J. Austral. Math. Soc. (*Series A*) **49** (1990), 386–398

LIE RINGS OF GROUPS OF PRIME EXPONENT

M. R. VAUGHAN-LEE

(Received 17 July 1989; revised 1 December 1989)

Communicated by H. Lausch

Dedicated to G. E. (Tim) Wall, in recognition of his distinguished contribution to mathematics in Australia, on the occasion of his retirement

Abstract

We investigate the identities which hold in the associated Lie rings of groups of prime exponent. The multilinear identities which hold in these Lie rings are known, and it is conjectured that all the identities which hold in these Lie rings are consequences of multilinear ones. This is known to be the case for the associated Lie rings of two generator groups of exponent 5, and we provide some additional evidence for the conjecture by confirming that it also holds true for the associated Lie rings of three generator groups of exponent five.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 20 D 15, 17 B 60.

Introduction

One of Tim Wall's interests in recent years has been the study of the identities which hold in the associated Lie rings of groups of prime exponent p. Sanov [8] showed that if L is the associated Lie ring of a group of exponent p, then L has characteristic p, and L satisfies the $(p-1)$-Engel identity $xy^{p-1} = 0$. Higman's solution [5] of the restricted Burnside problem for groups of exponent 5, and Kostrikin's solution [7] of the restricted Burnside problem for general prime exponent, are based on this fact. Higman proved that there is an integer N such that if L is an r generator Lie ring of characteristic 5 satisfying the Engel identity $xy^4 = 0$, then L is nilpotent of class at most rN. Havas, Newman and Vaughan-Lee [3] have shown that it is possible

to take $N = 6$ in Higman's theorem. Kostrikin [7] proved that if L is a finitely generated Lie ring of characteristic p satisfying the Engel identity $xy^{p^{-1}} = 0$, then L is nilpotent. (Kostrikin did not obtain a bound for the nilpotency class in terms of the number of generators.) In particular, if we let $E(r, p)$ be the free r generator Lie ring in the variety of Lie rings determined by the identities $px = 0$ and $xy^{p^{-1}} = 0$, then $E(r, p)$ is nilpotent and hence finite. If G is any finite r generator group of exponent p, and if L is the associated Lie ring of G, then G and L have the same order and class. Furthermore, L is an r generator Lie ring satisfying the identities $px = 0$, $xy^{p^{-1}} = 0$. It follows that L is a homomorphic image of the finite Lie ring $E(r, p)$, and so the order of G is bounded by the order of $E(r, p)$. Thus there is a bound on the orders of finite r generator groups of exponent p. This implies that there is a largest finite r generator group of exponent p, $R(r, p)$, with the property that any finite r generator group of exponent p is a homomorphic image of $R(r, p)$. To see this we let $F(r)$ be the free group of rank r, and we let M be the normal subgroup of $F(r)$ generated by $\{g^p : g \in F(r)\}$. Then we let $B(r, p)$ be the quotient group $F(r)/M$. The group $B(r, p)$ is known as the r generator Burnside group of exponent p, and any r generator group of exponent p is a homomorphic image of $B(r, p)$. In particular any finite r generator group of exponent p is isomomorphic to $B(r, p)/L$ for some normal subgroup L of finite index in $B(r, p)$. Kostrikin's theorem implies that there is a bound on the possible finite indexes of normal subgroups of $B(r, p)$. We let K be a normal subgroup of $B(r, p)$ with maximal finite index and we let $R(r, p) = B(r, p)/K$. If L is any normal subgroup of $B(r, p)$ with finite index then $K \cap L$ is also a normal subgroup of finite index, and so, by the maximality of the index of K, we have $K \cap L = K$. This implies that $K \leq L$ and hence that $B(r, p)/L$ is a homomorphic image of $R(r, p)$. As we shall see in Section 1, $B(r, p)$ and $R(r, p)$ have the same associated Lie ring, which we denote by $L(r, p)$. The remarks above imply that $L(r, p)$ is a homomorphic image of $E(r, p)$, and Sanov asked whether $L(r, p) = E(r, p)$ for all r and p. The Lie ring $E(r, 2)$ is abelian (that is, nilpotent of class 1) for all r, and so it is trivial to see that $L(r, 2) = E(r, 2)$ for all r. It is also easy to see that $E(2, 3)$ is nilpotent of class 2, and that $E(r, 3)$ is nilpotent of class 3 for $r \geq 3$. It follows from this that $L(r, 3) = E(r, 3)$ for all r. But in 1973 Wall [11] found a new identity which holds in the associated Lie rings of groups of exponent p, and he showed that if $p = 5$ or $p = 7$ and if $r \geq 3$ then $E(r, p)$ does not satisfy this new identity. Huhro [6] showed that $E(2, 7)$ does not satisfy Wall's identity. Thus $L(r, p)$ is a proper homomorphic image of $E(r, p)$ for $r = 2$ and $p = 7$, and for $r \geq 3$

and $p = 5, 7$. On the other hand, Havas, Wall, and Wamsley [4] have shown that $L(2, 5) = E(2, 5)$. In 1984 I found a sequence of multilinear identities $K_n = 0$ $(n \geq p)$ which hold in the associated Lie rings of groups of exponent p. These identities are described in [9], where it is proved that any multilinear identity which holds in the associated Lie ring of every group of exponent p must be a consequence of the identities $K_n = 0$ $(n \geq p)$ and the identity $px = 0$. The Engel identity $xy^{p-1} = 0$ is equivalent to a multilinear identity in characteristic p, and Wall's identity is also multilinear. So if we let $W(r, p)$ be the free r generator Lie algebra in the variety of Lie algebras determined by the identities $K_n = 0$, $px = 0$ then $L(r, p)$ is a homomorphic image of $W(r, p)$, which in its turn is a homomorphic image of $E(r, p)$. It seems natural to conjecture that $L(r, p) = W(r, p)$ for all r and p, and we provide some slight evidence for this conjecture by proving the following theorem.

THEOREM 1. $L(3, 5) = W(3, 5)$.

Havas, Newman, and Vaughan-Lee [3] have computed the order and class of $W(3, 5)$ and shown these to be 5^{2282} and 17 respectively. So we obtain the following theorem as a corollary to Theorem 1.

THEOREM 2. *$R(3, 5)$ and $L(3, 5)$ have order 5^{2282} and class 17.*

1. The associated Lie ring of a group

Let G be a group. Then we define the lower central series

$$\gamma_1 \geq \gamma_2 \geq \cdots \geq \gamma_i \geq \cdots$$

of G as follows. We let $\gamma_1 = G$, and for $i \geq 1$ we let γ_{i+1} be the subgroup of G generated by $\{[g, h]: g \in \gamma_i, h \in G\}$. For $i = 1, 2, \ldots$ we let $L_i = \gamma_i/\gamma_{i+1}$. We think of L_i as a $\mathbb{Z}$-module and we let

$$L = \bigoplus_{i=1}^{\infty} L_i.$$

Note that if G has exponent p then the quotients γ_i/γ_{i+1} are elementary abelian, and so L has characteristic p. If $a = g\gamma_{i+1} \in L_i$ and $b = h\gamma_{j+1} \in L_j$ then we define the Lie product ab of a and b in L by setting

$$ab = [g, h]\gamma_{i+j+1} \in L_{i+j}.$$

https://doi.org/10.1017/S1446788700032407 Published online by Cambridge University Press

We extend this Lie product to the whole of L by linearity, and this turns L into a Lie ring, the associated Lie ring of G. Since $L = \bigoplus L_i$ and $L_iL_j \leq L_{i+j}$, L is a graded Lie ring. It also satisfies the additional property that $L_iL_1 = L_{i+1}$ for $i = 1, 2, \ldots$, reflecting the fact that $[\gamma_i, \gamma_1] = \gamma_{i+1}$ for $i = 1, 2, \ldots$. This means that if some subset of L_1 generates L_1 as a $\mathbb{Z}$-module, then the same subset generates L as a Lie ring. Thus if G is an r generator group then its associated Lie ring L is an r generator Lie ring, and we can express L as a quotient Lie ring Λ/J, where Λ is the free Lie ring of rank r and where J is some ideal of Λ. The free Lie ring Λ is also graded. That is,

$$\Lambda = \Lambda_1 \oplus \Lambda_2 \oplus \cdots \oplus \Lambda_i \oplus \cdots .$$

where $\Lambda_i\Lambda_j \leq \Lambda_{i+j}$. In addition $\Lambda_i\Lambda_1 = \Lambda_{i+1}$ for all i. So we can express L as a quotient Λ/J for some graded ideal

$$J = J_1 \oplus J_2 \oplus \cdots \oplus J_i \oplus \cdots ,$$

and $L_i = \Lambda_i/J_i$ for $i = 1, 2, \ldots$.

If G is a finite p-group then G is nilpotent, and G has the same order and class as its associated Lie ring L. Recall that $R(r, p)$ was defined to be $B(r, p)/K$, where K is the normal subgroup of $B(r, p)$ with maximal finite index. If γ_i is any term of the lower central series of $B(r, p)$ then $B(r, p)/\gamma_i$ is a finite group and so $K \leq \gamma_i$. On the other hand $B(r, p)/K$ is a finite p-group and so is nilpotent, and this implies that $\gamma_i \leq K$ for some i. So there is some integer i such that $\gamma_j = K$ for all $j \geq i$. This implies that $B(r, p)$ and $R(r, p)$ have the same associated Lie ring $L(r, p)$, and that $L(r, p)$ has the same order and class as $R(r, p)$. We express $L(r, p)$ as a quotient Λ/J for some graded ideal J of Λ, as above.

2. Gradings and multigradings

The free Lie ring Λ of rank r is a graded Lie ring, as we described in the last section. But it is also possible to define a multigrading on Λ. Suppose that the free generators of Λ are $x_1, x_2, \ldots, x_r$. Then Λ_i is spanned as a $\mathbb{Z}$-module by the Lie products $y_1y_2 \cdots y_i$ with $y_1, y_2, \ldots, y_i \in \{x_1, x_2, \ldots, x_r\}$. We assign a multiweight $(w_1, w_2, \ldots, w_r)$ to the product $y_1y_2 \cdots y_i$ where (for each $j = 1, 2, \ldots, r$) w_j is the number of times x_j occurs in the sequence $y_1, y_2, \ldots, y_i$. Thus x_1 has multiweight $(1, 0, \ldots, 0)$, and $x_2x_3x_3$ has multiweight $(0, 1, 2, 0, \ldots, 0)$, and so on. For each possible multiweight $\mathbf{w}$ we let $\Lambda_{\mathbf{w}}$ be the multihomogeneous component of Λ spanned as a $\mathbb{Z}$-module by Lie products $y_1y_2 \ldots y_i$ with multiweight $\mathbf{w}$. So

$$\Lambda = \bigoplus \Lambda_{\mathbf{w}} ,$$

where the direct sum is taken over all possible multiweights. If $\mathbf{u}$ and $\mathbf{v}$ are any two multiweights then $\Lambda_{\mathbf{u}}\Lambda_{\mathbf{v}} \leq \Lambda_{\mathbf{u}+\mathbf{v}}$, with addition of multiweights defined componentwise.

The Lie rings $E(r, p)$ and $W(r, p)$ are also multigraded. (As we shall see later it is still an open question whether $L(r, p)$ is always multigraded.) The Lie ring $E(r, p)$ is the free Lie ring of rank r in the variety of Lie rings determined by the identities $px = 0$, $xy^{p-1} = 0$, and $W(r, p)$ is the free Lie ring of rank r in the variety of Lie rings determined by the identities $px = 0$, $K_n = 0$ $(n \geq p)$. The precise form of the identities $K_n = 0$ does not concern us here, but for completeness we include a description of them. The reader is referred to [9] for details. First we need to introduce some notation. If $a_1, a_2, \ldots, a_n, b$ are elements of a Lie ring L, and if $S = \{i, j, \ldots, k\}$ is a subset of $\{1, 2, \ldots, n\}$ with $i < j < \cdots < k$, then we let

$$ba_S = ba_i a_j \cdots a_k.$$

(Here, and throughout this article, we are adopting a left-normed convention, so that $ba_i a_j \cdots a_k = (\cdots((ba_i)a_j)\cdots)a_k$.) Note that the element ba_S depends only on the elements $a_1, a_2, \ldots, a_n, b$ and on the subset S, but that its definition exploits the fact that S has a natural ordering. Now we let $x_1, x_2, \ldots$ be free generators of a free Lie ring of countably infinite rank, and for $n \geq p-1$ we let $K_{n+1}(x_1, x_2, \ldots, x_{n+1})$ be the element

$$\sum x_{n+1} x_{S(1)} x_{S(2)} \cdots x_{S(p-1)},$$

where the summation is taken over all ordered sequences of disjoint non-empty subsets $S(1), S(2), \ldots, S(p-1)$ with the property that $S(1) \cup S(2) \cup \cdots \cup S(p-1) = \{1, 2, \ldots, n\}$. (Each partition of $\{1, 2, \ldots, n\}$ into $p-1$ disjoint non-empty subsets contributes $(p-1)!$ terms to the sum, as the subsets in the partition are permuted among themselves.) Note that if $n < p-1$ then the summation is empty, and so $K_{n+1} = 0$ for $n < p-1$. Note also that if $n = p-1$ then the subsets $S(1), S(2), \ldots, S(p-1)$ in any term of the summation must all be one element subsets, and so $K_p(x_1, x_2, \ldots, x_p)$ can be expressed in the form

$$\sum x_p x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(p-1)},$$

with the summation taken over all permutations σ of $\{1, 2, \ldots, p-1\}$. Thus $K_p(y, y, \ldots, y, x) = (p-1)!xy^{p-1}$, so that the identities $px = 0$, $K_p = 0$ imply the $(p-1)$-Engel identity. On the other hand if we substitute x_p for x and $x_1 + x_2 + \cdots + x_{p-1}$ for y in xy^{p-1}, expand, and pick out the terms which are multilinear in $x_1, x_2, \ldots, x_p$ then we obtain K_p. So

the two identities $px = 0$, $xy^{p-1} = 0$ are equivalent to the two identities $px = 0$, $K_p = 0$.

The Lie ring $W(r, p)$ can be expressed in the form $\Lambda/(p\Lambda + I)$, where I is the ideal of Λ generated by elements of the form

$$K_n(a_1, a_2, \ldots, a_n) \qquad (n \geq p, a_1, a_2, \ldots, a_n \in \Lambda).$$

As we showed in [9], if we pick a subset B of Λ which spans Λ as a $\mathbb{Z}$-module, then I is spanned as a $\mathbb{Z}$-module by elements of the form

$$K_n(a_1, a_2, \ldots, a_n) \qquad (n \geq p, a_1, a_2, \ldots, a_n \in B).$$

Provided B consists only of multihomogeneous elements (such as products $y_1 y_2 \cdots y_i$ with $y_1, y_2, \ldots, y_i \in \{x_1, x_2, \ldots, x_r\}$) then this spanning set for I also consists only of multihomogeneous elements, and so I and $p\Lambda + I$ are multigraded ideals of Λ. It follows that $W(r, p)$ is also multigraded. Similarly, $E(r, p)$ can be expressed in the form $\Lambda/(p\Lambda + E)$, where E is the ideal of spanned as a $\mathbb{Z}$-module by the elements

$$K_p(a_1, a_2, \ldots, a_p) \qquad (a_1, a_2, \ldots, a_p \in B).$$

So $E(r, p)$ is also multigraded.

On the other hand, although $L(r, p)$ can be expressed as a quotient Λ/J for some graded ideal J of Λ, it is not known whether J is always multigraded, and so it is not know whether $L(r, p)$ is multigraded. Nevertheless $L(r, p)$ does have a graded structure only slightly weaker than a multigrading. Wall [12] calls it a functional grading. To see how this functional grading arises it is convenient to express $L(r, p)$ as a quotient $W(r, p)/K$, for some graded ideal K of $W(r, p)$. First we define the functional grading on $W(r, p)$, using the fact that $W(r, p)$ is multigraded.

We define an equivalence relation on the set of all possible multiweights by setting

$$(u_1, u_2, \ldots, u_r) \sim (v_1, v_2, \ldots, v_r)$$

if $\sum u_i = \sum v_i$ and if for each $i = 1, 2, \ldots, r$ either $u_i = v_i = 0$ or u_i and v_i are non-zero and $u_i = v_i$ modulo $p - 1$. If $\mathbf{w}$ is a multiweight then we let $[\mathbf{w}]$ be the equivalence class of $\mathbf{w}$ under this equivalence relation. We let $W_{\mathbf{w}}$ be the multihomogeneous component of $W(r, p)$ of multiweight $\mathbf{w}$, and we let $W_{[\mathbf{w}]}$ be the sum of all the multihomogeneous components $W_{\mathbf{v}}$ of $W(r, p)$ such that $\mathbf{v} \sim \mathbf{w}$. Clearly $W(r, p)$ is the direct sum of the components $W_{[\mathbf{w}]}$, and $W_{[\mathbf{u}]} W_{[\mathbf{v}]} \leq W_{[\mathbf{u}+\mathbf{v}]}$ for all multiweights $\mathbf{u}$ and $\mathbf{v}$. So $W(r, p)$ admits this functional grading, and we show that the ideal K also admits it, so that the functional grading on $W(r, p)$ induces a grading on $L(r, p)$.

https://doi.org/10.1017/S1446788700032407 Published online by Cambridge University Press

We let W_i be the homogeneous component of $W(r, p)$ of weight i, and we let K_i be the homogeneous component of K of weight i. So, letting L_i be the homogeneous component of $L(r, p)$ of weight i, we have $L_i = W_i/K_i$. (Sanov [8] proved that $K_i = \{0\}$ for $i = 1, 2, \ldots, 2p-2$, and Wall [11] proved that $K_{2p-1} = \{0\}$.) Any $\mathbb{Z}$-module endomorphism of W_1 induces a Lie ring endomorphism of $W(r, p)$. (This is because $W(r, p)$ is a free Lie ring in the variety of Lie rings determined by the identities $px = 0$, $K_n = 0$, and because the free generators of $W(r, p)$ generate W_1 as a $\mathbb{Z}$-module.) Similarly $\mathbb{Z}$-module endomorphisms of L_1 induce Lie ring endomorphisms of $L(r, p)$. To see this, suppose that $x_1, x_2, \ldots, x_r$ generate $B(r, p)$ and suppose that $a_i = x_i\gamma_2 \in L_1$ for $i = 1, 2, \ldots, r$. Let α be a $\mathbb{Z}$-module endomorphism of L_1, and let $b_i = a_i\alpha$ for $i = 1, 2, \ldots, r$. Pick elements $y_1, y_2, \ldots, y_r$ in $B(r, p)$ such that $b_i = y_i\gamma_2$ for $i = 1, 2, \ldots, r$, and let β be the endomorphism of $B(r, p)$ which maps x_i to y_i for $i = 1, 2, \ldots, r$. Then β induces endomorphisms on the terms of the lower central series of $B(r, p)$, and so β induces an endomorphism θ of $L(r, p)$. Clearly α is the restriction of θ to L_1.

So if α is any $\mathbb{Z}$-module endomorphism of W_1 then α induces an endomorphism θ of $W(r, p)$. Identifying W_1 with L_1, α also induces an endomorphism of $L(r, p)$, and it follows that the ideal K of $W(r, p)$ is invariant under the action of θ. We use this fact to show that K admits the functional grading of $W(r, p)$.

We need to show that K is a sum of components of the form $K \cap W_{[\mathbf{w}]}$. Since K is graded it is sufficient to show that each of the homogeneous components K_i of K is a sum of components of the form $K_i \cap W_{[\mathbf{w}]}$. So let $a \in K_i$. Then a can be expressed as a sum of products of the form $y_1y_2\cdots y_i$ with $y_1, y_2, \ldots, y_i$ elements of the free generating set $\{x_1, x_2, \ldots, x_r\}$ for $W(r, p)$. We express a in the form

$$a = a_0 + a_1 + \cdots + a_{p-1},$$

where a_0 is a sum of products $y_1y_2\cdots y_i$ which do not involve x_1, and where (for $j = 1, 2, \ldots, p-1$) a_j is a sum of products $y_1y_2\cdots y_i$ which have multiweight $(w_1, w_2, \ldots, w_r)$ with $w_1 > 0$ and $w_1 = j$ modulo $p-1$. We show that $a_j \in K_i$ for $j = 0, 1, \ldots, p-1$. First let θ be the endomorphism of $W(r, p)$ which maps x_1 to 0 and maps x_k to x_k for $k = 2, 3, \ldots, r$. Then $K_i\theta \leq K_i$, and so $a_0 = a\theta \in K_i$. This implies that $b = a_1 + a_2 + \cdots + a_{p-1} \in K_i$. Next let n be any integer in the range $1 \leq n \leq p-1$, and let θ_n be the endomorphism of $W(r, p)$ which maps x_1 to nx_1 and maps x_k to x_k for $k = 2, 3, \ldots, r$. Then using the fact that $W(r, p)$ has characteristic p we see that

$$b\theta_n = na_1 + n^2a_2 + \cdots + n^{p-2}a_{p-2} + a_{p-1} \in K_i.$$

https://doi.org/10.1017/S1446788700032407 Published online by Cambridge University Press

Once more using the fact that $W(r, p)$ has characteristic p, we see that $a_1, a_2, \ldots, a_{p-1}$ lie in the linear span of $b\theta_1, b\theta_2, \ldots, b\theta_{p-1}$, and so $a_1, a_2, \ldots, a_{p-1}$ all lie in K_i. We refer to $a_0, a_1, \ldots, a_{p-1}$ as the components of a which are p-homogeneous in x_1. We can then apply the same argument with the generator x_2 to each of the components $a_0, a_1, \ldots, a_{p-1}$, expressing each of them as a sum of components which lie in K_i and are p-homogeneous in x_2. Repeating this argument for each of the generators of $W(r, p)$ we eventually obtain an expression for a as a sum of components each of which lies in K_i, and each of which is p-homogeneous in all of the generators of $W(r, p)$. Each of these components lies in $W_{[\mathbf{w}]}$ for some $\mathbf{w}$. This completes the proof that K admits the functional grading on $W(r, p)$.

3. Proof of Theorem 1

The most straightforward way to prove Theorem 1 would be to use the nilpotent quotient algorithm for groups to compute the order of $R(3, 5)$. If the computation showed that the order was 5^{2282} then this would provide a proof that $L(3, 5) = W(3, 5)$. On the other hand if the computation showed that the order was less than 5^{2282} then this would provide a proof that $L(3, 5)$ is a proper quotient of $W(3, 5)$. However computing $R(3, 5)$ would entail many, many hours of CPU time and so it is worth investigating how the theory of Sections 1 and 2 can be used to simplify the computation required. This theory implies that $L(3, 5)$ can be expressed as a quotient $W(3, 5)/K$ for some functionally graded ideal K of $W(3, 5)$. To prove Theorem 1, we need to show that $K = \{0\}$, and to this end it is sufficient to show that $K_i \cap W_{[\mathbf{w}]} = \{0\}$ for all i and all multiweights $\mathbf{w}$. For $p = 5$, Sanov's result mentioned above implies that $K_i = \{0\}$ for $i = 1, 2, \ldots, 8$, and Wall's result implies that $K_9 = \{0\}$. Wall [12] provided a general criterion which (when satisfied) implies that $K_i = \{0\}$ for $1 \leq i \leq 3p - 3$. Havas, Newman, and Vaughan-Lee [3] confirmed that this criterion is satisfied for $r = 3$, $p = 5$, and so Wall's result implies that $K_i = \{0\}$ for $i = 1, 2, \ldots, 12$. It was also shown in [3] that the multihomogeneous component $W_{\mathbf{w}}$ of $W(r, 5)$ is trivial if any of the entries in $\mathbf{w}$ exceeds 6. Furthermore the computation of $W(3, 5)$ in [3] showed that it has class 17, which implies that its multihomogeneous component with multiweight $(6, 6, 6)$ is trivial. So to prove Theorem 1 it is sufficient to prove that $K_i \cap W_{[\mathbf{w}]} = \{0\}$ when $13 \leq i \leq 17$ and when $\mathbf{w} = (a, b, c)$ with $0 < a, b, c \leq 6$, $a + b + c = i$.

First consider the case when $i = 17$. There are three multiweights to consider: $(6, 6, 5)$, $(6, 5, 6)$, $(5, 6, 6)$. These three multiweights lie in

https://doi.org/10.1017/S1446788700032407 Published online by Cambridge University Press

different equivalence classes under the functional equivalence relation described in Section 2, and so if K_{17} were non-trivial it would have non-trivial intersection with one of the three multihomogeneous components of $W(3, 5)$ corresponding to these multiweights. But these three multihomogeneous components of $W(3, 5)$ all have order 5, and so if K_{17} had non-trivial intersection with one of these components then it would contain the whole component. But then, applying automorphisms of $W(3, 5)$ induced by permutations of the generators, we would see that K_{17} contained all three components $W_{(6,6,5)}$, $W_{(6,5,6)}$, $W_{(5,6,6)}$. So if K_{17} were non-trivial then it would equal the whole of W_{17}, and this would imply that $R(3, 5)$ had class at most 16. So to prove tht $K_{17} = \{0\}$ it is sufficient to establish the existence of some finite 3 generator group of exponent 5 with class 17.

Next consider the case when $i = 16$. The components of W with multiweight $(6, 6, 4)$, $(6, 4, 6)$, $(4, 6, 6)$ are all trivial and so once again there are only three multiweights to consider: $(6, 5, 5)$, $(5, 6, 5)$, $(5, 5, 6)$. These three multiweights also lie in different equivalence classes under the functional equivalence relation defined above, and the corresponding multihomogeneous components of $W(3, 5)$ also all have order 5. So, as in the case above, to prove that $K_{16} = \{0\}$ it is sufficient to establish the existence of some finite 3 generator group of exponent 5 with class 16.

The case when $i = 15$ is somewhat different. There are 10 multiweights to consider: $(6, 6, 3)$, $(6, 3, 6)$, $(3, 6, 6)$, $(6, 5, 4)$, $(6, 4, 5)$, $(5, 6, 4)$, $(5, 4, 6)$, $(4, 6, 5)$, $(4, 5, 6)$, $(5, 5, 5)$. Once again, these multiweights all lie in different equivalence classes under the equivalence relation defined above. The multihomogeneous components of $W(3, 5)$ corresponding to the first 3 of these multiweights are all trivial, and the components corresponding to the next 6 all have order 5. The component $W_{(5,5,5)}$ has order 25. The argument used asbove for the cases $i = 16, 17$ does not work here, but (using the presentation of $W(3, 5)$) we easily see that if a is a non-trivial element of W_{15} then ab is a nontrivial element of W_{16} for some $b \in W_1$ (in other words W_{15} has trivial intersection with the centre of $W(3, 5)$). So if K_{15} were non-trivial then K_{16} would also be non-trivial, and so using the case $i = 16$ above we see that to show that K_{15} is trivial it is sufficient to establish the existence of some finite 3 generator group of exponent 5 with class 16.

The arguments used above for $i = 15, 16, 17$ no longer apply for $i = 13, 14$. For example, the three multiweights $(6, 6, 2)$, $(6, 2, 6)$, $(2, 6, 6)$ are equivalent under the functional equivalence relation, and the corresponding multihomogeneous components of $W(3, 5)$ are non-trivial and lie in the centre of $W(3, 5)$. Nevertheless it is possible to show that $L(3, 5)$ does not satisfy any new relation involving these multiweights without computing the

full class 14 quotient of $R(3, 5)$. We can define the multiweight of a group commutator $[y_1, y_2, \ldots, y_i]$ in $R(3, 5)$ in the same way as we define the multiweight of a Lie product $y_1 y_2 \ldots y_i$ in $W(3, 5)$. If (a, b, c) is a multiweight we let $N(a, b, c)$ be the normal subgroup of $R(3, 5)$ generated by commutators with multiweight (d, e, f) where $d > a$ or $e > b$ or $f > c$. The Canberra version of the nilpotent quotient algorithm has an option which makes it possible to compute the quotient group $R(3, 5)/N(a, b, c)$ for any multiweight (a, b, c). The group $R(3, 5)/N(6, 6, 2)$ has class at most 14, and if it has non-trivial commutators of weight 14 then these must have multiweight $(6, 6, 2)$. So to show that $L(3, 5)$ does not satisfy any new relation involving products in $W(3, 5)$ with multiweight $(6, 6, 2)$ it is sufficient to show that the 14th term of the lower central series of $R(3, 5)/N(6, 6, 2)$ has the same order as $W_{(6,6,2)}$. (It should be noted that the computing resources required to compute $R(3, 5)/N(6, 6, 2)$ are considerably less than those required to compute $R(3, 5)$.) In this way it would be possible to perform a number of relatively short computations to show that K_{13} and K_{14} are trivial. We could then complete the proof that $K = \{0\}$ by establishing the existence of a finite 3 generator group of exponent 5 with class 17.

In the event, I combined these two approaches into one single computation. I used the Canberra version of the nilpotent quotient algorithm to compute $R(3, 5)/N(5, 6, 6)$. The computation gave a presentation for a three generator group G of exponent 5 with class 17 and order 5^{2180}. I also computed the quotient $W(3, 5)/I(5, 6, 6)$, where $I(5, 6, 6)$ is the ideal of $W(3, 5)$ generated by products with multiweight (d, e, f) with $d > 5$. This Lie ring also has class 17 and order 5^{2180} and it can be shown that it is the associated Lie ring of G. (A presentation for the associated Lie ring of G can be read off from the power commutator presentation obtained for G. The Lie ring presentation obtained in this way is identical to the presentation given for $W(3, 6)/I(5, 6, 6)$ by the nilpotent quotient algorithm for graded Lie rings.) It follows from this that $K \leq I(5, 6, 6)$. Now if v is a non-trivial element of $I(5, 6, 6)$ then there is an automorphism θ of $W(3, 5)$ induced by a permutation of its generators such that $v\theta \notin I(5, 6, 6)$. Since $K\theta = K$ this implies that $K = \{0\}$ and that $L(3, 5) = W(3, 5)$.

4. The computation

In this section we give some details of the computation. We assume that the reader is familiar with the Canberra version of the nilpotent quotient algorithm. We refer the reader to Havas and Newman [2] and Vaughan-Lee [9] for a description of the algorithm.

It might be thought that there was little to be gained in computing the quotient $R(3,5)/N(5,6,6)$ rather than $R(3,5)$ itself, since their orders are so close. In the event there probably was very little gain, and (as we shall see) there was some disadvantage. The main problem with computing groups as large as these is the amount of memory required to store the presentations. The presentation generated for $R(3,5)/N(5,6,6)$ takes up 18.4 megabytes of memory, and I estimate that a presentation for $R(3,5)$ would take up about 22 megabytes of memory. At intermediate stages of the computation much larger presentations can be generated. I estimate that the standard version of the Canberra nilpotent quotient algorithm would generate intermediate presentations needing up to 75 megabytes of memory in calculating $R(3,5)/N(5,6,6)$, and needing up to 100 megabytes in calculating $R(3,5)$. The computations described here were carried out with a disk allocation of 25 megabytes, and it would probably not have been possible to compute $R(3,5)$ within that allocation. We describe below some of the modifications which were made to the algorithm to save space and to speed up the computation.

The algorithm was modified so that the 5th powers of the power-commutator presentation generators were trivial in all presentations (including intermediate ones). This was achieved by not adding 'tails' to 5th powers when going from one class to the next. The collection routine was modified to exploit this, and a version of collection from the left was used in which the 5th powers of all power-commutator presentation generators were assumed to be trivial. (See [10] for a description of collection from the left.)

Fifth powers of normal words on the generators were computed by formula evaluation. The 5-covering group of $R(2,5)$ was computed, and $b^{-5}a^{-5}(ab)^5$ was calculated in this group (where a and b were the defining generators of the group). An expression for this element was obtained as a product of commutators of weight 5 or more in a and b. This expression was used as a formula for computing 5th powers of words in the power-commutator presentation generators. A normal word $w = a_i^{\alpha}\cdots a_j^{\beta}a_k^{\gamma}$ is expressed as a product uv where $u = a_i^{\alpha}\cdots a_j^{\beta}$ and $v = a_k^{\gamma}$. Then $v^{-5}u^{-5}(uv)^5$ is evaluated by substituting u for a and v for b in the formula. The resulting normal word is then treated as an extra relator of the group. The process is then iterated with u in place of w. (Since v is a power of a power-commutator generator, v^5 is always trivial.) In this way the 5th power of w and of a number of subwords of w are factored out of the group. This method is significantly faster than the method of concatenating 5 copies of w, and collecting the resulting word.

The intermediate presentations generated by the algorithm were prevented from growing too large as follows. When extending a class $c-1$ presentation

to a class c presentation, the Canberra NQA adds 'tails' to the commutators in the presentation in descending order of weight. It first adds 'tails' to weight c commutators, then performs the consistency checks of class c, then adds 'tails' to commutators of weight $c-1$ and performs consistency checks of class $c-1$, then adds 'tails' to commutators of weight $c-2$ and performs consistency checks of class $c-2$, and so on. But the standard Canberra NQA does not eliminate redundant generators after each consistency check as this is not normally necessary and can waste time. So the algorithm was modified to perform these extra eliminations and cut down the size of the presentations being generated. The algorithm was also modified to perform some exponent checking after each consistency check. After the consistency checks of class $c-r$ were performed the 5th power evaluation formula was applied to normal words $a_i^{\alpha} \ldots a_j^{\beta} a_k^{\gamma}$ where a_k had weight $c-r-4$. Since the formula only involves commutators of weight 5 or more, applying the formula to normal words of this type only involves 'tails' of weight $c-r$ or more.

The normal words used to enforce exponent 5 were chosen in the following way. The Felsch-Neubüser algorithm [1] was used to compute a set of representatives for the conjugacy classes of cyclic subgroups of the class 13 quotient of $R(3, 5)/N(5, 6, 6)$. The Felsch-Neubüser algorithm was not applied in full, so there was some redundancy in this set of representatives. The set of normal words used to enforce exponent 5 was taken to be the subset of this set of representatives consisting of words of weight at most 17. While constructing the presentations at each class it was sufficient to use enough normal words from this set to bring the order down to that predicted by the Lie ring computations. In this way a presentation for a group G of class 17 and order 5^{2180} was obtained. Next, letting x, y, z be the images in G of the free generators of $R(3, 5)$, I checked that G admitted automorphisms δ and ε given by $x\delta = x$, $y\delta = yz$, $z\delta = z$, and $x\varepsilon = x$, $y\varepsilon = z^2$, $z\varepsilon = y$. (The automorphisms were chosen to correspond to the generators $\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}0&2\\1&0\end{smallmatrix}\right]$ of GL(2, 5).) I then confirmed that G had exponent 5 by considering the action of the automorphism group $\langle \delta, \varepsilon \rangle$ on the test set of normal words previously obtained, and by evaluating the 5th power of one element out of each orbit of the test set under this action. All these 5th powers were trivial, and so this confirmed that G had exponent 5. I then completed the proof of Theorem 1 by verifying that $W(3, 5)/I(5, 6, 6)$ was the associated Lie ring of G. The final stage of the computation would certainly have been easier with a presentation for $R(3, 5)$, since then I would have been able to use automorphisms corresponding to generators of GL(3, 5). The idea of using automorphisms was suggested to me by M. F. Newman, who has used them in a similar way in computing groups of exponent 4.

References

[1] Volkmar Felsch and Joachim Neubüser, 'An algorithm for the computation of conjugacy classes and centralizers in p-groups', Lecture Notes in Computer Science 72 (Springer, Berlin, 1979), pp. 452–465.
[2] George Havas and M. F. Newman, 'Applications of computers to questions like those of Burnside', Lecture Notes in Mathematics 806 (Springer, Berlin, 1980), pp. 211–230.
[3] George Havas, M. F. Newman and M. R. Vaughan-Lee, 'A nilpotent quotient algorithm for graded Lie rings', *J. Symbolic Computation*, to appear.
[4] George Havas, G. E. Wall and J. W. Wamsley, 'The two generator restricted Burnside group of exponent five', *Bull. Austral. Math. Soc.* **10** (1974), 459–470.
[5] Graham Higman, 'On finite groups of exponent five', *Proc. Cambridge Philos. Soc.* **52** (1956), 381–390.
[6] E. I. Huhro, 'The associated Lie ring of the free two generator group of prime exponent, and the Hughes conjecture for two generator p-groups', *Mat. Sb.* **118** (1982), 567–575.
[7] A. I. Kostrikin, 'The Burnside problem', *Izv. Akad. Nauk SSSR Ser. Mat.* **23** (1959), 3–34.
[8] I. N. Sanov, 'Establishment of a connection between periodic groups with period a prime number and Lie rings', *Izv. Akad. Nauk SSSR Ser. Mat.* **16** (1952), 23–58.
[9] M. R. Vaughan-Lee, 'The restricted Burnside problem', *Bull. London Math. Soc.* **17** (1985), 113–133.
[10] M. R. Vaughan-Lee, 'Collection from the left', *J. Symbolic Computation*, to appear.
[11] G. E. Wall, 'On the Lie ring of a group of prime exponent', Lecture Notes in Mathematics 372 (Springer, Berlin, 1974), pp. 667–690
[12] G. E. Wall, 'On the Lie ring of a group of prime exponent II', *Bull. Austral. Math. Soc.* **19** (1978), 11–28.

Christ Church
Oxford OX1 1DP
England