A., Weispfenning, V. (1986). Non-commutative Gröbner base in algebras of solvable type. *J. Symb. Comp.,* to be published.

Kemmer, N. (1939). The particle aspect of meson theory. *Proc. Roy. Soc. London* **173a,** 91–116.

Knuth, D. E., Bendix, P. B. (1970). Simple word problems in universal algebras. In (Leech, J., ed.). *Computational Problems in Abstract Algebra, Proc. Oxford Conf. 1967,* pp. 263–297. Oxford: Pergamon Press.

Labonté, G. (1987*a*). On the solution of matrix equations, example: application to invariant equations. *J. Comp. Phys.* **69,** 420–433.

Labonté, G. (1987*b*). Report on a program for solving polynomial equations in non-commuting variables. *SIGSAM Bulletin* **21,** 4–7.

Labonté, G. (1987 in prep. 1). On resolving polynomial equations in non-commuting variables: illustration with group presentations, submitted for publication.

Labonté, G. (1987 in prep. 2). A program solving polynomial equations for non-commuting as well as commuting variables, submitted for publication.

Labonté, G. (1988). On vector enumeration, submitted for publication.

Le Chenadec. (1986). *Canonical Forms in Finitely Presented Algebras.* New York: John Wiley.

Leech, J. (1970). Coset enumeration. In: (Leech, J., ed.). *Computational Problems in Abstract Algebra, Proc. Oxford Conf. 1967,* pp. 21–35. Oxford: Pergamon Press.

Métivier, Y. (1983). Systèmes de réécriture de termes et de mots, Thèse de 3ème cycle, Université de Bordeaux I.

Mora, T. (1985). Gröbner bases for non-commutative polynomial rings. *Proc. AAECC-3, Grenoble 1985, LNCS 229,* pp. 353–362. New York: Springer.

Mora, T. (1988*a*). Gröbner bases in non-commutative algebras. *Proc. Joint Conf. ISSAC-88 and AAECC-6, Roma*, to be published.

Mora, T. (1988*b*). Seven variations on standard bases, preprint.

Neubüser, J. (1983). Computing with groups and their character tables. In: (Buchberger, B. *et al.*, eds). *Computer Algebra, Symbolic and Algebraic Computation*, pp. 45–56. New York: Springer.

Todd, J. A., Coxeter, H. S. M. (1936). A practical method for enumerating cosets of a finite abstract group. *Proc. Edinb. Math. Soc.* **2**, 26–34.

Winkler, F., Buchberger, B. (1983). A criterion for eliminating unnecessary reductions in the Knuth–Bendix algorithm. *Proc. Coll. Algebra, Combinatorics and Logic in Comp. Sci. (1983)*, to appear in *Coll. Math. Soc. J. Bolyai.*

Winkler, F., Buchberger, B., Lichtenberger, F., Rolletschek, H. (1985). Algorithm 628: an algorithm for constructing canonical bases of polynomial ideals", *ACM Trans. Math. Soft.* **11**, 66–78.