THE FOX PROBLEM FOR FREE RESTRICTED LIE ALGEBRAS

HAMID USEFI

ABSTRACT. Let L be a free restricted Lie algebra and R a restricted ideal of L. Denote by $u(L)$ the restricted enveloping algebra of L and by $\omega(L)$ the associative ideal of $u(L)$ generated by L. The purpose of this paper is to identify the subalgebra $R \cap \omega^n(L)\omega(R)$ in terms of R only . This problem is the analogue of the Fox problem for free groups.

1. INTRODUCTION

The history of Fox's problem goes back to his original paper ([2]). His idea of free differential calculus has since been developed and has become an important tool in combinatorial algebra. Let F be a free group with the integral group ring $\mathbb{Z}F$ and R a normal subgroup of F. Recall that the augmentation ideal of $\mathbb{Z}F$, denoted by $\mathfrak{f}$, is the kernel of the $\mathbb{Z}$-linear map $\mathbb{Z}F \to \mathbb{Z}$ induced by $g \mapsto 1$ for every $g \in F$. Let $\mathfrak{r}$ be the kernel of the natural homomorphism $\mathbb{Z}F \to \mathbb{Z}(F/R)$. Fox introduced the problem of identifying the subgroup $F \cap (1+\mathfrak{f}^n\mathfrak{r})$ in terms of R. Following Gupta's initial work on the problem ([5]), Hurley ([8]) and Yunus ([15]) independently gave a complete solution to this problem. At the same time, Yunus gave a solution to the analogous problem for free Lie algebras ([16]). Recent progress on the Fox-type problem for free groups includes the work of Hurley and Sehgal ([9]) on the modular case: $\mathbb{Z}$ is replaced by the field of p elements. Also, in [7], Hurley gave an up-to-date account of the problem and announced a solution to the general form $F \cap (1 + \mathfrak{f}^n\mathfrak{r}^m)$.

Let L be a Lie algebra over a field $\mathbb{F}$ of characteristic p. The adjoint representation of L is given by $\mathrm{ad}x : L \to L$, $\mathrm{ad}x(y) = [y, x]$, where $x, y \in L$. Recall that L is called a restricted Lie algebra or Lie p-algebra if it additionally affords a p-map $^{[p]} : L \to L$, satisfying

(1) $(\mathrm{ad}x)^p = \mathrm{ad}(x^{[p]})$, for every $x \in L$;
(2) $(\alpha x)^{[p]} = \alpha^p x^{[p]}$, for every $x \in L$ and $\alpha \in \mathbb{F}$; and,

2000 *Mathematics Subject Classification.* Primary 17B50; Secondary 17A50.

(3) $(x+y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} s_i(x,y)$, for all $x, y \in L$, where $is_i(x,y)$ is the coefficient of λ^{i-1} in $\mathrm{ad}(\lambda x + y)^{p-1}(x)$.

For a restricted Lie algebra L, we denote the restricted enveloping algebra of L by $u(L)$. The associative ideal of $u(L)$ generated by L is called the augmentation ideal of $u(L)$ and is denoted by $\omega(L)$. The Poincaré-Birkhoff-Witt (PBW) Theorem for restricted Lie algebras allows us to view L as a restricted Lie subalgebra of $u(L)$. Henceforth, we identify the $[p]$-map of L with the exponentiation by p in $u(L)$. The reader is referred to the monographs [1] and [13] for basic background information.

Let $\mathbb{F}\langle X\rangle$ be the free associative algebra on a set X. The restricted Lie subalgebra L generated by X in $\mathbb{F}\langle X\rangle$ is the free restricted Lie algebra on X. For a Lie subalgebra H of L, we use H^{p^k} to denote the restricted Lie subalgebra of L generated by the elements x^{p^k} with x in H. For a positive integer n, the n^{th} term of the lower central series of L is denoted by $\gamma_n(L)$.

In this paper we examine the Fox problem for free restricted Lie algebras. Our main result is as follows.

Main Theorem. *Let R be a restricted ideal of a free restricted Lie algebra L. Then*

$$L \cap \omega^n(L)\omega(R) = \sum [R \cap \gamma_{i_1}(L), \ldots, R \cap \gamma_{i_k}(L)]^{p^j} + \sum (R \cap \gamma_i(L))^{p^\ell},$$

where the first sum is over all tuples $(i_1, \ldots, i_k)$, $k \geq 2$, and non-negative integer j such that $p^j(i_1 + \cdots + i_k) - i_t \geq n$, for every t in the range $1 \leq t \leq k$ and the second sum is over all positive integers i and ℓ such that $(p^\ell - 1)i \geq n$.

The basic definitions are given in Section 2. In Section 3, we prove some results about free restricted Lie algebras that might be of independent interest. In Section 4, we develop the well-known Magnus representations of free associative algebras by lower triangular matrices and show that the algebras $\omega^n(L)\omega(R)$ are the kernels of these representations. Proof of the Main Theorem will be presented in Section 5.

2. Preliminaries

Throughout this paper $\mathbb{F}$ denotes a field of characteristic p. Let L be a restricted Lie algebra over $\mathbb{F}$ and let $\mathcal{B}$ be a totally ordered basis for L. The PBW Theorem for restricted Lie algebras states that $u(L)$ has a basis consisting of PBW monomials, that is, monomials of the

form $z_1^{a_1} \cdots z_r^{a_r}$, where $z_1 \leq \cdots \leq z_r$ in $\mathcal{B}$, $0 \leq a_r < p$, and r is a non-negative integer.

For a subset $X \subseteq L$, we shall denote by $\langle X \rangle_{\mathbb{F}}$, $\langle X \rangle$, and $\langle X \rangle_p$ the vector subspace spanned by S, the Lie subalgebra generated by X, and the restricted subalgebra generated by X, respectively. For Lie subalgebras K and H of L we denote by $[K, H]$ the Lie subalgebra generated by all $[k, h]$ with $k \in K$ and $h \in H$. We use left-normed commutators for longer products in L, that is

$$[x_1, \ldots, x_{n+1}] = [[x_1, \ldots, x_n], x_{n+1}],$$

for every positive integer n. The n-th dimension subalgebra, $D_n(L)$, of L is defined by

$$D_n(L) = L \cap \omega^n(L).$$

Riley and Shalev in [11] showed that $D_n(L) = \sum_{ip^j \geq n} \gamma_i(L)^{p^j}$. It follows from the defining axioms of a restricted Lie algebra that for all x, y in L we have $[x, y^p] = (\mathrm{ad}y)^p(x)$ and $(x+y)^p = x^p + y^p$ modulo $\gamma_p(\langle x, y \rangle)$, and consequently that $D_m(L)^p \subseteq D_{pm}(L)$ and $[D_m(L), D_n(L)] = \gamma_{m+n}(L)$ for every $m, n \geq 1$. The latter two conditions together imply that the dimension subalgebras form a *restricted filtration* of L.

Consider the filtration of $u(L)$ given by the powers of $\omega(L)$:

$$u(L) = \omega^0(L) \supseteq \omega^1(L) \supseteq \omega^2(L) \supseteq \ldots.$$

Corresponding to this filtration is the graded associative algebra

$$\mathrm{gr}(u(L)) = \bigoplus_{i \geq 0} \omega^i(L)/\omega^{i+1}(L),$$

where the multiplication in $\mathrm{gr}(u(L))$ is induced by

$$(y_i + \omega^{i+1}(L))(z_j + \omega^{j+1}(L)) = y_i z_j + \omega^{i+j+1}(L),$$

for all $y_i \in \omega^i(L)$ and $z_j \in \omega^j(L)$. There is an analogous construction for restricted Lie algebras. That is, one can consider the graded restricted Lie algebra of L corresponding to its dimension subalgebras given by

$$\mathrm{gr}(L) = \bigoplus_{i \geq 1} D_i(L)/D_{i+1}(L).$$

It is proved in [11] and [14] that the embeddings

$$D_n(L)/D_{n+1}(L) \to \omega^n(L)/\omega^{n+1}(L)$$

induce an associative algebra isomorphism $u(\mathrm{gr}(L)) \to \mathrm{gr}(u(L))$.

For every $z \in L$, we define the height, $\nu(z)$, of z to be the largest subscript n such that $z \in \omega^n(L)$, if n exists, and to be infinite if it does not. We shall use these basic facts without explicit reference.

Throughout this paper the letters $\alpha, \beta, \alpha', \beta', \ldots$ denote the elements of $\mathbb{F}$.

We first give a generalization of Riley and Shalev's result in the following way:

Lemma 2.1. *Let R be a restricted subalgebra of a restricted Lie algebra L and m a positive integer. Then $\omega(R) \cap \omega(L)\omega^m(R) = \omega^{m+1}(R)$; hence, $L \cap \omega(L)\omega^m(R) = D_{m+1}(R)$.*

Proof. Obviously, $\omega^{m+1}(R) \subseteq \omega(R) \cap \omega(L)\omega^m(R)$. To prove the converse inclusion, we fix a basis $\mathcal{B}_2$ of R and extend $\mathcal{B}_2$ to a basis $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ of L. We order $\mathcal{B}$ in such a way that all the elements in $\mathcal{B}_1$ are less than all the elements in $\mathcal{B}_2$. So, a typical PBW monomial in $u(L)$ has the form $x_1^{a_1} \ldots x_r^{a_r} y_1^{b_1} \ldots y_t^{b_t}$, where each $x_i \in \mathcal{B}_1$, each $y_j \in \mathcal{B}_2$ and $x_1 < \cdots < x_r < y_1 < \cdots < y_t$, $0 \leq a_i, b_j \leq p-1$, and r, t are non-negative integers. Let z be a non-zero element in $\omega(R) \cap \omega(L)\omega^m(R)$. Then z is a sum of elements uv, where each u is a non-trivial PBW monomial of the form $x_1^{a_1} \ldots x_r^{a_r} y_1^{b_1} \ldots y_t^{b_t}$ and each $v \in \omega^m(R)$. So, each uv has the form $uv = x_1^{a_1} \ldots x_r^{a_r} y_1^{b_1} \ldots y_t^{b_t} v$, where either $\sum_{i=1}^r a_i \neq 0$ or $\sum_{i=1}^r a_i = 0$ and $\sum_{j=1}^t b_j \neq 0$. Now we have

$$z = \sum \alpha u' v' + \sum \beta w,$$

where each u' is a non-trivial PBW monomial in $\mathcal{B}_1$ only, each v' is a non-trivial PBW monomial in $\omega(R)$, and each w is a PBW monomial in $\omega(R)$ such that $\sum \beta w \in \omega^{m+1}(R)$. This is the unique PBW representation of z. However, $z \in \omega(R)$ and therefore, by the linear independence of PBW monomials, $z = \sum \beta w \in \omega^{m+1}(R)$. This proves the first assertion. To prove the second assertion, let $z \in L \cap \omega(L)\omega^m(R) \subseteq L \cap \omega(L)\omega(R)$. So, $z = \sum uv$, where each u is a (possibly trivial) PBW monomial in the $\mathcal{B}_1$ only and each $v \in \omega(R)$. In fact, all the u's must be trivial since every element of L is a linear combination of elements of $\mathcal{B}$. It follows that $z \in \omega(R)$. So, $z \in L \cap \omega(R) \cap \omega(L)\omega^m(R) = L \cap \omega^{m+1}(R) = D_{m+1}(R)$, as required.□

3. Free restricted Lie algebras

Let $\mathbb{F}\langle X \rangle$ be the free associative algebra on a set X. The free Lie algebra on the set X is the Lie subalgebra generated by X in $\mathbb{F}\langle X \rangle$; whereas, the restricted Lie subalgebra $L_p(X)$ generated by X in $\mathbb{F}\langle X \rangle$ is the free restricted Lie algebra on X. Throughout the rest of this paper, we write L for $L_p(X)$. It is known that $U(L(X)) \cong u(L) \cong \mathbb{F}\langle X \rangle$, where $U(L(X))$ is the universal enveloping algebra of $L(X)$. Henceforth, we identify these algebras. We write $\omega(L)$ for the augmentation ideal of

$\mathbb{F}\langle X\rangle$. Note that $L(X) \cap \omega^n(L) = \gamma_n(L(X))$ and $L \cap \omega^n(L) = D_n(L)$, see [12] or [14].

The free algebra $\mathbb{F}\langle X\rangle$ has a natural grading where the elements of X are called monomials of degree 1 and if u, v are monomials of degree r and s, then uv is a monomial of degree $r+s$. It is known that $L(X)$ and L inherit the grading of $\mathbb{F}\langle X\rangle$. Indeed, the vector subspace spanned by Lie commutators of length n in the generating set X form the n-th homogeneous component of $L(X)$. We now specify the grading of L more precisely. Note that we may identify $\langle X\rangle_{\mathbb{F}}$ and $\omega(L)/\omega^2(L)$ as vector spaces. Clearly we get a graded algebra epimorphism:

$$\mathbb{F}\langle X\rangle \to \bigoplus_{i\geq 0} \omega^i(L)/\omega^{i+1}(L).$$

Because of the freeness of $\mathbb{F}\langle X\rangle$ this homomorphism is injective. So, we may identify $\mathbb{F}\langle X\rangle$ and $\mathrm{gr}(u(L))$. As we mentioned in Section 2, we can identify $\mathrm{gr}(u(L))$ and $u(\mathrm{gr}(L))$, as algebras. Thus, we have the following identifications of algebras:

$$u(L) = \mathbb{F}\langle X\rangle = \mathrm{gr}(u(L)) = u(\mathrm{gr}(L)).$$

In particular, we have the following identification:

$$u(L) = u(\mathrm{gr}(L)).$$

Note that under this identification, $\langle X\rangle_{\mathbb{F}}$ coincides with $L/D_2(L)$. It follows that the restricted subalgebra generated by X in $u(L)$ may be identified with the restricted subalgebra generated by $L/D_2(L)$ in $u(\mathrm{gr}(L))$. We conclude that we can identify L and $\mathrm{gr}(L)$.

Every Lie commutatore in $L(X)$ can be written as a linear combination of left-normed Lie commutators. We need to choose an $\mathbb{F}$-basis $\mathbf{B}$ for $L(X)$ consisting of left-normed commutators. It is enough to choose a basis for each homogeneous component consisting of left-normed commutators. Throughout this paper, we shall assume that a basis $\mathbf{B}$ of $L(X)$ is constructed in the following way. We take the x_i's as a basis for the first homogeneous component. If a basis for n-th homogeneous component is constructed then a basis for the subspace spanned by all $[u, x]$, where u is a basis element of degree n and $x \in X$, provides a basis for the $(n + 1)$-th homogeneous component. A construction of normed basis of a free Lie algebra is given in [3].

M. Hall, Jr. and Shirshov constructed other bases for $L(X)$ that can be used in algorithmic problems, see [1]. But those bases may contain Lie commutatores that are not left-normed Lie commutators.

Let $u \in L(X)$ be a Lie commutator of length n and write u as a linear combination of basis elements in $\mathbf{B}$. Then, we have:

(1) Every basis element z that appears in the representation of u has height n. Note that $\nu(z)=n$ if and only if $z\in\gamma_n(L)\backslash\gamma_{n+1}(L)$.
(2) Every basis element z that appears in the representation of u involves the same generators x_i that u involves.

It is also well-known that the set $\mathbf{B}_p = \{z^{p^j} \mid z \in \mathbf{B}, j \geq 0\}$ is a basis for L, see for example [1]. So, if we order $\mathbf{B}$ in some way, a typical PBW monomial in $\mathbb{F}\langle X\rangle$ is of the form $z_{r_1} \dots z_{r_t}$, where $z_{r_1} \leq \dots \leq z_{r_t}$ in $\mathbf{B}$. Note that every monomial $x_{i_1} \dots x_{i_s} \in \mathbb{F}\langle X\rangle$ can be written in terms of PBW monomials $z_{r_1} \dots z_{r_t}$ with the property that $\sum_{k=1}^{t} \nu(z_{r_k}) = s$.

The *support* of an element $u \in \omega(L)$ denoted by $\mathrm{Supp}(u)$ is defined to be the set of all $x_i \in X$ that are involved in the unique expression of u in $\mathbb{F}\langle X\rangle$. By collecting the terms, we can write u as a sum of the terms $u_i x_i$, where $x_i \in \mathrm{Supp}(u)$ and $u_i \in \mathbb{F}\langle X\rangle$. The u_i are called the *Fox derivatives* of u (with respect to the generating set X). The following lemma is well-known, see Lemma 23.4 in [10]. We offer a different proof using the PBW Theorem.

Lemma 3.1. *Let $u \in L$. For every $x_i \in Supp(u)$, the Fox derivatives u_i are non-zero.*

Proof. Suppose that $x_i \in \mathrm{Supp}(u)$. We order the basis $\mathbf{B}_p$ so that every basis element that has x_i in its support is smaller than all the basis elements that do not have x_i in their supports. Suppose to the contrary that $u_i = 0$. Then u is of the form $u = \sum \alpha v x_i w + \sum \beta y$, where the v, w, y are monomials in $\mathbb{F}\langle X\rangle$ such that w and y do not involve x_i and w is non-trivial. Note that we can write each term vx_i as a sum of PBW monomials $z_{r_1} \dots z_{r_t}$ such that the first basis element z_{r_1} does involve x_i. So, $u = \sum \alpha' v' w' + \sum \beta' y'$, where each v' is a PBW monomial that involves x_i, each w' is a non-trivial PBW monomial, and each y' is a PBW monomial that does not involve x_i. Observe that this is the unique PBW representation of u. But $u \in L$ and by the PBW Theorem u can be written only in terms of basis elements in $\mathbf{B}_p$, a contradiction. □

Although subalgebras of free associative algebras are not necessarily free, it is known that the freeness is inherited by subalgebras in the category of Lie algebras and restricted Lie algebras. In particular, the following result is well-known. Its proof is implicitly given in Theorem 2.7.8 in [1].

Theorem 3.2. *Let H be a homogeneous restricted subalgebra of a free restricted Lie algebra L. Then H has a homogeneous free generating set.*

Definition 3.3. *A subset Y of a free restricted Lie algebra L is said to be algebraically independent if Y freely generates a restricted subalgebra of L.*

Let R be a restricted subalgebra of a free restricted Lie algebra L. By Witt's Theorem, the restricted subalgebra R is free, see Theorem 2.7.7 in [1]. However, we need a generating set to be chosen in another way as described in the following lemma. Note that for every element $z \in \mathbb{F}\langle X\rangle$, we denote by $\bar{z}$ the homogeneous component of z of least degree. It is clear that if $z \in L$, then $\bar{z}$ lies in L. Let us also denote by R_n the subalgebra $R \cap \gamma_n(L)$, for every $n \geq 1$. It is useful to observe that $\gamma_n(L) = \gamma_n(L(X))$, for every $n \geq 2$.

Lemma 3.4. *Let R be a restricted subalgebra of a free restricted Lie algebra L and let n be a positive integer. There exist linearly independent subsets $Y_1 \subseteq R$ and $Y_2 \subseteq R_n$ such that $Y_1 \cup Y_2 + D_2(R)$ is a basis for $R/D_2(R)$ and the elements $\bar{y}$ with $y \in Y_1$ are algebraically independent.*

Proof. Let H be the restricted subalgebra of L generated by the set

$$\bar{R} = \{\bar{r} \mid r \in R\}.$$

By Theorem 3.2, H can be freely generated by a homogeneous set W. We first claim that $W \subseteq \bar{R}$. Indeed let $w \in W$. Since $\bar{R}$ generates H, we can write w as a linear combination of elements $[\bar{r}_{i_1}, \ldots, \bar{r}_{i_k}]^{p^j}$ that have same degree as w, say $w = \sum \alpha[\bar{r}_{i_1}, \ldots, \bar{r}_{i_k}]^{p^j}$. If we let $u = \sum \alpha[r_{i_1}, \ldots, r_{i_k}]^{p^j}$ then it is not hard to see that $w = \bar{u} \in \bar{R}$, proving the claim. Now, for each $z \in W$, we fix an $r \in R$ such that $\bar{r} = z$ and denote the collection of these r by V. Since a relation between the elements of V clearly yields a relation between the elements of W, it follows that V is also algebraically independent. Our second claim is that V generates R modulo R_n. For suppose to the contrary and let $u \in R \setminus \langle V\rangle_p + R_n$ such that $\bar{u}$ has maximal degree ($< n$). Now write $\bar{u}$ in terms of the $\bar{r} \in W$. Substituting every $\bar{r}$ in the expression of $\bar{u}$ by the corresponding $r \in V$ gives a new element u_1 in $\langle V\rangle_p$. It follows that $u - u_1 \notin \langle V\rangle_p + R_n$, but degree of $\overline{u-u_1}$ is greater than degree of $\bar{u}$, contradicting the choice of u. We deduce, from the second claim, that there exists a subset $Y_1 \subseteq V$ such that $Y_1 + R_n + D_2(R)$ forms a basis for $R/R_n + D_2(R)$. To complete the construction, we choose a linearly independent subset Y_2 of R_n so that $Y_1 \cup Y_2 + D_2(R)$ is a basis for $R/D_2(R)$. □

The following lemma is known, see Lemma 2.4.3 in [1].

Lemma 3.5. *Let $L(X)$ be the free Lie algebra on X and let Y be a basis of the vector space spanned by X. Then Y is a free generating set for $L(X)$.*

In fact, it is enough that the image of Y is a basis of $L(X)/\gamma_2(L(X))$. We now deduce a similar statement for restricted Lie algebras.

Lemma 3.6. *Let Y be a subset of $L_p(X)$. If Y is linearly independent modulo $D_2(L_p(X))$ then Y is algebraically independent.*

Proof. By assumption, the set $\bar{Y} = \{\bar{y} \mid y \in Y\}$ can be extended to a basis Z of the vector space spanned by X. It follows, by Lemma 3.5, that $L(X) = L(Z)$. So, $L_p(X) = L_p(Z)$ and consequently $\bar{Y}$ is algebraically independent. Since every relation among the y's yields a relation among the $\bar{y}$'s, Y is also algebraically independent. □

4. Matrix representations of free algebras

Gupta and Passi in [6] developed the well-known Magnus representations of free groups. In this section, we provide similar representations for free associative algebras.

Let R be a restricted ideal of the free restricted Lie algebra L and set $A = u(L/R)$. Let $\Lambda = \{\lambda_{i,x} \mid i \geq 2, x \in X\}$ be a set of independent commuting indeterminates and $A[\Lambda]$ be the ring of polynomials in the $\lambda_{i,x}$ over A. We denote by $T_n(A[\Lambda])$ the ring of all $n \times n$ lower triangular matrices over $A[\Lambda]$. For every $z \in L$, we denote by $\mathbf{z}$ its image in L/R. Now, for each $x \in X$, we define

$$\varphi_n(x) = \begin{bmatrix} \mathbf{x} & 0 & 0 & - & - & - & 0 & 0 \\ \lambda_{2,x} & 0 & 0 & - & - & - & 0 & 0 \\ 0 & \lambda_{3,x} & 0 & - & - & - & 0 & 0 \\ - & - & - & - & - & - & - & - \\ - & - & - & - & - & - & - & - \\ - & - & - & - & - & - & - & - \\ 0 & 0 & 0 & - & - & - & \lambda_{n+1,x} & 0 \end{bmatrix}$$

The unique extension of the map $\varphi_n : X \to T_{n+1}(A[\Lambda])$ to $u(L) = \mathbb{F}\langle X \rangle$ will be again denoted by φ_n. Note that $\varphi_n(x)$ is a submatrix of $\varphi_{n+1}(x)$. The (i,j)-entry of φ_n will be denoted by $\phi_{i,j}$. We need the following useful observation for later use. We omit the proof as it is easy.

Lemma 4.1. *The following statements hold.*

1. *For all $u \in u(L)$ and positive integers i, j such that $j \geq 2$, we have $\phi_{i,j}(u) \in \mathbb{F}[\lambda_{t,x} \mid t \geq j+1, x \in X]$.*

2. *For all $u \in u(L)$ and positive integers i, j such that $i \geq 2$, we have $\phi_{i,j}(u) \in \mathbb{F}[\lambda_{t,x} \mid t \leq i, x \in X]$.*

Proposition 4.2. *For every $n \geq 0$, we have* $\mathrm{Ker}\varphi_n = \omega^n(L)R$.

Proof. We proceed by induction on n. Note that φ_0 is the natural map $u(L) \to u(L/R)$ and it is known that the kernel of this map is $u(L)R = \omega^0(L)R$. So suppose $n \geq 1$ and that the result is true for $n-1$. We first show that $\omega^n(L)R \subseteq \mathrm{Ker}\varphi_n$. Let $z \in \omega^n(L)R$. Then z is a linear combination of elements uv, where $u \in \omega(L)$ and $v \in \omega^{n-1}(L)R$. Since each v lies in $\omega^{n-1}(L)R$, by the induction hypothesis, we have $\varphi_{n-1}(v) = 0$. So $\varphi_{n-1}(z) = 0$. Consequently, $\phi_{i,j}(v) = 0 = \phi_{i,j}(z)$, for every $i, j \leq n$. So, for every $j \leq n+1$,

$$\begin{aligned} \phi_{n+1,j}(z) &= \sum_{k=j}^{n+1} \phi_{n+1,k}(u)\phi_{k,j}(v) \\ &= \phi_{n+1,n+1}(u)\phi_{n+1,j}(v) = 0. \end{aligned}$$

This proves that $\omega^n(L)R \subseteq \mathrm{Ker}\varphi_n$. For the converse inclusion, let $z \in \mathrm{Ker}\varphi_n$. Then $z \in \mathrm{Ker}\varphi_0 \leq \omega(L)$. It follows that z is a sum of elements of the form $x\mu(x)$, where $x \in X$ and $\mu(x) \in u(L)$. Now, for $j \leq i \leq n$, we have

$$\begin{aligned} \phi_{i+1,j}(z) &= \sum_x \sum_{k=j}^{n+1} \phi_{i+1,k}(x)\phi_{k,j}(\mu(x)) \\ &= \sum_x \phi_{i+1,i}(x)\phi_{i,j}(\mu(x)) \\ &= \sum_x \lambda_{i+1,x}\phi_{i,j}(\mu(x)). \end{aligned}$$

Note that, by Lemma 4.1, $\phi_{i,j}(\mu(x)) \in A[\lambda_{k,x} \mid k \leq i, x \in X]$. Since the $\lambda_{k,x}$ are independent, it follows that $\phi_{i,j}(\mu(x)) = 0$, for each x. This means that $\varphi_{n-1}(\mu(x)) = 0$. Hence, by the induction hypothesis, each $\mu(x) \in \omega^{n-1}(L)R$ and therefore $z \in \omega^n(L)R$. □

Lemma 4.3. *The following assertions hold for every $n \geq 2$.*

(1) *For all $u \in \omega^{n-1}(L)$ and integers $2 \leq j \leq i$ such that $i - j \leq n-2$, we have $\phi_{i,j}(u) = 0$.*
(2) *For every $u \in \omega^{n-1}(L)$, we have $\phi_{n+1,2}(u) = 0$ if and only if $u \in \omega^n(L)$.*

Proof. Note that, for every $x \in X$, the submatrix of $\varphi_n(x)$ obtained by deleting the first row and first column is independent of the subalgebra R. So, it is enough to prove the assertions in the case $R = L$. We

first prove part (1) by induction on n. If $n = 2$, the statement is clear. So, suppose that $n \geq 3$ and let $u \in \omega^{n-1}(L)$ and $2 \leq j \leq i$ such that $i - j \leq n - 2$. We write u as a linear combination of elements of the form $x\mu(x)$, where $x \in X$ and $\mu(x) \in \omega^{n-2}(L)$. So,

$$\phi_{i,j}(u) = \sum_x \sum_{k=1}^{i} \phi_{i,k}(x)\phi_{k,j}(\mu(x)) = \sum_x \lambda_{i,x}\phi_{i-1,j}(\mu(x)).$$

Since $i-1-j \leq n-3$, each term $\phi_{i-1,j}(\mu(x))$ is zero, by the induction hypothesis. Thus, $\phi_{i,j}(u) = 0$, as required. Now we prove part (2). If $u \in \omega^n(L)$ then $\phi_{n+1,2}(u) = 0$, by part (1). To prove the converse, we use induction on n. Suppose that $n = 2$ and let $u \in \omega(L)$ such that $\phi_{3,2}(u) = 0$. Note that u is a linear combination of the $x \in X$ modulo $\omega^2(L)$, say $u = \sum_x \alpha x$ modulo $\omega^2(L)$. But, $\phi_{3,2}(\omega^2(L)) = 0$, by part (1). So we have,

$$\phi_{3,2}(\sum_x \alpha x) = \sum_x \alpha\lambda_{3,x} = 0.$$

Since the $\lambda_{3,x}$'s are independent, each α is zero and so u lies in $\omega^2(L)$. Now suppose that $n \geq 3$ and let $u \in \omega^{n-1}(L)$ be such that $\phi_{n+1,2}(u) = 0$. We write u as a linear combination of elements of the form $x\mu(x)$, where $x \in X$ and $\mu(x) \in \omega^{n-2}(L)$. Now,

$$\phi_{n+1,2}(u) = \sum_x \sum_{k=1}^{n+1} \phi_{n+1,k}(x)\phi_{k,2}(\mu(x)) = \sum_x \lambda_{n+1,x}\phi_{n,2}(\mu(x)) = 0.$$

Since $\phi_{n,2}(\mu(x)) \in A[\lambda_{k,x} \mid k \leq n, x \in X]$, by Lemma 4.1 and the $\lambda_{i,x}$ are linearly independent, we have $\phi_{n,2}(\mu(x)) = 0$, for each x. So, by the induction hypothesis, each $\mu(x)$ lies in $\omega^{n-1}(L)$. Thus, $u \in \omega^n(L)$. The proof is complete. □

5. Proof of the Main Theorem

We need some notations to rephrase the Main Theorem. Let R be a restricted ideal of the free restricted Lie algebra L on X, and n a positive integer. Recall that $R_i = R \cap \gamma_i(L)$, for every $i \geq 1$. For every $k \geq 2$, we define

$$P_k(n, R) = \sum [R_{i_1}, \ldots, R_{i_k}]^{p^j},$$

where the sum is over all k-tuples $(i_1, \ldots, i_k)$ of positive integers and non-negative integer j with the property that $p^j(i_1 + \cdots + i_k) - i_t \geq n$, for every t in the range $1 \leq t \leq k$. We also define

$$Q(n, R) = \sum R_i^{p^j},$$

where the sum is over all positive integers i and j such that $(p^j-1)i \geq n$. We set

$$P(n,R) = \sum_{k=2}^{n+1} P_k(n,R),$$

and

$$F(n,R) = L \cap \omega^n(L)R = L \cap \omega^n(L)\omega(R).$$

So, we need to prove that:

Theorem 5.1. *For every positive integer n, we have*

$$F(n,R) = P(n,R) + Q(n,R).$$

Proof. It is clear that $P(n,R) + Q(n,R) \subseteq F(n,R)$, for every $n \geq 1$. We prove the reverse inclusion for every $n \geq 1$. Note that, by Lemma 2.1,

$$F(1,R) = D_2(R) = \gamma_2(R) + R^p.$$

So, $F(1,R) = P(1,R) + Q(1,R)$. Now suppose that $n \geq 2$. Let $u \in F(n,R)$ and suppose to the contrary that $u \notin P(n,R) + Q(n,R)$. By Lemma 3.4, there exist linearly independent subsets $Y_1 \subseteq R$ and $Y_2 \subseteq R_n$ such that the image of $Y := Y_1 \cup Y_2$ modulo $D_2(R)$ forms a basis for $R/D_2(R)$ and the elements $\bar{y}$ with $y \in Y_1$ are algebraically independent. It follows from Lemma 3.6 that the set Y is algebraically independent. It is not hard to see that

$$R = \langle Y \rangle_p + D_t(R),$$

for every $t \geq 1$. But if $t \geq n+1$, then

$$D_t(R) \subseteq F(n,R) \cap (P(n,R) + Q(n,R)).$$

Thus, without loss of generality, we can assume that $u \in \langle Y \rangle_p$. Now we fix a basis $\mathbf{B}$ of $\langle Y \rangle$ as described in Section 3. We can write u uniquely as a linear combination of some basis elements in the basis $\mathbf{B}_p$:

$$u = \sum \alpha [y_{i_1}, \ldots, y_{i_k}]^{p^j}. \tag{1}$$

We first observe that for every basis element in the representation of u in equation (1) if $k = 1$ then $j \geq 1$, since Y is linearly independent modulo $D_2(R)$. Moreover, since $u \notin P(n,R)+Q(n,R)$, we may assume that for every such basis element there exists an integer s in the range $1 \leq s \leq k$ such that

$$p^j(\nu(y_{i_1}) + \cdots + \nu(y_{i_k})) - \nu(y_{i_s}) \leq n-1.$$

Now choose $y_{i_s} \in Y$ so that there exists a basis element

$$[y_{i_1}, \ldots, y_{i_k}]^{p^j}$$

in the representation of u that involves y_{i_s} and

$$m := p^j(\nu(y_{i_1}) + \cdots + \nu(y_{i_k})) - \nu(y_{i_s})$$

is minimum. Certainly, $m \leq n-1$. We write u as a sum of elements of the form $u_i y_i$, where the u_i are the Fox derivatives of u with respect to the generating set Y. By Proposition 4.2, we have $\phi_{m+2,1}(u) = 0$, since $u \in F(n,R) \subseteq F(m+1,R)$. Also, note that each u_i lies in $\omega^m(L)$. So, by part (1) of Lemma 4.3, we have

$$\begin{aligned} \phi_{m+2,1}(u) &= \sum_i \sum_{k=1}^{m+1} \phi_{m+2,k}(u_i)\phi_{k,1}(y_i) \\ &= \sum_i \phi_{m+2,2}(u_i)\phi_{2,1}(y_i) = 0. \end{aligned}$$

Notice that, by Lemma 4.1, we have

$$\phi_{2,1}(y_r) \in A[\lambda_{2,x} \mid x \in X],$$

and

$$\phi_{m+2,2}(u_i) \in A[\lambda_{t,x} \mid t \geq 3, x \in X].$$

Since

$$\mathrm{Ker}(\phi_{2,1}) \cap R = \omega(L)R \cap R = D_2(R),$$

by Proposition 4.2 and Theorem 2.1, and the y_i are linearly independent modulo $D_2(R)$, it follows that $\phi_{m+2,2}(u_i) = 0$, for every i. So, by part (2) of Lemma 4.3, each u_i lies in $\omega^{m+1}(L)$. To obtain the desired contradiction, it is, therefore, enough to prove that $u_{i_s} \notin \omega^{m+1}(L)$. In other words, we need to show that $\bar{u}_{i_s} \notin \omega^{m+1}(L)$. To prove this, we may assume that the generating set X is infinite. We can also replace u by its projection onto the subspace spanned by the basis elements $[y_{i_1}, \ldots, y_{i_s}, \ldots, y_{i_k}]^{p^j}$ in the representation of u that satisfy

$$p^j(\nu(y_{i_1}) + \cdots + \nu(y_{i_k})) - \nu(y_{i_s}) = m. \tag{2}$$

It follows from equation (2) that u_{i_s} is a linear combination of monomials of degree m. So, by the freeness of $\mathbb{F}\langle X\rangle$, to prove the claim it is enough to prove that $u_{i_s} \neq 0$ or equivalently, $\bar{u}_{i_s} \neq 0$.

It follows from equation (2) that every $y_i \in \mathrm{Supp}(u)$, $i \neq i_s$, is contained in Y_1, since $m \leq n-1$ and $Y_2 \subseteq \gamma_n(L)$. Note that if $y_{i_s} \in Y_2$ then u has the form

$$u = \sum \beta[y_{i_1}, \ldots, y_{i_s}, \ldots, y_{i_k}],$$

where each commutator involves one y_{i_s} and $\nu(y_{i_1}) + \cdots + \nu(y_{i_k}) - \nu(y_{i_s}) = m$. Since $\mathrm{Supp}(u)$ is finite, there exists $x \in X$ such that the set

$$\{\bar{y}_i \mid y_i \in \mathrm{Supp}(u), i \neq i_s\} \cup \{x\}$$

is algebraically independent. If $y_{i_s} \in Y_2$ we then replace u by the element that is obtained from u by replacing y_{i_s} with x in the expression of u. So, we may assume that either

$$u = \sum \alpha[y_{i_1}, \ldots, y_{i_s}, \ldots, y_{i_k}]^{p^j} \in \langle Y_1 \rangle_p$$

or

$$u = \sum \beta[y_{i_1}, \ldots, x, \ldots, y_{i_k}].$$

It follows that $\bar{u}_{i_s}$ is either a Fox derivative of

$$\sum \alpha[\bar{y}_{i_1}, \ldots, \bar{y}_{i_s}, \ldots, \bar{y}_{i_t}]^{p^j}$$

with respect to the free generating set $\{\bar{y} \mid y \in Y_1\}$ or a Fox derivative of

$$\sum \beta[\bar{y}_{i_1}, \ldots, x, \ldots, \bar{y}_{i_t}]$$

with respect to the free generating set $\{\bar{y}_i \mid y_i \in \mathrm{Supp}(u), i \neq i_s\} \cup \{x\}$. In either case $\bar{u}_{i_s}$ is non-zero, by Lemma 3.1, which yields the desired contradiction. The proof is complete. □

Remark. *Note that the algebras $\omega(R)\omega^n(L)$ and $\omega^n(L)\omega(R)$ do not coincide in general, for example take $R = D_2(L)$ and $n = 1$. If $\omega(L)\omega(R) = \omega(R)\omega(L)$, then*

$$\gamma_3(L) = [L, D_2(L)] \subseteq L \cap \omega(L)\omega(R).$$

So, by Lemma 2.1, we have

$$\gamma_3(L) \subseteq D_2(R) = D_2(L)^p + \gamma_2(D_2(L)) \subseteq D_4(L).$$

Hence,

$$\gamma_4(L) = [L, \gamma_3(L))] \subseteq [L, D_4(L)] = \gamma_5(L).$$

It follows that the lower central series of L stabilizes, a contradiction.

However, the proof of the Main Theorem (with some symmetric modifications) yields the same formula for $L \cap \omega(R)\omega^n(L)$ as in the Main Theorem.

ACKNOWLEDGMENT

I would like to thank my advisor Professor David Riley for his inspiration and contributions and the referee for useful comments and suggestions.

References

[1] Yu.A. Bahturin, *Identical Relations in Lie Algebras* (VNU Science Press, Utrecht, 1987).

[2] R.H. Fox, Free differential calculus I, *Ann. of Math.* **57** (1953), 547–560.

[3] E.S. Chibrikov, A right normed basis for free Lie algebras and Lyndon-Shirshov words, *J. Algebra* 302 (2006), no. 2, 593–612.

[4] K.W. Gruenberg, *Cohomological topics in group theory*, (Lecture Notes in Mathematics, 143, Springer, Berlin, 1970).

[5] N.D. Gupta, A problem of R.H. Fox, *Canad. Math. Bull.* **24** (1981) 129–136.

[6] N.D. Gupta, I.B.S. Passi, Some properties of Fox subgroups of free groups. *J. Algebra* **43** (1976), no. 1, 198–211.

[7] T.C. Hurley, Dimension and Fox subgroups, Around group rings (Jasper, AB, 2001), *Resenhas* **5** (2002), no. 4, 293–304.

[8] T.C. Hurley, Identifications in a free group, *J. Pure and Applied Algebra* **48** (1987), 249–261.

[9] T.C. Hurley, S.K. Sehgal, The modular Fox subgroups, *Communications in Algebra* **24** (14) (1996), 4563–4580.

[10] A.A. Mikhalev, A.A. Zolotykh, *Combinatorial Aspects of Lie Superalgebras* (CRC Press, Boca Raton, FL, 1995).

[11] D.M. Riley, A. Shalev, Restricted Lie algebras and their envelopes, *Canad. J. Math.* **47** (1995), 146–164.

[12] D.M. Riley, H. Usefi, The isomorphism problem for enveloping algebras of Lie algebras, Algebras and Representation Theory, to appear.

[13] H. Strade, R. Farnsteiner, *Modular Lie Algebras and Their Representations*, (Dekker, New York, 1988).

[14] H. Usefi, *Lie Algebras and their Universal Envelopes*, Ph.D. Thesis, University of Western Ontario, London, ON, 2006.

[15] I.A. Yunus, A problem of Fox, *Dokl. Akad. Nauk SSSR* **278** (1984), no. 1, 53–56.

[16] I.A. Yunus, The Fox problem for Lie algebras, *Uspekhi Mat. Nauk* **39** (1984), no. 3 (237), 251–252.

Department of Mathematics, The University of Western Ontario, London, ON, N6A 5B7, Canada

E-mail address: husefi@uwo.ca