J. Symbolic Computation (1990) **9**, 653–664

A Nilpotent Quotient Algorithm for Graded Lie Rings

GEORGE HAVAS†, M. F. NEWMAN‡ AND M. R. VAUGHAN-LEE§

National Center for Supercomputing Applications, University of Illinois at Urbana-Champaign, IL 61820, USA

‡ *Mathematics Research Section, Institute of Advanced Studies, Australian National University, Canberra, ACT 2601, Australia*

§ *Christ Church College, University of Oxford, Oxford OX1 1DP, UK*

Dedicated to our teacher and colleague Tim Wall on the occasion of his 65th birthday

(*Received* 15 *October* 1988)

A nilpotent quotient algorithm for graded Lie rings of prime characteristic is described. The algorithm has been implemented and applications have been made to the investigation of the associated Lie rings of Burnside groups. New results about Lie rings and Burnside groups are presented. These include detailed information on groups of exponent 5 and 7 and their associated Lie rings.

1. Introduction

We describe a nilpotent quotient algorithm for graded Lie rings of prime characteristic. We have implemented a computer program for this algorithm by modifying the Canberra nilpotent quotient program for groups which is described in Havas & Newman (1980). We have used the program to study the associated Lie rings of relatively free groups of exponent 5 and 7. Vaughan-Lee (1985) and Wall (1974, 1978, 1986) provide underlying definitions for the Lie ring context. Most importantly, they describe identities which hold in the associated Lie rings of groups of prime exponent and which are incorporated into our implementation of the algorithm.

Let $B(d, p)$ be the d-generator Burnside group of exponent p (that is, the free group of rank d in the variety of groups of exponent p). Let $R(d, p) = B(d, p)/J$, where J is the intersection of all normal subgroups of finite index in $B(d, p)$. It follows that every finite d-generator group of exponent p is a homomorphic image of $R(d, p)$ and, by a result of Kostrikin (1959, see also his book, 1986) that $R(d, p)$ is finite. Let $L(d, p)$ be the associated Lie ring of $B(d, p)$. Then, $L(d, p)$ is also the associated Lie ring of $R(d, p)$, and $L(d, p)$ has the same order and class as $R(d, p)$. We adopt the following notation for (Lie) products in Lie rings. If L is a Lie ring and $a, b \in L$ then we let ab denote the product of a and b. We use the left-normed convention for products of higher weight: if $a, b, c \in L$ then we let $abc = (ab)c$. We also let $ab^0 = a$, and inductively define $ab^{i+1} = (ab^i)b$.

It is known that $L(d, p)$ has characteristic p and satisfies the $(p-1)$-Engel condition $xy^{p-1} = 0$ for all x, y. So $L(d, p)$ is a homomorphic image of $E(d, p)$, where $E(d, p)$ is the freest d-generator Lie ring of characteristic p satisfying the $(p-1)$-Engel condition. In characteristic p the $(p-1)$-Engel condition is equivalent to the multilinear identity $K_p = 0$

† Permanent address: Key Centre for Software Technology, Department of Computer Science, University of Queensland, St Lucia, Queensland 4067, Australia.

0747–7171/90/050653 + 12 $03.00/0

where

$$K_p(x_1, x_2, \ldots, x_p) = \sum_{\sigma \in S_{p-1}} x_p x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(p-1)}.$$

So $L(d, p)$ satisfies the identity $K_p = 0$, and in fact $L(d, p)$ satisfies a sequence of multilinear identities $K_n = 0$ for $n = p, p+1, \ldots$. These identities are described in section 4.

It follows that $L(d, p)$ is a homomorphic image of $W(d, p)$, where $W(d, p)$ is the freest d-generator Lie ring of characteristic p satisfying the identities $K_n = 0$ for $n \geq p$. Thus, we have a projection from $E(d, p)$ onto $W(d, p)$ and a projection from $W(d, p)$ onto $L(d, p)$. By investigating $E(d, p)$ and $W(d, p)$ we obtain upper bounds for the order and class of $L(d, p)$, and hence of $R(d, p)$.

The main results obtained may be outlined as follows.

(a) If any seven factors of a Lie product of elements of $E(d, 5)$ are equal then the product is zero. In particular, if $a_1, a_2, \ldots, a_k \in E(d, 5)$ and any seven of the a_i are equal then $a_1 a_2 \ldots a_k = 0$. It follows that $E(d, 5)$ has class at most $6d$, and hence $R(d, 5)$ also has class at most $6d$.

(b) $E(3, 5)$ has dimension 2292 and class 17. $W(3, 5)$ has dimension 2282 and class 17. The class of $R(3, 5)$ is at most 17 and its order is at most 5^{2282}. The maximal class 12 quotient of $R(3, 5)$ has order 5^{2133}.

(c) The maximal class 18 quotient of $E(2, 7)$ has dimension 6473. The maximal class 18 quotient of $W(2, 7)$ has dimension 6366. The maximal class 18 quotient of $R(2, 7)$ has order 7^{6366}.

2. Background

The results in this paper rely heavily on a nilpotent quotient program for graded Lie rings. The first such program was used by Havas *et al.* (1974) to compute a presentation for $L(2, 5)$ in parallel with a calculation of a power-commutator presentation for $R(2, 5)$ by an implementation of a group nilpotent quotient algorithm. The current program improves on that earlier program in the following significant ways: it uses a substantially more efficient set of consistency relations; it uses general purpose routines for calculating specified multilinear relations; and it uses improved data structures. The program bears a strong resemblence to the analogous program for groups and has been implemented as a variant of the Canberra group program which is described in Havas & Newman (1980).

The group nilpotent quotient program comprises a set of routines which manipulate power-commutator presentations of groups. The Lie ring program is a set of routines which manipulate what we call product presentations of Lie rings. At this stage the implementation is restricted to Lie rings of prime characteristic. Use of the program enables us to study some graded Lie rings of prime characteristic with dimension into the thousands.

For a Lie ring L we define the *lower central series*

$$L = L^1 \geq L^2 \geq \ldots \geq L^k \geq L^{k+1} \geq \ldots$$

by setting $L^{k+1} = L^k L^1$. The ring L is *nilpotent* if there exists an integer n such that $L^{n+1} = \{0\}$. The smallest such integer n is the *class* of L.

A *product presentation* of a Lie ring of prime characteristic p consists of a finite set $\{a_1, a_2, \ldots, a_n\}$ of generators and a finite set of $n(n-1)/2$ relations

$$a_j a_i = \sum_{l=j+1}^{n} \alpha(i, j, l) a_l,$$

where $i<j$ and $\alpha(i,j,l)\in Z_p$ (the field of integers modulo p). We denote this presentation by $(n; p, \alpha)$ and the Lie ring it presents by $\langle n; p, \alpha\rangle$. Clearly, every Lie ring $\langle n; p, \alpha\rangle$ is nilpotent. Furthermore, every finitely generated nilpotent Lie ring of characteristic p has product presentations. (This can be proved in essentially the same way as the fact that every finite p-group has power-commutator presentations.)

Every element of $\langle n; p, \alpha\rangle$ can be represented by a word of the form $\sum_{l=1}^{n}\xi(l)a_l$ with $\xi(l)\in Z_p$, which we call a *normal* word. The product relations together with linearity and anticommutativity make it straightforward to calculate a normal word representing the (Lie) product of two elements given by normal words. Since the number of normal words for the Lie presentation $(n; p, \alpha)$ is p^n, the Lie ring $\langle n; p, \alpha\rangle$ has order at most p^n. If $\langle n; p, \alpha\rangle$ has order p^n we say that the presentation $(n; p, \alpha)$ is *consistent.*

The Lie rings $L(d, p)$ associated with Burnside groups are *graded* in the following sense. A Lie ring L of characteristic p is graded (by weights) if $L=L_1\oplus L_2\oplus\ldots\oplus L_c$ and $L_{i+1}=L_iL_1$ with $L_{c+1}=\{0\}$. The elements of L_i are the elements of L of *weight* i and we define the weight function ω from L to the integers accordingly. Note that this grading corresponds with the lower central series of L, that $L_iL_j\leq L_{i+j}$ and that L has class c. Also, a finitely presented Lie ring L of characteristic p is graded if all its relations are *homogeneous*; that is, if every relation has the form $\sum\alpha_i m_i=0$, where each m_i is a product of the same number of factors from the generating set.

We can obtain a *weighted* product presentation for a graded Lie ring L of characteristic p in the following way. First we pick a basis $a_1, a_2,\ldots, a_d$ for L_1 as a vector space over Z_p. Note that $\{a_1, a_2,\ldots, a_d\}$ is a minimal generating set for L. We assign weight one to each of these generators, that is, set $\omega(a_1)=\omega(a_2)=\ldots=\omega(a_d)=1$. Since $L_2=L_1L_1$, it follows that L_2 is spanned by the products a_ja_i with $1\leq i<j\leq d$. We choose a basis $a_{d+1}, a_{d+2},\ldots, a_r$ for L_2 out of this spanning set of products, and we set $\omega(a_i)=2$ for $d<i\leq r$. Thus $a_1, a_2,\ldots, a_r$ is a basis for $L_1\oplus L_2$. Suppose, as an inductive hypothesis, that we have extended the basis $a_1, a_2,\ldots, a_d$ for L_1 to a basis $a_1, a_2,\ldots, a_t$ for $L_1\oplus L_2\oplus\ldots\oplus L_k$ such that $a_{s+1}, a_{s+2},\ldots, a_t$ is a basis for L_k. Since $L_{k+1}=L_kL_1$ it is spanned by elements of the form a_ja_i, with $s<j\leq t$ and $1\leq i\leq d$. We pick a basis $a_{t+1}, a_{t+2},\ldots, a_u$ for L_{k+1} out of this spanning set, and we assign

$$\omega(a_{t+1})=\omega(a_{t+2})=\ldots=\omega(a_u)=k+1.$$

Thus $a_1, a_2,\ldots, a_u$ is a basis for $L_1\oplus L_2\oplus\ldots\oplus L_{k+1}$. Continuing in this way we obtain a weighted basis $a_1, a_2,\ldots, a_n$ for L with the property that

$$1=\omega(a_1)=\omega(a_2)=\ldots=\omega(a_d)<\omega(a_{d+1})\leq\ldots\leq\omega(a_n)=c.$$

L is generated by the basis elements of weight one, and each basis element a_k with $\omega(a_k)>1$ has a *definition* $a_ja_i=a_k$, where $1\leq i\leq d, j>i$ and $\omega(a_k)=\omega(a_j)+1$. For each $1\leq i<j\leq n$, where a_ja_i is not the left-hand side of a definition, we can obtain a *relation* $a_ja_i=w_{ij}$, where w_{ij} is a linear combination of basis elements of weight $\omega(a_i)+\omega(a_j)$.

Conversely, suppose that we have a weighted presentation $(n; p, \alpha)$ which includes definitions for all non-basic generators and let $L=\langle n; p, \alpha\rangle$. Then, the product of any two linear combinations of $a_1, a_2,\ldots, a_n$ can be expressed as a linear combination of $a_1, a_2,\ldots, a_n$ by using the relations together with linearity and anticommutativity. Thus, the underlying additive group of L is spanned by $a_1, a_2,\ldots, a_n$. The presentation is *consistent* if $a_1, a_2,\ldots, a_n$ form a basis of this group. In this case, if we let L_i be the subspace of L spanned by those a_k which have weight i for $1\leq i\leq c$, then $L=L_1\oplus L_2\oplus\ldots\oplus L_c$

with $L_iL_j \leq L_{i+j}$ and $L_iL_1 = L_{i+1}$. Note that in a consistent presentation $a_ja_i = 0$, if $\omega(a_i) + \omega(a_j) > \omega(a_n)$.

It is possible to test whether or not the presentation is consistent in the following way. Let V be the elementary abelian p-group with basis $a_1, a_2, \ldots, a_n$. We define a bilinear product on V as follows. For $1 \leq i < j \leq n$ let $a_ja_i = w_{ij}$ and $a_ia_j = -w_{ij}$. Also define $a_ia_i = 0$ for $1 \leq i \leq n$ and let $(\sum \alpha_ia_i)(\sum \beta_ia_i) = \sum \alpha_i\beta_ja_ia_j$. This turns V into an alternating ring A of dimension n and characteristic p. If A satisfies the Jacobi identity $xyz + yzx + zxy = 0$ for all $x, y, z \in A$ then A is a Lie ring, and clearly $A = L$ and the presentation is consistent. To determine whether A is a Lie ring it is sufficient (by linearity) to check whether $a_ka_ja_i + a_ja_ia_k + a_ia_ka_j = 0$ for all $1 \leq i < j < k \leq n$. We show that, in fact, it is sufficient to check whether these relations hold for triples (i, j, k) with $1 \leq i < j < k \leq n$ and $w(a_i) = 1$. This result is an easier to prove analogue of a consistency checking condition for the group nilpotent quotient algorithm, given in Vaughan-Lee (1984).

Consider a triple (i, j, k) with $1 \leq i < j < k \leq n$ and $\omega(a_i) > 1$, and suppose, as an inductive hypothesis, that $a_wa_va_u + a_va_ua_w + a_ua_wa_v = 0$ whenever $1 \leq u < v < w \leq n$ and $u < i$. We show that $a_ka_ja_i + a_ja_ia_k + a_ia_ka_j = 0$. Since $\omega(a_i) > 1$, $a_i = a_ra_s$ for some $s < r < i$. In A the product a_ka_j can be expressed as a sum $\sum \alpha_ta_t$. So

$$\begin{aligned}
a_ka_ja_i &= \textstyle\sum \alpha_ta_ta_i \\
&= \textstyle\sum \alpha_ta_t(a_ra_s) \\
&= \textstyle\sum \alpha_t(a_ta_ra_s - a_ta_sa_r) \qquad \text{(by hypothesis)} \\
&= (\textstyle\sum \alpha_ta_t)a_ra_s - (\textstyle\sum \alpha_ta_t)a_sa_r \\
&= a_ka_ja_ra_s - a_ka_ja_sa_r.
\end{aligned}$$

Similarly,

$$\begin{aligned}
a_ja_ia_k &= a_j(a_ra_s)a_k \\
&= (a_ja_r)a_sa_k - (a_ja_s)a_ra_k \\
&= -a_sa_k(a_ja_r) - a_k(a_ja_r)a_s + a_ra_k(a_ja_s) + a_k(a_ja_s)a_r \\
&= a_ka_s(a_ja_r) - a_ka_r(a_ja_s) + (a_ja_r)a_ka_s - (a_ja_s)a_ka_r
\end{aligned}$$

and

$$\begin{aligned}
a_ia_ka_j &= -a_ka_ia_j \\
&= -a_k(a_ra_s)a_j \\
&= -(a_ka_r)a_sa_j + (a_ka_s)a_ra_j \\
&= a_sa_j(a_ka_r) + a_j(a_ka_r)a_s - a_ra_j(a_ka_s) - a_j(a_ka_s)a_r \\
&= a_ka_r(a_ja_s) - a_ka_s(a_ja_r) - (a_ka_r)a_ja_s + (a_ka_s)a_ja_r.
\end{aligned}$$

Adding these three equations we obtain

$$\begin{aligned}
a_ka_ja_i + a_ja_ia_k + a_ia_ka_j &= a_ka_ja_ra_s - a_ka_ja_sa_r \\
&\quad + a_ja_ra_ka_s - a_ja_sa_ka_r \\
&\quad - a_ka_ra_ja_s + a_ka_sa_ja_r \\
&= (a_ka_ja_r + a_ja_ra_k - a_ka_ra_j)a_s \\
&\quad - (a_ka_ja_s + a_ja_sa_k - a_ka_sa_j)a_r \\
&= 0 \qquad \text{by induction.}
\end{aligned}$$

This completes the proof that it is only necessary to consider triples (i, j, k) with $\omega(a_i) = 1$ to test consistency. This is the set of test words we use in our algorithm which is described in the next section.

3. The Basic Algorithm and Its Implementation

The Canberra group program works by constructing, in succession, consistent power-commutator presentations for the maximal nilpotent quotients with increasing (exponent-p central) class of suitably given groups. The Lie ring algorithm, which we now describe, constructs, in succession, consistent product presentations for the maximal nilpotent quotients with increasing class of suitably given Lie rings. After initialisation, the basic algorithm iterates the NEXTCLASS procedure until termination. Given a consistent weighted presentation for the maximal class $c-1$ quotient of a Lie ring L (that is, for L/L^c), the NEXTCLASS procedure, acts in outline as follows, to construct a consistent weighted presentation for the maximal class c quotient of L.

(1) Introduce weight c generators by modifying the relations $a_ja_i=0$ with $\omega(a_j)=c-1$ and $\omega(a_i)=1$.
(2) Modify the other relations $a_ja_i=0$ with $\omega(a_j)+\omega(a_i)=c$ using appropriate instances of the Jacobi identity.
(3) Introduce new relations $a_ja_i=0$ for all new generators a_j and $i<j$.
(4) Enforce the Jacobi identity to make this new presentation consistent.
(5) Enforce the defining relations of L.

We now amplify this outline to show how our nilpotent quotient algorithm operates in more detail. The nilpotent quotient algorithm takes, as input, a finitely presented Lie ring of characteristic p with homogeneous relations and a positive integer c, and yields as output a consistent weighted product presentation for L/L^{c+1}. There is no loss in assuming all the relations are homogeneous of weight at least 2, and then the generating set $\{a_1, a_2, \ldots, a_d\}$ for L is minimal. Thus, L/L^2 has a consistent weighted presentation with generators $a_1, a_2, \ldots, a_d$ all of weight one, and relations $a_ja_i=0$ for all $1\leq i<j\leq d$. The recording of this is the initial step of our algorithm.

Suppose now that we have obtained for $c\geq 2$ a consistent weighted presentation for L/L^c on generators $a_1, a_2, \ldots, a_n$. Note that $a_ja_i=0$ is a relation in this presentation for all i, j such that $1\leq i<j\leq n$ and $\omega(a_i)+\omega(a_j)\geq c$. We obtain a consistent weighted presentation for L/L^{c+1} as follows.

(1) For all i, j such that $1\leq i<j\leq n, \omega(a_i)=1$ and $\omega(a_j)=c-1$, we introduce a new generator a_k of weight c, and we replace the relation $a_ja_i=0$ in the presentation for L/L^c by the new relation $a_ja_i=a_k$ which provides the definition of a_k. We number the new generators which are introduced in this way $a_{n+1}, a_{n+2}, \ldots, a_m$.

(2) We then modify the other relations $a_ja_i=0$ with $\omega(a_i)+\omega(a_j)=c$. We order these relations lexicographically on the pairs (i, j), and modify them in ascending order. Thus, we first treat those with $i=d+1$, then those with $i=d+2$, and so on. This ordering is significant because it ensures that prerequisite calculations are done before relations which rely upon them are modified. For each of these relations, a_i has a definition $a_i=a_ra_s$ where $s<r<i$. We replace the relation $a_ja_i=0$ of L/L^c by the relation $a_ja_i=(a_ja_r)a_s-(a_ja_s)a_r$, using the previously modified relations to express $(a_ja_r)a_s-(a_ja_s)a_r$ as a linear combination of the new generators $a_{n+1}, a_{n+2}, \ldots, a_m$.

(3) When all the relations $a_ja_i=0$ of L/L^c with $\omega(a_i)+\omega(a_j)=c$ have been modified in this way we add extra relations $a_ja_i=0$ for all $i<j$ and $n<j\leq m$.

(4) This gives a not necessarily consistent presentation on $a_1, a_2, \ldots, a_m$. Now consider the value v of $a_ka_ja_i+a_ja_ia_k+a_ia_ka_j$ in the corresponding alternating ring A defined as in section 2. If $\omega(a_i)+\omega(a_j)+\omega(a_k)<c$ then $v=0$, since the presentation of L/L^c was assumed

to be consistent, and the relations of weight less than c are precisely the same as those of L/L^c. Also $v = 0$ if $\omega(a_i)+\omega(a_j)+\omega(a_k) > c$. But if $\omega(a_i)+\omega(a_j)+\omega(a_k) = c$ then v may be non-zero. Using the result of section 2 we evaluate v for all $1 \le i < j < k \le n$ such that $\omega(a_i) = 1$ and $\omega(a_j)+\omega(a_k) = c-1$. For each of these triples (i, j, k), v is a linear combination of $a_{n+1}, a_{n+2}, \ldots, a_m$. If $v \neq 0$ we can treat v as a relation on $a_{n+1}, a_{n+2}, \ldots, a_m$. This means that we can express some of the generators $a_{n+1}, a_{n+2}, \ldots, a_m$ in terms of others, and eliminate redundant generators from the presentation of A. When all eliminations of this form have been carried out (and after the remaining generators are renumbered) the weighted presentation is consistent.

(5) Finally, we have to enforce the homogeneous defining relations of L of weight c. For each defining relation $\sum \alpha_i m_i$ of L of weight c we use the weighted presentation to evaluate $\sum \alpha_i m_i$ as a linear combination of generators of weight c. Again these values can be treated as additional relations on the weight c generators, and redundant generators can be eliminated from the presentation. When all these eliminations have been carried out the resulting presentation is a consistent weighted presentation for L/L^{c+1}.

This basic algorithm accepts as input an integer specifying the number of generators, a prime specifying the characteristic of the ring, a finite set of homogeneous relations, and an integer specifying the class c. It produces a consistent product presentation for the largest class c quotient of the Lie ring described by this data. If the Lie ring actually has class $f < c$, the algorithm terminates as soon as the maximal class $f+1$ quotient is determined to be the same as the maximal class f quotient. This is discovered either while consistency is being enforced or while relations are being enforced and it is found that no generators of weight $f+1$ remain. In the next section, we show how the basic algorithm has been extended to handle special types of relations relevant to Lie rings associated with Burnside groups.

As mentioned before this algorithm was implemented by modifying the Canberra group program. This enabled us to utilise the data structures and input and output routines incorporated in that program. We wrote new subroutines to add and multiply elements in a Lie ring, to modify the relations generated at the previous class (as described above), and to enforce consistency via the Jacobi identity. These subroutines were substituted for existing subroutines performing analogous tasks in the group context.

4. Multilinear Identities and Relations

We extend the basic Lie ring nilpotent quotient algorithm described above to handle certain identities in the same kind of way that the group nilpotent quotient algorithm has been extended to handle exponent laws. Identities may be enforced by enforcing as relations suitable spanning sets of instances. Of interest to us are identities satisfied by Lie rings associated with Burnside groups.

We have already observed that $L(d, p)$ has characteristic p and $L(d, p)$ satisfies the $(p-1)$-Engel condition, and so $L(d, p)$ is a homomorphic image of $E(d, p)$. In fact, $L(d, p)$ satisfies a sequence of multilinear identities and the Engel condition is equivalent to the first of these. To describe the identities we introduce the following notation for (Lie) products. Suppose that $x, x_1, x_2, \ldots, x_n$ are elements in a Lie ring L. If $S = \{i, j, \ldots, k\}$ is a nonempty subset of $\{1, 2, \ldots, n\}$ with $i < j < \ldots < k$ we set $xx_S = xx_ix_j \ldots x_k$.

With this notation we set

$$K_n = K_n(x_1, x_2, \ldots, x_n) = \sum x_n x_{S(1)} x_{S(2)} \ldots x_{S(p-1)},$$

where the summation is taken over all partitions of $\{1, 2, \ldots, n-1\}$ into $(p-1)$ disjoint nonempty subsets $S(1), S(2), \ldots, S(p-1)$; so $n \geq p$. It follows from Theorem 1 of Vaughan-Lee (1985) that $L(d, p)$ satisfies the identities $K_n = 0$ for $n \geq p$. By Theorem 2 of Vaughan-Lee (1985) every multilinear identity which holds in $L(d, p)$ for all d is a consequence of these identities and the identity $px = 0$. Wall (1986) has shown that, if $n > p$ and $n \not\equiv 1 \bmod (p-1)$, then $K_n = 0$ is a consequence of the identity $px = 0$ and the identities $K_m = 0$ for $p \leq m < n$. Thus, the multilinear identities which hold in $L(d, p)$ for all d are consequences of the identity $px = 0$ and the identities $K_p = 0, K_{2p-1} = 0, K_{3p-2} = 0, \ldots$. In characteristic p the identity $K_p = 0$ is equivalent to the $(p-1)$-Engel identity.

Let $F(d, p)$ be the free Lie ring of characteristic p on free generators $x_1, x_2, \ldots, x_d$, and let I_n be the ideal of $F(d, p)$ generated by

$$\{K_m(u_1, u_2, \ldots, u_m) : u_i \in F(d, p), m \leq n\}.$$

We let $I = \bigcup_{n=1}^{\infty} I_n$. Clearly, $I_p \leq I_{p+1} \leq \ldots \leq I_n \leq \ldots \leq I$. It was shown in Vaughan-Lee (1985, Lemma 8) that I_n is spanned modulo I_{n-1} by the set S_n consisting of elements $K_n(b_1, b_2, \ldots, b_n)$, where $b_1, b_2, \ldots, b_n$ are basic Lie products on $x_1, x_2, \ldots, x_d$; $b_1 \leq b_2 \leq \ldots \leq b_n$ relative to the ordering on the basic Lie products; and $b_i \neq b_{i+p-1}$ for $1 \leq i < i+p-1 \leq n$ (that is, no basic product occurs more than $p-1$ times). Note that S_n is *multihomogeneous*; that is, each x_i occurs the same number of times as a factor in each element of S_n.

Wall's result (mentioned above) is that $I_n = I_{n-1}$ whenever $n \not\equiv 1 \bmod (p-1)$. Additionally, Vaughan-Lee has shown that if $p = 5$ then $I_{13} = I_9$. Combining these results we see that, in general, I is spanned by $S_p \cup S_{2p-1} \cup S_{3p-2} \cup \ldots$, and I is spanned by $S_5 \cup S_9 \cup S_{17} \cup \ldots$ when $p = 5$. This gives us effective methods for calculating consistent product presentations for the Lie rings $E(d, p)$ and $W(d, p)$ and for calculating quotients of these rings. We denote the maximal class c quotients of $E(d, p)$, $W(d, p)$ and $L(d, p)$ by $E(d, p; c)$, $W(d, p; c)$ and $L(d, p; c)$, respectively.

Given a consistent product presentation for $E(d, p; c-1)$ we obtain a consistent product presentation for $E(d, p; c)$ by following the basic algorithm described in section 3, with the following change. In addition to simply enforcing a listed set (in this case empty) of homogeneous defining relations, we also enforce the set S_p (provided $p \leq c$). Likewise, for $W(d, p; c)$ we enforce the appropriate sets S_i, for $i \leq c$, selected from the spanning set for I. More precisely, we enforce certain subsets of the relevant sets S_i because we take advantage of some relations between instances of K_i which follow from instances of the relation at the beginning of the proof of Lemma 8 of Vaughan-Lee (1985). In practice we wrote a subroutine to enforce the set S_p for any prime p. We also wrote specific subroutines for $p = 5$ and $p = 7$ to enforce the sets S_9 and S_{13}, respectively.

Certain quotient rings defined by other sets of relations are particularly useful for our purposes. To describe them we need to introduce the notion of multiweight. Suppose we have a consistent weighted presentation for a Lie ring B on a set of generators $a_1, a_2, \ldots, a_n$, where the generators of weight one are $a_1, a_2, \ldots, a_d$. We say that a product $a_{i_1} a_{i_2} \ldots a_{i_k}$ of weight-one generators has *multiweight* $(w_1, w_2, \ldots, w_d)$ if for each i $(1 \leq i \leq d)$ the index i occurs w_i times in the sequence $i_1, i_2, \ldots, i_k$. Thus a_2 has multiweight $(0, 1, 0, \ldots, 0)$ and $a_2 a_1 a_2$ has multiweight $(1, 2, 0, \ldots, 0)$. In general two products with different multiweights can equal the same element of B. But if B is the class c quotient of a finitely presented Lie ring L, and if all the relations of L are multihomogeneous, then products with different multiweights are linearly independent, and the grading of L respects multiweight. That is, if we have two multihomogeneous elements with multiweights $(u_1, u_2, \ldots, u_d)$ and $(v_1, v_2, \ldots, v_d)$ then their product is multihomogeneous and has multiweight $(u_1+v_1, u_2+v_2, \ldots, u_d+v_d)$.

The rings $E(d, p)$ and $W(d, p)$ are *multigraded* in this sense. It is an open question whether or not $L(d, p)$ is multigraded.

Quotients of interest for multigraded rings may be specified by a *maximal occurrence sequence* $(m_1, \ldots, m_d)$ of non-negative integers. For such a sequence we let $I(m_1, \ldots, m_d)$ be the ideal generated by all products in the generating set $(a_1, \ldots, a_d)$ with multiweight $(w_1, \ldots, w_d)$, where $w_i > m_i > 0$ for some i. (For $m_i = 0$, no restriction on occurrences of a_i is applied.) Given a maximal occurrence sequence $(m_1, \ldots, m_d)$ the program automatically calculates the largest class c quotient of $L/I(m_1, \ldots, m_d)$.

Multiweight analysis also provides some practical short cuts in enforcing a multihomogeneous identity. It can happen that instances of the identity with multiweight $(w_1, \ldots, w_d)$ arise when no generators of multiweight $(w_1, \ldots, w_d)$ remain. Evaluation of such instances is unnecessary and can be skipped. The program keeps track of the number of generators remaining of each multiweight so that when none of a given multiweight are left no further instances of the identity with that multiweight are evaluated. This process is referred to as applying a *weight pattern filter*. In some enforcing contexts (one of which is described later), we may know that, even though there are still some generators of multiweight $(w_1, \ldots, w_d)$, no further relations of that multiweight will be found from instances of the identity. A refined weight pattern filter based on this has been implemented.

5. Lie Rings Associated with Groups of Exponent 5

In his solution of the restricted Burnside problem for groups of exponent 5, Higman (1956) proved, in effect, that there is an integer N such that if L is a Lie ring of characteristic prime to 6 satisfying the fourth Engel condition then a product of elements in L is zero if an element of L occurs more than N times in the product. (Higman deliberately does not give an explicit value for N; using his Lemma 2 in essentially the same way as he does yields $N = 25$.) This can be restated using the notation introduced at the end of section 4: a product in $E(d, 5)$ of multiweight $(w_1, \ldots, w_d)$ is zero if some $w_i > N$. It follows that $E(d, 5)$ is nilpotent of class at most Nd. Higman (p. 382) says, "I believe that at the cost of a rather more complicated calculation one can get $N = 9$". Now, more than a generation later, we use the program to help prove the following sharp result.

THEOREM 1. *A product in $E(d, 5)$ with multiweight $(w_1, \ldots, w_d)$ is zero if some $w_i > 6$.*

This is best possible since it is well known [see Havas *et al.* (1974)], and quickly confirmed by the program, that $E(2, 5)$ has a nonzero element with multiweight (6, 6). We show in section 6 that all products in $E(3, 5)$ with multiweight (6, 6, 6) are zero and that $E(3, 5)$ has a nonzero product with multiweight (6, 6, 5). This naturally raises the question of to what extent Theorem 1 can be sharpened for larger numbers of generators. It seems likely that Theorem 1 extends to the setting Higman used, namely, all Lie rings of characteristic prime to 6 which satisy the fourth Engel condition.

Theorem 1 has the following result as an immediate corollary.

THEOREM 2. *The ring $E(d, 5)$ and the group $R(d,5)$ have class at most $6d$.*

To prove Theorem 1 it is clearly sufficient to prove that a product in $E(d, 5)$ with multiweight $(w_1, \ldots, w_d)$ is zero if $w_1 > 6$. Let $a_1, \ldots, a_d$ be a free generating set for $E(d, 5)$.

We show, using the same reduction as used by Higman, that it is sufficient to consider the Lie ring $H(d)=E(d,5)/M$ where M is the ideal generated by the products $a_j a_i$ where $2 \leq i < j \leq d$.

For, suppose that for every positive integer d the products in $H(d)$ of multiweight $(w_1, \ldots, w_d)$ with $w_1 > 6$ are zero. Let u be a product in $E(d,5)$ with multiweight $(7, w_2, w_3, \ldots, w_d)$. We show by induction on $w_2+w_3+\ldots+w_d$ that $u=0$. (This is trivially true if $w_2+w_3+\ldots+w_d=1$.) By hypothesis $u \in M$, and so u is a sum of products $a_i \ldots a_j(a_r a_s)a_m \ldots a_n$ with $2 \leq s < r \leq d$. Now $E(d,5)$ is multigraded and the generators of M are multihomogeneous, so we can assume that each of these products has the same multiweight as u. Thus, it is sufficient to prove that a product $a_i \ldots a_j(a_r a_s)a_m \ldots a_n$ with multiweight $(7, w_2, w_3, \ldots, w_d)$ is zero. But

$$a_i \ldots a_j(a_r a_s)a_m \ldots a_n = (a_i \ldots a_j a_{d+1} a_m \ldots a_n)\pi,$$

where π is the epimorphism from $E(d+1,5)$ to $E(d,5)$ such that $a_k\pi = a_k$ for $1 \leq k \leq d$ and $a_{d+1}\pi = a_r a_s$. And the product $a_i \ldots a_j a_{d+1} a_m \ldots a_n$ has multiweight $(7, w_1, \ldots, w_s-1, \ldots, w_r-1, \ldots, w_d, 1)$ and so is zero by induction.

Thus, Theorem 1 is a consequence of the corresponding result for $H(d)$. It is convenient to prove the following stronger result.

THEOREM 3. *A product in $H(d)$ with multiweight $(w_1, \ldots, w_d)$ is zero if $w_1 > 6$ or $w_2+\ldots+w_d > 6$.*

To prove Theorem 3 it clearly suffices to show that a product in $H(d)$ with multiweight $(w_1, \ldots, w_d)$ is zero if $w_1 = 7$ or $w_2+\ldots+w_d=7$. Thus, it suffices to work in $H(8)$ and the result, if correct, can be read off a product presentation for the largest class 13 quotient of $H(8)$.

It is beyond readily available resources to use the program to obtain such a presentation. (For example, we can show that the dimension of this ring is greater than 10000.) Note, however, that it suffices to show that the relevant multihomogeneous components with $w_2, \ldots, w_s \leq 1$ are trivial because then use of suitable homomorphisms shows that all the required multihomogeneous components are trivial. Thus, it suffices to obtain a product presentation for the largest class 13 quotient of $H = H(8)/I(7, \overbrace{1, \ldots, 1}^{7})$.

This ring has, as we know from other calculations, dimension 3235, so the program could be used but direct calculation would be rather lengthy. The calculation can be made of reasonable length by using the refined form of weight pattern filtering mentioned earlier. Observe first that the dimensions of all the multihomogeneous components of H with only three nonzero weights are given by the dimensions of the corresponding multihomogeneous components of $H(3)/I(7,1,1)$. That is, the multihomogeneous component of H with multiweight $(w, 0, \ldots, 0, 1, 0, \ldots, 0, 1, 0, \ldots, 0)$ has the same dimension as the multihomogeneous component of $H(3)/I(7,1,1)$ with multiweight $(w,1,1)$. Thus, one can stop looking for relations of such multiweights in H as soon as the appropriate dimension has been reached. A similar argument applies for all multihomogeneous components of H with a zero component in their multiweight. So we use the program to calculate a product presentation for $H(d)/I(7, \overbrace{1, \ldots, 1}^{d-1})$ with $d=3,4,5,6,7$.

The first three calculations are easy, the rings have dimensions 17, 62, 217 and the total time needed is less than 40 seconds on a VAX 8700. For $d=6$ the dimension is 626 and the time taken about 8 minutes. The calculation for $d = 7$ takes less than an hour with filtering and gives dimension 1519. The final calculation, which can (in the light of the results from the case $d = 7$) be done in $H(8)/I(6, \overbrace{1, \ldots, 1}^{7})$, takes less than 5 hours.

6. Four Computations

We have computed consistent weighted presentations for $E(3, 5)$ and $W(3, 5)$, and also for $E(2, 7; 18)$ and $W(2, 7; 18)$. The following table summarises the results obtained.

First we computed $E(3, 5) = F(3, 5)/I_5$. In this computation we were able to use the result of section 5 and impose the maximal occurrence sequence (6, 6, 6). This has no effect on the final result, but shortens the computation. As tabulated, $E(3, 5)$ has class 17 and it follows from this that $W(3, 5) = F(3, 5)/I$ has class at most 17. As elements in the spanning set S_n are composed of products of n basic products, the condition that no basic product occurs more than $p-1$ times in K_n implies that, for $d = 3$ and $p = 5$, the elements of S_{17} have weight greater than 17. So, for $d = 3$ and $p = 5$, I is spanned by $S_5 \cup S_9$, and $W(3, 5)$ was computed by imposing relations on $E(3, 5)$ corresponding to the elements of S_9.

Similarly, $W(2, 7; 18)$ was computed by imposing relations corresponding to the elements of S_{13} on $E(2, 7; 18)$.

	$E(3, 5)$		$W(3, 5)$		$E(2, 7)$		$W(2, 7)$	
Class	rank	total	rank	total	rank	total	rank	total
1	3	3	3	3	2	2	2	2
2	3	6	3	6	1	3	1	3
3	8	14	8	14	2	5	2	5
4	18	32	18	32	3	8	3	8
5	30	62	30	62	6	14	6	14
6	71	133	71	133	9	23	9	23
7	132	265	132	265	12	35	12	35
8	240	505	240	505	23	58	23	58
9	421	926	411	916	36	94	36	94
10	486	1412	486	1402	61	155	61	155
11	453	1865	453	1855	94	249	94	249
12	278	2143	278	2133	159	408	159	408
13	87	2230	87	2220	260	668	260	668
14	48	2278	48	2268	407	1075	406	1074
15	8	2286	8	2276	644	1719	640	1714
16	3	2289	3	2279	995	2714	985	2699
17	3	2292	3	2282	1538	4252	1510	4209
18	0		0		2221	6473	2157	6366
19					?	?	?	?

$L(d, p) = F(d, p)/J$ for some graded ideal $J \geq I$. Thus,

$$I_p = I_{2p-2} \leq I_{2p-1} = I_{3p-3} \leq I \leq J.$$

(While the ideals I_n and I are multigraded it is, as noted before, still an open question whether or not J is always multigraded.) If U is a graded ideal of $F(d, p)$ then for each positive integer w we let $U(w)$ be the homogeneous component of U of weight w. We summarise some of the results which are known about the equalities and inequalities occurring in the chain

$$I_p(w) = I_{2p-2}(w) \leq I_{2p-1}(w) = I_{3p-3}(w) \leq I(w) \leq J(w)$$

for various d, p and w.

(1) If $w \leq 2p-2$ then $I_p(w) = J(w)$ (Sanov, 1952).
(2) If $d=2$ then $I_p(2p-1) = J(2p-1)$ (Kostrikin, 1957).
(3) If $d=2$ and $p=5$ then $I_5 = J$ (Havas *et al.*, 1974).
(4) If $p=5$ then $I_9 = I_{13}$ (Vaughan-Lee, 1985).
(5) If $d \geqslant 3$ and $p=5$ or 7 then $I_p(2p-1) \neq I_{2p-1}(2p-1)$ (Wall, 1974).
(6) If $d=2$ and $p=7$ then $I_7(14) \neq I_{13}$ (Khukhro, 1982).
(7) If $d=2$ then $I_{2p-1}(2p) = J(2p)$ (Khukhro, 1982).
(8) If the elements of S_p of weight at most $2p-2$ are linearly independent in $F(d, p)$ then $I_{2p-1}(w) = J(w)$ for $w \leq 3p-3$ (Wall, 1978).

Result (5) for $p=5$ is independently confirmed both in the calculations for $E(3, 5)$ and $W(3, 5)$ tabulated here and also by a group nilpotent quotient calculation reported in Havas & Newman (1980). Result (6) is independently confirmed both in the calculations for $E(2, 7; 18)$ and $W(2, 7; 18)$ tabulated here and also by a group nilpotent quotient calculation.

Kostrikin (1957) showed that the hypothesis of (8) is satisfied for $d=2$ and $p=5$. We have verified that this hypothesis is satisfied for $d=3$, $p=5$ and for $d=2$, $p=7$. To do this we compared the dimensions of the homogeneous components of $F(d, p)$ of weight $p, p+1, \ldots, 2p-2$ with the dimensions of the corresponding components of $E(d, p)$. For each weight we showed that the difference between the two dimensions is equal to the number of elements in S_p of that weight. It follows that $L(3, 5; 12)$ is the same as $W(3, 5; 12)$, and that $L(2, 7; 18)$ is the same as $W(2, 7; 18)$. The results on R(3, 5) and R(2, 7) in section 1 are consequences.

A calculation in $E(2, 7)/I(13, 8)$ has shown that $E(2, 7)$ has class at least 21. We guess that the class of $W(2, 7)$ is at least 30 and that its dimension exceeds 20 000.

The scale of the calculations can be assessed from the fact that when initially done on a Cyber 205 supercomputer at Csironet in Canberra, the calculation for $W(3, 5)$ took about 56 cpu hours. The effectiveness of the weight pattern filtering techniques is illustrated by the fact that of 959 299 elements of weight 17 in S_5 for $E(3, 5)$ only 162 740 needed to be tested while 796 559 were filtered out.

Note added in proof: Vaughan-Lee has now shown that the order of R(3,5) is 5^{2282}. The details have been submitted for publication.

References

Havas, G., Newman, M. F. (1980). Applications of computers to questions like those of Burnside. In: (Mennicke, J. L., ed.) *Burnside Groups. Lecture Notes in Mathematics* **806**, pp. 211–230. Berlin: Springer.

Havas, G., Wall, G. E., Wamsley, J. W. (1974). The two generator restricted Burnside group of exponent five. *Bull. Austral. Math. Soc.* **10**, 459–470.

Higman, G. (1956). On finite groups of exponent five. *Proc. Cambridge Philos. Soc.* **52**, 381–390.

Khukhro, E. I. (1982). The associated Lie ring of the free two generator groups of prime exponent and the Hughes conjecture for two generator p-groups. *Mat. Sb.* **118**, 567–575; (1983) *Math. USSR Sbornik* **46**, 571–579.

Kostrikin, A. I. (1957). On the connection between periodic groups and Lie rings. *Izv. Akad. Nauk SSSR Ser. Mat.* **21**, 289–310; (1965) *Amer. Math. Soc. Transl. (2)* **45**, 165–189.

Kostrikin, A. I. (1959). The Burnside problem. *Izv. Akad. Nauk SSSR Ser. Mat.* **23**, 3–34; (1964) *Amer. Math. Soc. Transl. (2)*, **36**, 63–99.

Kostrikin, A. I. (1986). *Around Burnside*. Moscow: Nauka (Russian, an English translation is in preparation).
Sanov, I. N. (1952). Establishment of a connection between periodic groups with period a prime number and Lie rings. *Izv. Akad. Nauk SSSR Ser. Mat.* **16**, 23–58.
Vaughan-Lee, M. R. (1984). An aspect of the nilpotent quotient algorithm. In: (Atkinson, M. D., ed.) *Computational Group Theory*, pp. 75–83. London: Academic Press.
Vaughan-Lee, M. R. (1985). The restricted Burnside problem. *Bull. London Math. Soc.* **17**, 113–133.
Wall, G. E. (1974). On the Lie ring of a group of prime exponent. In: (Newman, M. F., ed.) *Proc. Second Int. Conf. Theory of Groups. Lecture Notes in Mathematics* **372**, pp. 667–690. Berlin: Springer.
Wall, G. E. (1978). On the Lie ring of a group of prime exponent II. *Bull. Austral. Math. Soc.*, **19**, 11–28.
Wall, G. E. (1986). On the multilinear identities which hold in the Lie ring of a group of prime-power exponent. *J. Algebra*, **104**, 1–22.