Constructing bases of finitely presented Lie algebras using Gröbner bases in free algebras

W. A. de Graaf
School of Mathematical and Computational Sciences
University of St Andrews
St Andrews Scotland
wdg@dcs.st-and.ac.uk

J. Wisliceny
Schwaaner Str. 45
18273 Güstrow Germany
juergen.wisliceny@mathematik.uni-rostock.de

Abstract

We derive a sufficient condition for a generating set of an ideal in the free (non-associative, non-commutative) algebra to be a Gröbner basis. Using this we formulate an algorithm for computing a basis of a finitely presented Lie algebra. At the end of the paper we discuss the practical implementation of the algorithm.

1 Introduction

One of the natural ways of describing a Lie algebra is by generators and relations. One specifies a set X of generators and a set R consisting of certain Lie polynomials in the generators, that constitute the relations the generators must satisfy. Then the Lie algebra L described by this data is the "most general" Lie algebra generated by X and satisfying the relations in R (in the sense that any Lie algebra generated by X and satisfying the relations R is a homomorphic image of L). Lie algebras given by generators and relations occur in a number of places in mathematics. Examples are Serre's presentation of the simple Lie algebras (see [11]), Lie algebras satisfying an Engel identity (see, e.g., [16]), sandwich Lie algebras (see, e.g., [16]).

Though being a natural and compact way of presenting often high dimensional Lie algebras, the presentation by generators and relations does usually not reveal much about the Lie algebra. To investigate the Lie algebra we first need a basis of it together with a way of multiplying the basis elements. For this purpose several algorithms have been proposed, which roughly fall into two categories. There are algorithms that basically work inside the free algebra (and regard anticommutativity and the Jacobi identity as an extra set of defining relations). The algorithm proposed in [14] belongs to this category. This algorithm successively builds the multiplication table by combining the operations of introducing new basis elements when they are needed to fill the table and deleting basis elements when they are contained in some relation. In [7] and [15] algorithms are described for the more specialized task of computing nilpotent quotients. These follow roughly the same pattern (of introducing and deleting basis elements while building the multiplication table).

The second category consists of algorithms calculating inside the free Lie algebra using some kind of Hall or Lyndon-Shirshov basis. These algorithms calculate a Gröbner basis of the ideal I of the free Lie algebra $L(X)$ generated by R. Using this Gröbner basis one can enumerate basis elements modulo the ideal I. Algorithms of this kind were described in [6], [12], [13].

In the past there has been a lot of interest in Gröbner bases for ideals in non-commutative algebras. Attention has mainly focussed on non-commutative associative algebras (see, e.g., [2], [10]), but also non-associative algebras have been looked at (see [1], [8], [12], [13]). When dealing with algebras given by generators and relations, it has proved to be a fruitful idea to look at Gröbner bases. As an example we mention the proof of the Poincaré-Birkhoff-Witt theorem in [2]. In this paper we view a finitely presented Lie algebra as a quotient of the free non-associative algebra. Therefore we consider ideals and Gröbner bases in free non-commutative, non-associative algebras. In Section 3 we describe a straightforward reduction method and we show that if G is a self-reduced set then G is a Gröbner basis. In Section 4 this is used to construct an algorithm for computing a basis of a finitely presented Lie algebra that is finite-dimensional. This algorithm falls into the first category above (i.e., it works inside the free algebra). However, we focus on finding a basis of the finitely-presented Lie algebra, rather than on finding a multiplication table of it. A multiplication table of the resulting algebra can easily be calculated once a basis has been found. Finally in Section 5 we discuss the implementation of the algorithm, and we show the running times of the algorithm on some sample inputs.

2 Preliminaries

In this section we briefly describe the main objects that we will be dealing with in this paper, namely Lie algebras, the free magma, the free algebra, and the free Lie algebra. For a more elaborate treatment we refer to [3].

A Lie algebra L is a vector space over a field F, together with a bilinear operation (product) $[\ ,\ ] : L \times L \to L$ satisfying

$$[x,x] = 0 \text{ for all } x \in L \tag{1}$$

$$[x,y] + [y,x] = 0 \text{ for all } x,y \in L \tag{2}$$

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0 \text{ for all } x,y,z \in L. \tag{3}$$

Condition (3) is called the Jacobi identity; in the rest of the paper we will abbreviate the left hand side of (3) as $\mathrm{Jac}(x,y,z)$. Condition (1) implies (2); so (2) is redundant. The reason for listing both conditions is that if they are satisfied for x,y in a basis of L, then they are satisfied for all elements of L.

Let X be a set. Then $M(X)$ is the set inductively defined as follows:

1. $X \subset M(X)$,
2. if $m,n \in M(X)$, then also the pair $(m,n) \in M(X)$.

The set $M(X)$ is called the free magma on X. On $M(X)$ we define a binary operation $\cdot : M(X) \times M(X) \to M(X)$ by $m \cdot n = (m,n)$ for all $m,n \in M(X)$.

For $m \in M(X)$ we define its degree recursively: $\deg(m) = 1$ if $m \in X$ and $\deg(m) = \deg(m') + \deg(m'')$ if $m = (m', m'')$.

Let F be a field and let $A(X)$ be the vector space over F spanned by $M(X)$. If we extend the binary operation on $M(X)$ bilinearly to $A(X)$, then $A(X)$ becomes a (non-associative) algebra; it is called the free algebra over F on X. The elements of $M(X)$ are called monomials. The support of an element $f \in A(X)$ is the set of all monomials that occur in f with nonzero coefficient. Then for $f \in A(X)$ we define $\deg(f)$ to be the maximum of $\deg(m)$ where m lies in the support of f.

Let I_0 be the ideal of $A(X)$ generated by all elements

$$\begin{gathered}(m,m) \text{ for } m \in M(X),\\ (m,n) + (n,m) \text{ for } m,n \in M(X)\\ (m,(n,p)) + (n,(p,m)) + (p,(m,n)) \text{ for } m,n,p \in M(X).\end{gathered} \tag{4}$$

Set $L(X) = A(X)/I_0$. Then the product on $A(X)$ induces a product $[\ ,\ ]$ on $L(X)$. Furthermore, (1), (2) and (3) hold for all elements in a basis of $L(X)$. Hence $L(X)$ is a Lie algebra; it is called the free Lie algebra on X over F.

3 Gröbner bases in free algebras

Let X be a set. Let J be an ideal of the free algebra $A(X)$ generated by $a_i \in A(X)$ for $i \geq 1$ (so we may have an infinite generating set). We first introduce some machinery that allows us to describe elements of J. Let $\sigma = (m_1, \dots, m_k)$ be a sequence of elements of the free magma $M(X)$, and let $\delta = (d_1, \dots, d_k)$ be a sequence (of length equal to the length of σ) of letters $d_i \in \{l, r\}$. Set $\alpha = (\sigma, \delta)$, then we call α an *appliance*. The integer k is called the *length* of α.

For an appliance α we define a map $P_\alpha : M(X) \to M(X)$ in the following way. If $k = 0$, then $P_\alpha(m) = m$ for all $m \in M(X)$. On the other hand, if $k > 0$, then we set $\beta = ((m_2, \dots, m_k), (d_2, \dots, d_k))$. If $d_1 = l$, then $P_\alpha(m) = P_\beta((m_1, m))$, and $P_\alpha(m) = P_\beta((m, m_1))$ if $d_1 = r$. So the map corresponding to an appliance consists of a series of multiplications and the letter d_i determines whether we multiply from the left or the right by m_i. Finally we extend the map P_α to a map $P_\alpha : A(X) \to A(X)$ by linearity.

Example 1 Let $X = \{x, y, z\}$ and set $\sigma = (x, (y, z), z)$ and $\delta = (l, r, r)$, and $\alpha = (\sigma, \delta)$. Then $P_\alpha(m) = (((x, m), (y, z)), z)$ for $m \in M(X)$.

Now a general element f of J will be of the form

$$f = \lambda_1 P_{\alpha_1}(a_{i_1}) + \cdots + \lambda_r P_{\alpha_r}(a_{i_r}). \tag{5}$$

An element $m_1 \in M(X)$ is called a *factor* of $m_2 \in M(X)$ if there is an appliance α such that $m_2 = P_\alpha(m_1)$.

Now we describe the reduction process. For this we need a a total order $<$ on $M(X)$ that is multiplicative (i.e., $m < n$ implies $(m,p) < (n,p)$ and $(p,m) < (p,n)$ for all $p \in M(X)$). Furthermore we assume that $<$ satisfies the descending chain condition, i.e., if $m_1 \geq m_2 \geq m_3 \geq \dots$ is a descending chain of monomials then there is a $k > 0$ such that $m_k = m_j$ for $j \geq k$. Such an order can for instance be constructed by fixing it arbitrarily on X, and by postulating that $\deg(m) < \deg(n)$ implies $m < n$. Furthermore the elements of equal degree are ordered lexicographically, i.e., if $\deg(m) = \deg(n) > 1$ (so that $m = (m', m'')$ and $n = (n', n'')$) then $m < n$ if $m' < n'$ or ($m' = n'$ and $m'' < n''$).

In the sequel $<$ will denote a total order on $M(X)$ that is multiplicative and satisfies the descending chain condition. As usual, the leading monomial $\mathrm{LM}(f)$ of $f \in A(X)$ is the largest monomial in the support of f. Since $<$ is multiplicative we have that $\mathrm{LM}(P_\alpha(f)) = P_\alpha(\mathrm{LM}(f))$ for any appliance α and $f \in A(X)$.

Let $f, g \in A(X)$ then f is called *reduced* modulo g if $\mathrm{LM}(g)$ is not a factor of any monomial in the support of f. If f is not reduced modulo g, then there is a monomial m in the support of f and an appliance α such that $P_\alpha(\mathrm{LM}(g)) = m$. Let λ be the coefficient of m in f and μ the coefficient of $\mathrm{LM}(g)$ in g. Set $h = f - \frac{\lambda}{\mu} P_\alpha(g)$. We say that f reduces modulo g in one step to h. We say that f reduces to f' modulo g if there exist $f_1, \dots, f_k$ such that $f = f_1$, $f' = f_k$ and f_i reduces modulo g in one step to f_{i+1} for $1 \leq i \leq k-1$. Because $<$ satisfies the descending chain condition we have that any maximal sequence of reduction steps finishes in a finite number of steps with an element that is reduced modulo g.

Let $G \subset A(X)$. Then we say that f reduces to f' modulo G if there are elements $f_1, \dots, f_{l+1} \in A(X)$ such that $f_1 = f$, $f_{l+1} = f'$ and for $1 \leq i \leq l$ there is a $g_i \in G$ such that f_i reduces to f_{i+1} modulo g_i.

Definition 2 *A set $G \subset A(X)$ generating an ideal J is called a Gröbner basis if for all $f \in J$ there is a $g \in G$ such that $\mathrm{LM}(g)$ is a factor of $\mathrm{LM}(f)$.*

If G is a Gröbner basis for the ideal J, then all $f \in J$ reduce to 0 modulo G.

Definition 3 *A set $G = \{a_1, a_2, \dots\} \subset A(X)$ is said to be* self-reduced *if $\mathrm{LM}(a_i)$ is no factor of $\mathrm{LM}(a_j)$ for $i \neq j$.*

We remark that if G is a finite subset of $A(X)$, then by successively reducing the elements of G modulo each other we can compute a finite set G' such that G' is self-reduced and generates the same ideal as G. The rest of this section is devoted to showing that a self-reduced set is a Gröbner basis.

Lemma 4 *Let $m_1, m_2 \in M(X)$ be such that m_1 is not a factor of m_2 and m_2 is not a factor of m_1. Suppose that there are appliances α, β such that $P_\alpha(m_1) = P_\beta(m_2)$. Then m_2 is a factor of $P_\alpha(n)$ and m_1 is a factor of $P_\beta(n)$ for all $n \in M(X)$.*

Proof. First we note that the lengths of α and β are at least 1, since otherwise one of m_1, m_2 would be a factor of the other one. Let $\beta = (\sigma, \delta)$, where $\sigma = (p_1, \dots, p_k)$ and $\delta = (d_1, \dots, d_k)$. For $0 \le i \le k$ we set

$$\beta_i = ((p_1, \dots, p_i), (d_1, \dots, d_i))$$

and $n_i = P_{\beta_i}(m_2)$ (so that $n_0 = m_2$). Now m_1 is not a factor of n_0, but it is a factor of n_k. So there is an index $i > 0$ such that m_1 is not a factor of n_{i-1} but m_1 is a factor of n_i. We have that $n_i = (n_{i-1}, p_i)$ or $n_i = (p_i, n_{i-1})$. And since $n_i \ne m_1$ (otherwise m_2 would be a factor of m_1) we have that m_1 must be a factor of p_i and hence m_1 is a factor of $P_\beta(n)$ for all n in $M(X)$. The proof for P_α is similar. $\square$

Lemma 5 *Let $m \in M(X)$ and let $\alpha \ne \beta$ be appliances such that $P_\alpha(m) = P_\beta(m)$. Then m is a factor of $P_\alpha(n)$ and $P_\beta(n)$ for all $n \in M(X)$.*

Proof. Let k and l be the lengths of α and β respectively. If one of them is zero, then the other must be zero as well and $\alpha = \beta$. So k and l are both nonzero. We prove the statement by induction on $k + l$. Suppose that $\alpha = (\sigma_1, \delta_1)$ and $\beta = (\sigma_2, \delta_2)$, where $\sigma_1 = (m_1, \dots, m_k)$ and $\sigma_2 = (n_1, \dots, n_l)$. Suppose that $P_\alpha(m) = (a, b)$. Then $m_k = a$ or $m_k = b$. First suppose that $m_k = a$. If also $n_l = a$ then we can erase the last element from α and β and obtain two appliances α', β' of smaller length that also satisfy the hypothesis of the lemma. So we can conclude by induction. On the other hand, if $n_l = b$, then $a = P_{\beta'}(m)$ where β' is obtained from β by erasing n_l. Hence m is a factor of m_k and in the same way, m is a factor of n_l. As a consequence m is a factor of $P_\alpha(n)$ and of $P_\beta(n)$ for all $n \in M(X)$. The proof for the case where $m_k = b$ is completely analogous. $\square$

Now we turn to our ideal J generated by a_i for $i \ge 1$. If $m \in M(X)$ then by $J_{<m}$ we denote the subspace of J consisting of all elements of the form $\lambda_1 P_{\alpha_1}(a_{i_1}) + \dots + \lambda_r P_{\alpha_r}(a_{i_r})$ such that $\mathrm{LM}(P_{\alpha_j}(a_{i_j})) < m$ for $1 \le i \le r$.

Lemma 6 *Let b_1, b_2 be generators of J and set $m_i = \mathrm{LM}(b_i)$ for $i = 1, 2$. If $b_1 \ne b_2$ then we assume that m_1 is not a factor of m_2 and m_2 is not a factor of m_1. Let α_1, α_2 be two appliances such that $m = P_{\alpha_1}(m_1) = P_{\alpha_2}(m_2)$ and set $b = P_{\alpha_1}(b_1) - P_{\alpha_2}(b_2)$. Then $b \in J_{<m}$.*

Proof. First we deal with the case where $b_1 \ne b_2$. Then by Lemma 4 we have that m_2 is a factor of $P_{\alpha_1}(n)$ and m_1 is a factor of $P_{\alpha_2}(n)$ for all $n \in M(X)$. We have that m is a bracketed expression containing m_1 and m_2 as subexpressions. Furthermore, $P_{\alpha_1}(n)$ is obtained from m by replacing one occurrence of m_1 in m at position p_1 by n. Similarly, there is a position p_2 in m such that $P_{\alpha_2}(n)$ is obtained from m by replacing the m_2 at p_2 by n. Now we define a function $P_m : A(X) \times A(X) \to A(X)$. If $n_1, n_2 \in M(X)$, then $P_m(n_1, n_2)$ is obtained from m by replacing m_1 at position p_1 in m by n_1, and replacing the m_2 at position p_2 by n_2. Furthermore the function P_m is extended to the whole of $A(X) \times A(X)$ by bilinearity.

To ease notation a little we suppose that the coefficient of m_i in b_i is 1 (it is obvious that we can do this without loss of generality). Set $\bar{b}_i = b_i - m_i$ for $i = 1, 2$. And let $P_1, P_2 : A(X) \to A(X)$ be functions defined by $P_1(n) = P_m(n, -\bar{b}_2)$ and $P_2(n) = P_m(-\bar{b}_1, n)$. Then P_1 and P_2 are linear combinations of functions P_γ for appliances γ. Also we have that $P_{\alpha_1}(n) = P_m(n, m_2)$ and $P_{\alpha_2}(n) = P_m(m_1, n)$. So

$$\begin{aligned} P_{\alpha_1}(b_1) - P_{\alpha_2}(b_2) =& P_m(m_1, m_2) + P_m(\bar{b}_1, m_2) - \\ & P_m(m_1, m_2) - P_m(m_1, \bar{b}_2) \\ =& P_m(\bar{b}_1, m_2) - P_m(m_1, \bar{b}_2). \end{aligned}$$

And

$$\begin{aligned} P_1(b_1) - P_2(b_2) =& P_m(m_1, -\bar{b}_2) + P_m(\bar{b}_1, -\bar{b}_2) - \\ & P_m(-\bar{b}_1, m_2) - P_m(-\bar{b}_1, \bar{b}_2) \\ =& P_m(m_1, -\bar{b}_2) - P_m(-\bar{b}_1, m_2). \end{aligned}$$

Hence $P_{\alpha_1}(b_1) - P_{\alpha_2}(b_2) = P_1(b_1) - P_2(b_2)$. Furthermore, $P_i(b_i) \in J_{<m}$.

Now we consider the case where $b_1 = b_2$. If in addition $\alpha_1 = \alpha_2$ then $b = 0$ and we are done. So suppose that $\alpha_1 \ne \alpha_2$, and set $q = m_1 = m_2$. Then $P_{\alpha_1}(q) = P_{\alpha_2}(q)$. By Lemma 5 also in this case q is a factor of $P_{\alpha_1}(n)$ and of $P_{\alpha_2}(n)$ for all $n \in M(X)$. Hence we are in exactly the same situation as in the case where $b_1 \ne b_2$. So we can proceed as above. $\square$

Proposition 7 *Let $G = \{a_1, a_2, \dots\} \subset A(X)$ be a self-reduced set. Then G is a Gröbner basis.*

Proof. Let J be the ideal of $A(X)$ generated by G. Let $f \in J$ and write

$$f = \lambda_1 P_{\alpha_1}(a_{i_1}) + \dots + \lambda_r P_{\alpha_r}(a_{i_r}),$$

where $\alpha_1, \dots, \alpha_r$ are certain appliances. Set $n_j = \mathrm{LM}(P_{\alpha_j}(a_{i_j}))$. We suppose that the summands have been ordered such that the leading monomials are in increasing order, i.e.,

$$m = n_1 = \ldots = n_k > n_{k+1} \ge \dots \ge n_r.$$

If $k = 1$, then $\mathrm{LM}(f) = \mathrm{LM}(P_{\alpha_1}(a_{i_1})) = P_{\alpha_1}(\mathrm{LM}(a_{i_1}))$ and there is nothing to prove. So assume that $k > 1$. Then by Lemma 6 we have that $P_{\alpha_1}(a_{i_1}) - P_{\alpha_2}(a_{i_2}) \in J_{<m}$. Furthermore

$$f = \lambda_1(P_{\alpha_1}(a_{i_1}) - P_{\alpha_2}(a_{i_2})) + (\lambda_1 + \lambda_2) P_{\alpha_2}(a_{i_2}) + \sum_{k=3}^{r} \lambda_k P_{\alpha_k}(a_{i_k}).$$

Since the first term of this expression is in $J_{<m}$ we can write it as a linear combination of $P_{\gamma_k}(a_{i_k})$ such that

$\mathrm{LM}(P_{\gamma_k}(a_{i_k})) < m$. Hence we find a new expression for f where the term m has decreased (in the case where $k = 2$ and $\lambda_1 + \lambda_2 = 0$), or the number k has decreased. Now because $<$ satisfies the descending chain condition, we are done. $\square$

Corollary 8 *Let J be an ideal of $A(X)$ generated by the set $G = \{a_i \mid i \geq 1\}$. Suppose that G is self-reduced. Let $S \subset M(X)$ be the set of all $m \in M(X)$ such that $\mathrm{LM}(a_i)$ is not a factor of m for $i \geq 1$. Then the image of S in $A(X)/J$ forms a basis of $A(X)/J$.*

Proof. Let V be the span of S inside $A(X)$. Then $V \cap J = 0$ by Proposition 7. Also if $f \in A(X)$, then by reducing the monomials occurring in f modulo elements of G we obtain an element $v \in V$. Since in the reduction process we subtract elements of J from f, we have that $f = v + g$ for some $g \in J$. Hence $A(X) = V \oplus J$ and the proposition follows. $\square$

4 Constructing a basis of finitely presented Lie algebras

Let X be a finite set and let $R = \{r_1, \ldots, r_s\}$ be a finite subset of the free Lie algebra $L(X)$. Let I be the ideal of $L(X)$ generated by R and set $L = L(X)/I$. Then L is called a finitely presented Lie algebra. In this section we use the results of the preceding section to describe an algorithm for calculating a basis of a finitely presented Lie algebra. We note that an algorithm like this will never be able to succeed if L is not finite-dimensional. So we only require our algorithm to finish whenever L is finite-dimensional.

Let $\pi : A(X) \to L(X)$ be the projection map. For $1 \leq i \leq s$ we let $h_i \in A(X)$ be such that $\pi(h_i) = r_i$. Then we let $J \subset A(X)$ be the ideal generated by the set G consisting of the generators of I_0 (4) together with the h_i. Then $A(X)/J \cong L$. Hence we are in the situation considered in Section 3. We have an ideal J of $A(X)$ generated by an infinite number of generators, and supposing that the quotient $A(X)/J$ is finite-dimensional, we want to construct a basis of it. By Corollary 8 this is easy as soon as we have found a self-reduced generating set for J. We will show that the hypothesis that L is finite-dimensional guarantees that we can find a self-reduced generating set for J. In the sequel we suppose that the order $<$ is degree compatible, i.e., $\deg(m) < \deg(n)$ implies $m < n$ for all $m, n \in M(X)$.

For $k > 0$ we let $M_k(X)$ be the set of all $m \in M(X)$ such that $\deg(m) = k$, and we set

$$G_k = \{g \in G \mid \deg(g) \leq k\}.$$

We let $J_k \subset A(X)$ be the ideal generated by G_k. Note that G_k is a finite set. So by doing successive reductions of the elements of G_k we can calculate a self-reduced set G'_k that also generates J_k. Set

$$\mathrm{LM}(J_k) = \{\mathrm{LM}(f) \mid f \in J_k\},$$

and for $k, l > 0$, let $B_{k,l}$ be the set of all $m \in M_k(X)$ that are not contained in $\mathrm{LM}(J_l)$. It is straightforward to see that $J = \bigcup_{l>0} J_l$. Hence, since $A(X)/J$ is finite-dimensional there are $k_0, l_0 \geq 0$ such that $B_{k_0+1,l_0} = \emptyset$. Now since $J_l \subset J_{l+1}$, also $B_{k_0+1,l} = \emptyset$ for $l \geq l_0$. In the sequel we let l be the smallest number such that $l \geq l_0$, $l \geq 2k_0 + 1$ and such that $h_i \in G_l$ for $1 \leq i \leq s$. We set

$$B = \bigcup_{1 \leq i \leq k_0} B_{i,l}.$$

In the sequel we prove that $J_l = J$, thereby proving that J is generated by G_l and since G_l is finite this allows us to calculate a self-reduced generating set for J.

Lemma 9 *Let $m \in M_{d+1}(X)$, then modulo elements of J_{d+1}, m can be written as a linear combination of elements of the form (n, x) where $n \in M_d(X)$ and $x \in X$.*

Proof. This is trivial if $\deg(m) = 1$. So suppose that $\deg(m) \geq 2$ and $m = (m', m'')$. We prove the lemma by induction on $\deg(m'')$. If $m'' \in X$ then there is nothing to prove. So suppose that $m'' = (a, y)$ for $a, y \in M(X)$. Furthermore, by induction (note that $J_k \subset J_{d+1}$ whenever $k \leq d+1$) we may assume that $y \in X$. Then since J_{d+1} contains all relations of the form $(p, q) + (q, p)$ such that $\deg(p) + \deg(q) \leq d+1$ and all Jacobi identities of degree $\leq d+1$ we can write modulo J_{d+1},

$$(m', (a, y)) = ((y, m'), a) + ((m', a), y).$$

The second summand is of the required form. Also, since $\deg(a) < \deg(m'')$, by induction the first summand can be written as a linear combination of elements of the required form. $\square$

Lemma 10 *Let $m \in M(X)$; then modulo J_l, m can be written as a unique linear combination of elements from B.*

Proof. We note that uniqueness follows from the fact that B is linearly independent modulo J_l. We show by induction that every $m \in M(X)$ can modulo J_l be written as a linear combination of elements of B, assuming that the result holds for all monomials $n \in M(X)$ such that $n < m$. First suppose that $\deg(m) \leq k_0 + 1$. Then $m \in B$ or there is a $g \in J_l$ such that $\mathrm{LM}(g)$ is a factor of m. In the first case we are done. In the second case m reduces modulo J_l to a linear combination of monomials $n_i \in M(X)$ such that $n_i < m$. Since $<$ is degree compatible, also $\deg(n_i) \leq k_0 + 1$ and we finish by induction.

Now suppose that $k_0 + 1 < \deg(m) \leq 2k_0 + 1$. Then by lemma 9, m can modulo J_l be rewritten as a linear combination of elements of the form (n, x) where $\deg(n) = \deg(m) - 1$ and $x \in X$. (Note that $l \geq 2k_0 + 1$). For all such n we have that $\deg(n) < \deg(m)$ and hence, by induction, n can modulo J_l be rewritten as a linear combination of elements of B. But this means that m can modulo J_l be rewritten as a linear combination of elements of the form (b, x) for $b \in B$ and $x \in X$. Now because $\deg(b, x) \leq k_0 + 1$, as seen above, we can rewrite every (b, x) as a linear combination of elements of B.

Finally, suppose that $\deg(m) > 2k_0 + 1$. Then $m = (m', m'')$ and by induction, m' and m'' can both modulo J_l be rewritten as a linear combination of elements of B. Hence m can be rewritten as a linear combination of elements of the form (a, b) for $a, b \in B$. But $\deg(a, b) \leq 2k_0$ so, as seen above, every such element can modulo J_l be rewritten as a linear combination of elements of B and hence the same holds for m.

$\square$

Lemma 11 *Let K be an ideal of $A(X)$ containing all $(m_1, m_2) + (m_2, m_1)$ for $m_1, m_2 \in M(X)$. Suppose that* $\mathrm{Jac}(x, m, n) = 0 \pmod K$ *for all $m, n \in M(X)$, and all $x \in X$. Then* $\mathrm{Jac}(p, m, n) = 0 \pmod K$ *for all $m, n, p \in M(X)$.*

Proof. The proof is by induction on $\deg(p)$. If $\deg(p) = 1$, then there is nothing to prove. If $\deg(p) > 1$, then $p = (a, b)$. Using induction and relations $(m_1, m_2) = -(m_2, m_1) \pmod K$ we calculate modulo K,

$$\begin{aligned}((a,b),(m,n)) =& -((b,(m,n)),a) - (((m,n),a),b)\\ =&((m,(n,b)),a) + ((n,(b,m)),a) +\\ &(((n,a),m),b) + (((a,m),n),b)\\ =& -(((n,b),a),m) - ((a,m),(n,b)) -\\ &(((b,m),a),n) - ((a,n),(b,m))\\ &-((m,b),(n,a)) - ((b,(n,a)),m) -\\ &((n,b),(a,m)) - ((b,(a,m)),n)\\ =& -(((n,b),a) + (b,(n,a)),m) -\\ &(((b,m),a) + (b,(a,m)),n)\\ =&((n,(a,b)),m) - ((m,(a,b)),n).\end{aligned}$$

Hence $\mathrm{Jac}(p, m, n) = 0 \pmod K$. □

Now let $p, q \in M(X)$. Then by Lemma 10, $(p, q) + (q, p)$ can modulo J_l be written as a linear combination of elements $(p', q') + (q', p')$ where $p', q' \in B$. But since $l \geq 2k_0 + 1$ all these elements lie in J_l. Also by Lemma 10, modulo J_l all elements $\mathrm{Jac}(x, m, n)$ for $x \in X$ and $m, n \in M(X)$ can be written as linear combinations of elements of the form $\mathrm{Jac}(x, m', n')$, where $m', n' \in B$. But since $l \geq 2k_0 + 1$ all those elements are in J_l. So J_l satisfies the hypothesis of Lemma 11. It follows that J_l contains all elements $\mathrm{Jac}(p, m, n)$ for all $p, m, n \in M(X)$. Also J_l contains (a pre-image of) R. The conclusion is that all generators of J lie in J_l, i.e., $J_l = J$. So by Corollary 8, B is a basis of $A(X)/J$.

We summarize our findings in the following algorithm.

Algorithm `FpLieAlgebra`
Input: a finite set X and a finite subset $R \subset L(X)$.
Output: a basis of $L(X)/I$ where I is the ideal generated by R.

Step 1 Let J be the ideal of $A(X)$ generated by a pre-image of R together with the elements (4). Set $l := 1$ and repeat the following:

- Step 1a Calculate a self-reduced generating set G'_l of J_l.
- Step 1b For $1 \leq k \leq l$ calculate the set $B_{k,l}$ of monomials $m \in M(X)$ of degree k such that $\mathrm{LM}(b)$ is not a factor of m for all $b \in G'_l$.
- Step 1c If there is a $k \in \{1, \ldots, l-1\}$ such that $B_{k+1,l} = \emptyset$ then go to Step 2. Otherwise increase l by 1 and return to Step 1a.

Step 2 Increase l such that J_l contains a pre-image of R in $A(X)$. Set $t = \max(2k + 1, l)$.

Step 3 Calculate a self-reduced generating set G'_t of J_t. Calculate the set B of all monomials m in $M(X)$ of degree $\leq k$ such that $\mathrm{LM}(b)$ is not a factor of m for $b \in G'_t$. Return B.

Remark. This algorithm can easily be extended so as to produce a multiplication table of $L(X)/I$. Indeed, any product of elements of B can be reduced (uniquely) modulo the elements of G'_t to a linear combination of the elements of B.

Example 12 Let $X = \{x, y\}$, $R = \{[x, [x, y]] - [x, y], [y, [y, [x, y]]]\}$ (as usual we use the brackets [,] to denote the product in $L(X)$). While performing the algorithm it is much more convenient to use the anticommutativity relations $(m, m) = 0$ and $(m, n) + (n, m) = 0$ directly to reduce expressions to a convenient form, than to put them into the ideal first. So in the ideal we only consider (pre-images) of the elements of R together with the Jacobi identities.

By anticommutativity we immediately have that $\mathrm{Jac}(m, n, p) = 0$ if any two of m, n, p are equal. It follows that the Jacobi identity of lowest degree is $\mathrm{Jac}(x, y, (x, y))$. So we consider the set G_4 consisting of this Jacobi identity together with the elements of R. We have

$$\mathrm{Jac}(x, y, (x, y)) = (x, (y, (x, y))) + (y, ((x, y), x)) + ((x, y), (x, y)).$$

The last summand is zero by anticommutativity. The second summand is equal to $-(y, (x, (x, y)))$ which is equal to $-(y, (x, y))$ by the first relation in R. So the self-reduced set G'_4 generating the same ideal as G_4 is

$$\begin{aligned}G'_4 = \{&(x, (x, y)) - (x, y), (y, (y, (x, y))),\\ &(x, (y, (x, y))) - (y, (x, y))\}.\end{aligned}$$

Now we enumerate the basis elements of $A(X)$ upto degree 4 modulo the elements in G'_4. By anticommutativity we see that these are $x, y, (x, y), (y, (x, y))$ (an element of degree 4 is the product of an element of degree 1 and an element of degree 3, but all those elements are leading monomials of elements of G'_4). Therefore $B_{4,4} = \emptyset$. So we set $t = 7$ and reduce all elements of G_7. We only have to consider Jacobi identities of those monomials that do not already reduce modulo G'_4. The first of these is

$$\begin{aligned}\mathrm{Jac}(x, y, (y, (x, y))) = (x, (y, (y, (x, y)))) + (y, ((y, (x, y)), x))\\ + ((y, (x, y)), (x, y)).\end{aligned}$$

The first two summands reduce to zero modulo G'_4. Hence only the last summand remains. Using this, the Jacobi identities $\mathrm{Jac}(x, (x, y), (y, (x, y)))$ and $\mathrm{Jac}(y, (x, y), (y, (x, y)))$ reduce to zero. So G'_7 consists of the elements of G'_4 together with $((y, (x, y)), (x, y))$. Hence $B = \{x, y, (x, y), (y, (x, y))\}$ is a basis of $L(X)/I$ where I is the ideal of $L(X)$ generated by R.

Remark. The algorithm described here can be adapted to work for other types of algebras like Lie super algebras, Jordan algebras and associative algebras. However, the axiom of associativity is relatively simple and allows one to compute conveniently in the free associative algebra. For this case special techniques are available (see, e.g., [9], [13]) that are more elegant than an approach via the free algebra.

Remark. In some cases Lie algebras are given by generators together with a number of Lie polynomials containing indeterminates. All elements of the Lie algebra determined by this are required to satisfy these Lie polynomials. An example is the so-called $(p-1)$-Engel identity, which reads $xy^{p-1} = 0$ for all x, y (where we define $xy = [x, y]$ and $xy^{k+1} = [xy^k, y]$) (see, e.g., [16]). This gives rise to an infinite number of relations.

These polynomials might not be linear in the indeterminates (in which case it is not sufficient to check them on a basis of the Lie algebra). However, by a technique similar to polarization it is possible to derive an equivalent polynomial (in more variables) which is linear in all its variables. We refer to [15] for the details. If the dimension of the quotient is finite, then this situation can also be handled by our algorithm. (The relations coming from the polynomials with indeterminates are processed in similar fashion as the Jacobi identities.)

Remark. In [7] and [15] the authors describe algorithms to calculate nilpotent quotients of algebras given by generators X and homogeneous relations R. Let L be the quotient algebra $A(X)/J$ where J is generated by R together with the defining relations of the algebra (Jacobi identities in the case of Lie algebras, associativity in the case of associative algebras and so on). Then the algorithm successively calculates bases of the quotients L/L^c for $c > 1$. An algorithm for this task can also be formulated along the lines of this section. We just have to add to the ideal J all relations of the form $m = 0$ where $m \in M(X)$ is such that $\deg(m) = c$.

5 Practical experiences

We have implemented the method inside the computer algebra system GAP4 ([5]). The routine is currently available in the last beta version of that system (GAP4b5). It produces a Lie algebra of the format that is used by GAP4, so that a direct interface is provided to the functionality that is present in GAP4 for dealing with the structure of Lie algebras.

As in Example 12 we use the anticommutativity to reduce the monomials in the free algebra to a convenient form, rather than to put these relations in the ideal. By doing this consistently throughout the program we are assured of reaching the same result as when we put the relations into the ideal. Furthermore, to save memory during the computation we store in the multiplication table only products of the form $[m, n]$ where $m > n$. Also, using Lemma 9 it is straightforward to see that any monomial in the Lie algebra can be written as a linear combination of left normed ones. So in the internals of the program we avoid tedious bracketings by representing monomials as lists (and assume left normed bracketing).

In Table 1 we list the experimental data [1] concerning computations of a basis of the simple Lie algebra of type D_n over the rational numbers, given by a Serre presentation.

We see that the program can easily handle Lie algebras of dimension into the hundreds. Furthermore, a little calculation shows that the running times are roughly proportional to n^5.

As a second set of examples we consider Lie algebras L_n over $\mathbb{Q}$ generated by a set X of size n subject to the relations $[x, [x, m]] = 0$ for $x \in X$ and $m \in L_n$. Such a Lie algebra is called a (free) sandwich algebra (see [4], [16]). This is an example of a Lie algebra given by generators subject to a number of Lie polynomials containing indeterminates.

[1] The calculations were performed on a PentiumII 266.

	dimension	running time
D_9	153	62
D_{11}	231	175
D_{13}	325	429
D_{15}	435	845
D_{17}	561	1631

Table 1: Running times (in seconds) for the calculation of a basis of D_n over $\mathbb{Q}$ for $n = 9, 11, 13, 15, 17$

Furthermore, these Lie polynomials are linear in m, so our program can deal with them. In Table 2 we show the running times of the program when computing a basis of L_n for $n = 3, 4, 5$. It is seen that the dimension of L_n increases rapidly with n. The Lie algebras L_n are nilpotent (see, e.g., [13]). The nilpotency class of a nilpotent Lie algebra is defined as the number $c > 0$ such that $L^c \neq 0$ but $L^{c+1} = 0$. Now from a basis of L_n we can read off the nilpotency class of the Lie algebra (it is the maximum degree of a monomial occurring in this basis).

	dimension	running time	nilpotency class
L_3	8	0.2	3
L_4	28	1	5
L_5	537	7560	15

Table 2: Running times (in seconds) for the calculation of a basis of L_n over $\mathbb{Q}$ for $n = 4, 5, 6$

References

[1] Bahturin, Y. A., Mikhalev, A. A., Petrogradsky, V. M., and Zaicev, M. V. *Infinite-dimensional Lie superalgebras.* Walter de Gruyter & Co., Berlin, 1992.

[2] Bergman, G. M. The diamond lemma for ring theory. *Adv. in Math. 29*, 2 (1978), 178–218.

[3] Bourbaki, N. *Groupes et Algèbres de Lie, Chapitre II.* Hermann, Paris, 1972.

[4] Cohen, A. M., Steinbach, A., Ushirobira, R., and Wales, D. Lie algebras generated by extremal elements. preliminary version, December 1998.

[5] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.* Aachen, St Andrews, 1998. (`http://www-gap.dcs.st-and.ac.uk/~gap`).

[6] Gerdt, V. P., and Kornyak, V. V. Construction of finitely presented Lie algebras and superalgebras. *Journal of Symbolic Computation 21*, 3 (1996), 337–349.

[7] Havas, G., Newman, M. F., and Vaughan-Lee, M. R. A nilpotent quotient algorithm for graded Lie rings. *Journal of Symbolic Computation 9*, 5-6 (1990), 653–664. Computational group theory, Part 1.

[8] Lalonde, P., and Ram, A. Standard Lyndon bases of Lie algebras and enveloping algebras. *Trans. Amer. Math. Soc. 347*, 5 (1995), 1821–1830.

[9] Linton, S. A. On vector enumeration. *Linear Algebra and its Applications 192* (1993), 235–248. Computational linear algebra in algebraic and related problems (Essen, 1992).

[10] Mora, T. An introduction to commutative and non-commutative Gröbner bases. *Theoretical Computer Science 134*, 1 (1994), 131–173. Second International Colloquium on Words, Languages and Combinatorics (Kyoto, 1992).

[11] Serre, J.-P. *Algèbres de Lie semi-simples complexes.* W. A. Benjamin, inc., New York-Amsterdam, 1966.

[12] Shirshov, A. I. Some algorithmic problems for Lie algebras. *Sib. Mat. Zh. 3* (1962), 292–296. (Russian).

[13] Ufnarovskij, V. A. *Combinatorial and Asymptotic Methods in Algebra*, vol. 57 of *Encyclopedia of Mathematical Sciences*. Springer Verlag, Berlin, Heidelberg, New York, 1995, ch. I, pp. 1–196.

[14] van Leeuwen, M. A. A., and Roelofs, M. Termination for a class of algorithms for constructing algebras given by generators and relations. *Journal of Pure and Applied Algebra 117/118* (1997), 431–445. Algorithms for algebra (Eindhoven, 1996).

[15] Vaughan-Lee, M. R. An algorithm for computing graded algebras. *Journal of Symbolic Computation 16*, 4 (1993), 345–354.

[16] Vaughan-Lee, M. R. On Zel'manov's solution of the restricted Burnside problem. *J. Group Theory 1*, 1 (1998), 65–94.