Hall and Gröbner bases and rewriting in free Lie algebras (extended abstract)

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

1 Introduction

Lie algebras given by generators and relations occur in my contexts. Some examples are Kac-Moody algebras ([2]), Engel and sandwich algebras ([7]) and Serre's presentation of the simple Lie algebras ([4]).

In this abstract we sketch methods for rewriting elements in a Lie algebra given by generators and relations. Such an algebra is a quotient of a free algebra A by an ideal I generated by the relations. One of the main problems is computing the product of two elements in the factor A/I. This problem is solved once we have a method for rewriting elements in A modulo I.

This document is organized as follows. In Section 2 a class of bases of the free Lie algebra, called Hall sets, is described and we indicate how to multiply two basis elements. In Section 3 we consider the problem of rewriting in the free Lie algebra. We show that we can do this if we can decide whether a given basis element is a factor of another basis element. Then in Section 4 we describe two particular Hall sets for which we can decide this. The first of these is known as the set of Lyndon-Shirshov words. The second is to the best of our knowledge not described elsewhere. Then in Section 5 we sketch some Gröbner bases theory for the free Lie algebra, and we state a theorem by A. I. Shirshov giving a sufficient condition for a set to be a Gröbner basis. Finally in Section 6 we use this theorem to give a short proof of a (rather classical) theorem in the theory of Lie algebras.

2 Free Lie algebras and Hall sets

Let X be a set. The *free magma* on X is inductively defined as follows. First $X \subset M(X)$, and if $m, n \in M(X)$ then also $(m, n) \in M(X)$. The degree of an element of $M(X)$ is defined inductively by $\deg(m) = 1$ if $m \in X$ and $\deg((m, n)) = \deg(m) + \deg(n)$. The free magma $M(X)$ is endowed with a binary operation $\cdot$ defined by $m \cdot n = (m, n)$.

Let F be a field and let $A(X)$ be the vector space spanned by $M(X)$. The binary operation $\cdot$ extends bilinearly to $A(X)$ making $A(X)$ into an algebra, called the free (non-associative) algebra on X.

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

$$\begin{gathered}(m,m) \text{ for } m \in M(X),\\ (m,n)+(n,m) \text{ for } m,n \in M(X)\\ (m,(n,p))+(n,(p,m))+(p,(m,n)) \text{ for } m,n,p \in M(X).\end{gathered} \tag{1}$$

Set $L(X) = A(X)/I_0$. Then the multiplication of $A(X)$ induces a multiplication on $L(X)$. It is straightforward to see that the product in $L(X)$ is anticommutative (i.e., $xy = -yx$) and satisfies the Jacobi identity (i.e., $x(yz) + y(zx) + z(xy) = 0$ for $x, y, z \in L(X)$). Hence $L(X)$ is a Lie algebra; it is called the free Lie algebra on X.

If we want to calculate in $L(X)$ then we need a basis of this algebra (i.e., a set of coset representatives of $A(X)$ modulo the ideal I_0) and a way of rewriting a product of basis elements modulo I_0 as a linear combination of basis elements. A solution to this problem is formed by the so-called Hall sets.

Definition 1 *We say that a total order $\leq_H$ of $M(X)$ is a* Hall order *if for $m, n \in M(X)$ we have $(m, n) <_H n$.*

Definition 2 *Let $\leq$ be a Hall order on $M(X)$. A subset $H \subset M(X)$ is called a* Hall set *if $X \subset H$ and for $h', h'' \in H$ such that $h' <_H h''$ and either $h' \in X$ or $h' = (a, b)$ with $b \geq_H h''$, we have $(h', h'') \in H$.*

We note that a Hall order defines a unique Hall set. Using the conditions of Definition 2 we can decide whether a given element of $M(X)$ lies in a given Hall set. We now state some important results on Hall sets. The proofs of these can be found in e.g., [3].

Theorem 3 *Let I_0 be the ideal of $A(X)$ generated by the elements (1). Let $H \subset M(X)$ be a Hall set and let V be the subspace of $A(X)$ spanned by H. Then $A(X) = V \oplus I_0$.*

Let H, V be as in the theorem. We define a multiplication $*$ on V as follows. Let $u, v \in V$, then there are unique elements $w \in V$ and $a \in I_0$ such that $u \cdot v = w + a$. We set $u * v = w$. It is immediate that V together with the multiplication $*$ is isomorphic to the free Lie algebra $L(X)$. Now let $m \in M(X)$ then by using the Jacobi identity and anticommutativity we can rewrite m as a linear combination of elements of H modulo I_0. We refer to [3] for the details. The conclusion is that the multiplication in $L(X)$ is algorithmically tractable.

By X^* we denote the free monoid on X, i.e., the set of all (associative) words in the elements of X, including the empty word. We define a map $\varphi : M(X) \to X^*$ by $\varphi(m) = m$ if $\deg(m) = 1$ and if $m = (m', m'')$ then $\varphi(m) = \varphi(m')\varphi(m'')$. The word $\varphi(m)$ is called the *foliage* of $m \in M(X)$ (cf. [3]). The following is [3][Corollary 4.5].

Proposition 4 *The function φ is injective, i.e., every element of H corresponds to a unique word in X^*.*

Example 5 Let $X = \{x, y\}$. Let $<_{\text{lex}}$ denote the lexicographical order on X^*. Let $\leq_H$ be defined as follows. If $\deg(m) < \deg(n)$ then $m >_H n$. Furthermore, if $\deg(m) = \deg(n)$ then $m >_H n$ if $\varphi(m) >_{\text{lex}} \varphi(n)$. Finally extend $\leq_H$ to a total order on $M(X)$. It is immediate that $\leq_H$ is a Hall order. Let H be the Hall set corresponding to $\leq_H$. Then by Proposition 4 we see that for elements of H the order $\leq_H$ is determined by the lexicographic order of their foliages. So using this order we can determine whether any given $m \in M(X)$ lies in H. For instance $(x,(x,y)) \notin H$ because $x >_H (x,y)$, but $((x,y),x)$ is an element of H. Since we can decide whether elements of $M(X)$ are in H we can rewrite any element of $M(X)$ as a linear combination of $h \in H$ modulo the ideal I_0. Let $m = (m', m'')$ where $m' = (((x,y),y),(x,y))$ and $m'' = x$. Then both $m', m'' \in H$ and $m' <_H m''$. But $m \notin H$ since $(x,y) <_H x$. Now by the Jacobi identity we see that

$$((((x,y),y),(x,y)),x)) = -(((xy),x),((x,y),y)) - ((x,((xy),y)),(x,y)).$$

By some applications of anticommutativity this is seen to be equal to $-(((xy),x),((x,y),y)) + ((((x,y),y),x),(x,y))$.

3 Rewriting in free Lie algebras

Let X be a set and $L(X)$ the free Lie algebra on X (over a field F). In this section we consider the problem of rewriting an element of $L(X)$ modulo a set $G \subset L(X)$. Throughout H will be a fixed Hall set relative to a Hall order $\leq_H$. Furthermore, we identify $L(X)$ with the span of H in $A(X)$. The product of two elements u, v in this span is denoted by $u * v$.

Let $\leq$ be a total order on H (not to be confused with the Hall order $\leq_H$). Let $f \in L(X)$, then the leading monomial $\mathrm{LM}(f)$ of f will be the biggest element of H occurring in f (with respect to the order $\leq$). The order $\leq$ is called a *reduction order* if it is multiplicative (i.e., if $h_1 < h_2$, then $\mathrm{LM}(h_1 * g) < \mathrm{LM}(h_2 * g)$ and $\mathrm{LM}(g * h_1) < \mathrm{LM}(g * h_2)$ for all $g \in H$) and it satisfies the descending chain condition (i.e., if $h_1 \geq h_2 \geq h_3 \geq \cdots$ is a descending chain of elements of H then there is a $k > 0$ such that $h_k = h_j$ for all $j \geq k$). Throughout we suppose that $\leq$ is a reduction order.

Let $\sigma = (h_1, \ldots, h_k)$ be a sequence of elements of H, and let $\delta = (d_1, \ldots, d_k)$ 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 linear map $P_\alpha : L(X) \to L(X)$. Since P_α is linear we only need to define it for elements of H. If $k = 0$, then $P_\alpha(h) = h$ for all $h \in H$. And if $k > 0$, then we set $\beta = ((h_2, \ldots, h_k), (d_2, \ldots, d_k))$. If $d_1 = l$, then $P_\alpha(h) = P_\beta(h_1 * h)$, and $P_\alpha(h) = P_\beta(h * h_1)$ 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 h_i.

An element $h_1 \in H$ is called a *factor* of $h_2 \in H$ if there is an appliance α such that $h_2 = \mathrm{LM}(P_\alpha(h_1))$. Now let $f, g \in L(X)$ and suppose that $\mathrm{LM}(g)$ is a factor of $\mathrm{LM}(h)$. Suppose for convenience that the coefficients of $\mathrm{LM}(f), \mathrm{LM}(g)$ in f, g respectively are 1. Let α be an appliance such that $\mathrm{LM}(P_\alpha(\mathrm{LM}(g))) = \mathrm{LM}(f)$ and set $h = f - P_\alpha(g)$. Then we say that f reduces to h modulo g. More generally, if $G \subset L(X)$, then we say that f reduces to f' modulo G if there is a sequence $f = f_1, \ldots, f_k = f'$ such that for $1 \leq i \leq k-1$ there is a $g \in G$ such that f_i reduces to f_{i+1} modulo g. Since the order $<$ is multiplicative and satisfies the descending chain condition, we have that any maximal sequence of reduction steps must finish with an element that cannot be reduced further.

The main problem with the reduction algorithm is how to decide whether a given $h_1 \in H$ is a factor of a $h_2 \in H$. Indeed, from Example 5 we see that $(((x,y),y),(x,y))$ is a factor of $((((x,y),y),x),(x,y))$, but this is not apparent from the structure of the elements. In the next section we describe two Hall sets for which we can decide this.

4 Two examples of Hall orders

Example 6 (Lexicographical order) Let $X = \{x_1, \dots, x_r\}$ be a set. We consider the lexicographical order $<_{\text{lex}}$ on X^*. For two words $w_1, w_2 \in X^*$ we have $w_1 <_{\text{lex}} w_2$ if and only if either $w_2 = w_1 u$ for some nonempty word $u \in X^*$ (i.e., w_1 is a prefix of w_2) or $w_1 = u x_i v_1$ and $w_2 = u x_j v_2$ where $u, v_1, v_2 \in X^*$ and $i < j$ (i.e., if on the left-most position where w_1 and w_2 differ, the entry in w_1 is the smaller one).

Now a non-empty word $w \in X^*$ is called a *Lyndon-Shirshov* word if for all factorizations $w = uv$ where u, v are not empty we have $w <_{\text{lex}} v$. Let w be a Lyndon-Shirshov word and write $w = uv$ where v is the smallest non-empty proper right factor of w; then uv is called the standard factorization of w. We define a map b that maps a Lyndon-Shirshov word into the free magma $M(X)$. For $x \in X$, $b(x) = x$ and for $w \in X^* \setminus X$ we set $b(w) = (b(u), b(v))$ where $w = uv$ is the standard factorization of w. The following is [3][Theorem 5.1].

Theorem 7 *The set $\{b(w) \mid w$ is a Lyndon-Shirshov word$\}$ is a Hall set in $M(X)$.*

Example 8 (Reverse lexicographical order) Let X be as in Example 6. Here we consider the reverse-lexicographical order $<_{\text{Rlex}}$, defined as follows. Let $w_1, w_2 \in X^*$ then $w_1 <_{\text{Rlex}} w_2$ if and only if $w_1 = u w_2$ (i.e., w_2 is a proper right factor of w_1), or $w_1 = v_1 x_i u$ and $w_2 = v_2 x_j u$ where $v_1, v_2, u \in X^*$ and $x_i, x_j \in X$ are such that $i < j$. We call $<_{\text{Rlex}}$ the reverse lexicographical order. We call a word $w \in X^*$ an *Rlex-word* if for each factorization $w = uv$ where u, v are non-empty we have $w >_{\text{Rlex}} u$. The standard factorization of an Rlex-word $w \in X^*$ is $w = uv$ where u is the biggest proper left factor of x (in the order $<_{\text{Rlex}}$). The bracketing of an Rlex-word is somewhat complicated. For $x \in X$ we set $b(x) = x$. For a $w \in X^* \setminus X$ with standard factorization $w = uv$ we set $b(w) = c(b(u), b(v))$. Here $c(b(u), b(u)) = (b(u), b(v))$ if $u \in X$ or $b(u) = (h', h'')$ where $\varphi(h'') \geq_{\text{Rlex}} v$. Otherwise set $u' = \varphi(h')$ and $u'' = \varphi(h'')$ and $c(b(u), b(v)) = c(b(u'), b(u''v))$. It is not difficult to prove that $u''v$ is also an Rlex-word. So by induction on the degree of $b(u)$ it is clear that the function c is well-defined.

Theorem 9 *The set $\{b(w) \mid w$ is an Rlex-word$\}$ is a Hall set in $M(X)$.*

Now let H be the Hall set of Example 6 or the one of Example 8. We define a reduction order $<$. In both cases $\deg(h_1) < \deg(h_2)$ implies $h_1 < h_2$. So we only need to define the order in the case where $\deg(h_1) = \deg(h_2)$. If H is the Hall set of Example 6, then $h_1 < h_2$ if $\varphi(h_1) >_{\text{lex}} \varphi(h_2)$. Furthermore, if H is the Hall set of Example 6, then $h_1 < h_2$ if $\varphi(h_1) <_{\text{Rlex}} \varphi(h_2)$.

Theorem 10 *Let H be the Hall set of Example 6 or the one of Example 8. Let $h_1, h_2 \in H$. Then h_1 is a factor of h_2 if and only if $\varphi(h_1)$ is a subword of $\varphi(h_2)$.*

Proof.(sketch) In both cases we use a map $p : L(X) \to F\langle X\rangle$ (where $F\langle X\rangle$ is the associative algebra spanned by X^*), defined by $p(x) = x$ for $x \in X$, and $p(h, g) = p(h)p(g) - p(g)p(h)$. One then proves that the biggest word occurring in $p(h * g)$ is $\varphi((h, g))$ for $h <_H g \in H$. $\square$

5 Gröbner bases in free Lie algebras

Let H be a Hall set and $\leq$ a reduction order. Let $G \subset L(X)$ and let $I \subset L(X)$ be the ideal generated by G. Let $N(I)$ be the set of all $h \in H$ such that $\mathrm{LM}(f)$ is not a factor of h for all $f \in I$. The elements of $N(I)$ are said to be *normal* with respect to I. Let $C(I)$ be the span of $N(I)$ inside $L(X)$. Then $L(X) = C(I) \oplus I$. In $C(I)$ we define a multiplication $\circledast$ as follows. Let $a, b \in C(I)$, then there are unique $c \in C(I)$ and $g \in I$ such that $a * b = c + g$ (where $*$ is the multiplication of $L(X)$, defined in Section 2). We set $a \circledast b = c$. It is immediate that the algebra $C(I)$ with $\circledast$ is isomorphic to $L(X)/I$. It follows that we can calculate in the algebra $L(X)/I$ as soon as we have a method for rewriting any element of $L(X)$ modulo I to a unique element of $C(I)$. For this we use reduction modulo the set G. However, it is by no means guaranteed that reduction modulo G of an element $a \in L(X)$ always gives a unique result lying in $C(I)$. For this we need G to be a Gröbner basis of I.

Definition 11 *Let $G \subset L(X)$ be a set generating an ideal I of $L(X)$. Then G is called a* Gröbner basis *of I if for all $f \in I$ there is a $g \in G$ such that* $\mathrm{LM}(g)$ *is a factor of* $\mathrm{LM}(f)$.

Now if G is a Gröbner basis of I, then any maximal sequence of reduction steps of $a \in L(X)$ will end with a unique element of $C(I)$. In the remainder of this section we describe a theorem by A. I. Shirshov ([5]) giving a sufficient condition for a set G to be a Gröbner basis (see also [6]).

Let H be the Hall set of Example 6 or the one of Example 8. Let the reduction order $<$ be as in Section 4. A word of the form $\varphi(h)$ for $h \in H$ is called a *Hall word.* We skip the proof of the next proposition. In the case where H is the Hall set of Example 6 it can be found in [5].

Proposition 12 *Let uv and vw be Hall words, where u, v, w are non-empty. Then uvw is a Hall word.*

Now let $G \subset L(X)$ and suppose that the coefficient of $\mathrm{LM}(g)$ in g is 1 for all $g \in G$. Let $g_1, g_2 \in G$ be such that $\varphi(\mathrm{LM}(g_1)) = uv$ and $\varphi(\mathrm{LM}(g_2)) = vw$ where u, v, w are non-empty words. Then by Proposition 12, uvw is a Hall word. Let $h \in H$ be such that $\varphi(h) = uvw$. Then by Theorem 10 both $\mathrm{LM}(g_1)$ and $\mathrm{LM}(g_2)$ are factors of h. Let α_1, α_2 be appliances such that $\mathrm{LM}(P_{\alpha_i}(\mathrm{LM}(g_i))) = h$ for $i = 1, 2$. Set $q = P_{\alpha_1}(g_1) - P_{\alpha_2}(g_2)$. Then q is called a *composition* of g_1 and g_2.

Theorem 13 (Shirshov) *Let $G \subset L(X)$ be such that* $\mathrm{LM}(g_1)$ *is not a factor of* $\mathrm{LM}(g_2)$ *for $g_1 \neq g_2 \in G$. Suppose further that the coefficient of* $\mathrm{LM}(g)$ *in g is* 1 *for all $g \in G$. If every composition of any two elements of G reduces to zero modulo G, then G is a Gröbner basis.*

Remark. This theorem was proved by A. Shirshov in 1962 ([5]), i.e., well before the invention of Gröbner bases for polynomial rings. Therefore it would be more appropriate to call the basis a Shirshov basis instead of Gröbner basis. However, since it is the exact analogue of Gröbner bases in associative algebras we have opted for the second name.

So we have two Hall sets and two corresponding reduction orders for which we can apply the reduction process and for which we have a criterion for a set to be a Gröbner basis. It would be interesting to find more Hall sets and corresponding reduction orders for which this is possible.

6 An application: the Chevalley-Harish-Chandra theorem

The objective of this section is to sketch a proof of a theorem that was first obtained independently by C. Chevalley and Harish-Chandra. With some simplifications it appears in [1], and in some more generality in [2]. The proof we describe here uses Theorem 13.

Let $A = (a_{ij})$ be an $n \times n$-matrix and let X be the set of $3n$ symbols $h_1, \dots, h_n, x_1, \dots, x_n, y_1, \dots, y_n$. In $L(X)$ we consider the set of elements $R = \{(h_i, h_j)$ for $i < j, (x_i, y_j) - \delta_{ij} h_i, (h_i, x_j) - a_{ij} x_j, (h_i, y_j) + a_{ij} x_j$ for $1 \leq i, j \leq n\}$.

Theorem 14 *Let I be the ideal of $L(X)$ generated by R and set $K = L(X)/I$. Then $K = N^- \oplus H \oplus N^+$, where N^- is the free Lie algebra generated by $y_1, \dots, y_n$, N^+ the free Lie algebra generated by $x_1, \dots, x_l$ and H the Abelian Lie algebra spanned by $h_1, \dots, h_n$.*

Proof. Let H be the Hall set relative to the lexicographical order or the one relative to the reverse-lexicographical order. In both cases it is straightforward to see that R is a Gröbner basis, using Theorem 13. Indeed, all compositions of the elements of R reduce to zero modulo R.

Now a basis of K is formed by all Hall elements h not having any $\mathrm{LM}(r)$ as a factor for $r \in R$. Using Theorem 10 we see that this is equivalent to $\varphi(h)$ not having $h_i h_j$, or $x_i y_j$, or $h_i x_j$, or $h_i y_j$ as a subword. By induction on the degree it is seen that such an h either only consists of letters x_i, or only of letters y_i or only of letters h_i. If h only consists of letters h_i, then it can be reduced unless $\deg(h) = 1$. Furthermore the elements h consisting only of letters x_i or only of letters y_i can not be reduced. The theorem follows. □

References

[1] N. Jacobson. *Lie Algebras.* Dover, New York, 1979.

[2] V. G. Kac. *Infinite Dimensional Lie Algebras.* Cambridge University Press, Cambridge, third edition, 1990.

[3] C. Reutenauer. *Free Lie Algebras*, volume 7 of *New Series.* Oxford University Press, Oxford, 1993.

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

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

[6] V. A. Ufnarovskij. *Combinatorial and Asymptotic Methods in Algebra*, volume 57 of *Encyclopedia of Mathematical Sciences*, chapter I, pages 1–196. Springer Verlag, Berlin, Heidelberg, New York, 1995.

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