UNIVERSAL ALGEBRA AND APPLICATIONS
BANACH CENTER PUBLICATIONS, VOLUME 9
PWN—POLISH SCIENTIFIC PUBLISHERS
WARSAW 1982

ON BASIC AND AXIOMATIC RANKS OF NILPOTENT VARIETIES OF LIE ALGEBRAS

JURI A. BAHTURIN

Department of Mechanics and Mathematics, Moscow State University, 117234, Moscow, U.S.S.R.

1. Introduction

In the present paper Lie algebra varieties are considered as determined over an arbitrary but fixed associative and commutative ring R with unity 1. Given any such variety $\boldsymbol{V}$, the number $r_a = r_a(\boldsymbol{V})$ is called the *axiomatic rank* of $\boldsymbol{V}$ if r_a is the least number for which $\boldsymbol{V}$ can be determined by a set of identical relations, each depending on at most r_a variables. Number r_b is referred to as the basic rank of $\boldsymbol{V}$ if r_b is the least possible number for which $\boldsymbol{V}$ is generated by its relatively free algebra $L_{r_b}(\boldsymbol{V})$ (or, in other words, is determined by identical relations holding in all its r_b-generator algebras). These definitions in the general setting of algebraic systems are given by A. I. Malcev in [7]. In a book by Hanna Neumann [8], Chapter 3, one can find some rather straight-forward theorems on these ranks (in the group theory setting) stating in particular that in the case of a group variety consisting of nilpotent groups of class c one has $r_a, r_b \leqslant c$. In a series of papers devoted to the basic rank of the variety $\boldsymbol{N}_c$ of all nilpotent groups of class $\leqslant c$ it was shown that $r_b(\boldsymbol{N}_c) = c-1$ (see, e.g., [5], [6], [10]).

Turning back to the varieties of Lie algebra, we remark that while the first of the above-mentioned results almost automatically transfers from group theory, attempts to prove an analogue of the second one soon lead to counter-examples. It turns out that the number $r_b(c, R)$ (that is, the basic rank of the variety $\boldsymbol{N}_c$ of all Lie algebras over R whose nilpotency class does not exceed c) essentially depends on the additive torsion in R. Namely, the following theorem (the main theorem in this paper) holds:

THEOREM 1. *Assume that c is an even number such that $c/2 = p^s$, the prime number p being the order of a nonzero element from R. Then $r_b(c, R) = c$. For all the remaining $c \geqslant 3$ one has $r_b(c, R) = c-1$.*

The main tool in the proof is the application of different bases of free Lie algebras (M. Hall [4], A. I. Širšov [9]). We shall repeatedly use the following

LEMMA 1. *The elements of the form*

$$(*)\qquad [x_1, x_{i_1}, x_{i_2}, \ldots, x_{i_n}], \quad 1 \neq i_1, i_2, \ldots, i_n \in \{2, 3, \ldots, m\}$$

constitute a free basis of a free R-submodule M of a free Lie algebra $L = L(\{x_1, x_2, \ldots, x_m\})$ generated by monomials of degree exactly 1 in x_1. [1]

The proof is carried out with the use of A. I. Širšov's basis of a free Lie algebra consisting of so-called basic nonassociative monomials, that is, nonassociative monomials obtained by the unique arrangement of brackets on the basic associative words a satisfying the condition $a = bc > cb$, the words being ordered lexicographically. It is easily seen that the associative supports of the elements from the system $(*)$ are basic, provided that the ordering is such that the element x_1 is the greatest one.

According to what is proved in the quoted paper of A. I. Širšov, any monomial w having form $(*)$ is representable as a linear combination of basic nonassociative monomials, the basic nonassociative monomial obtained by a unique arrangement of brackets in the associative support of w meeting with coefficient 1. Restricting ourselves to some finitely generated submodule of M (e.g. to its multihomogeneous components), we immediately obtain the conclusion of the lemma since the finite subsets of the set $(*)$ may be derived from the finite subsets of a free set of basic nonassociative monomials by using linear transformations with unitriangular matrices.

Of use in the sequel will also be the next lemma, evidently related to the one just proved.

LEMMA 2. *The following identity holds for any $(n+1)$-tuple of elements of an arbitrary Lie algebra:*

$$[a_0, a_1, a_2, \ldots, a_n] = \sum_{\substack{r+s=n \\ i_1 > \ldots > i_r \\ j_1 < \ldots < j_s}} (-1)^{r+1} [a_n, a_{i_1}, \ldots, a_{i_r}, a_0, a_{j_1}, \ldots, a_{j_s}].$$

The evident induction proof of the lemma is left to the reader.

Finally, before coming to the main sections of the paper, it is worth mentioning that the proof of the particular case of Theorem 1 where the base ring R has no additive torsion may be done in a simpler fashion by using the correspondence between the torsion free nilpotent groups and rational Lie algebras given by the Baker–Hausdorff formula, details of which can be found in paper [1] due to K. K. Andreev.

(1) The notation $[a, b, \ldots, c]$ shortens that of the so-called left-normed commutator $[[\ldots[a, b], \ldots], c]$.

2. Axiomatic rank

Remark firstly that just in the same manner as in the case of group varieties (see [8], 34.12 and 34.13) one can show that the identities of any class c nilpotent variety $\boldsymbol{V}$ of a Lie algebra over an arbitrary ring R follow from its identities in $\leqslant c$ variables and the identity

$$(1)\qquad [x_1, x_2, \ldots, x_c, x_{c+1}] \equiv 0.$$

Having this in mind, let us prove that (1) follows from a system of identities in c variables also valid in $\boldsymbol{V}$ and having the form

$$(2)\qquad [x_1, x_2, \ldots, \underset{i}{u}, \ldots, \underset{j}{u}, \ldots, x_c, x_{c+1}] \equiv 0.$$

We proceed by induction on c. If (2) with $c > 3$ holds in a Lie algebra A, then an analogous system of identities (with c changed to $c-1$) holds in $A/Z(A)$, $Z(A)$ being the centre of A. So it remains to apply the induction hypothesis and the theorem holds. The case $c = 3$, forming the base of the induction, should be dealt with separately. Namely, the linearization of identities in (2) by the variable u gives a skew symmetry of the left normed commutator of weight $c+1$ by any pair of arguments. On the other hand, the derivation rules (see also Lemma 2) imply the following relation:

$$[x_1, x_2, x_3, x_4] = -[x_4, x_1, x_2, x_3] + [x_4, x_2, x_1, x_3] + \\ + [x_4, x_3, x_1, x_2] - [x_4, x_3, x_2, x_1].$$

Interchanging the variables on the right and using the above-mentioned skew symmetry, one obtains $[x_1, x_2, x_3, x_4] = 0$. Thus we have proved the following

THEOREM 2. *The axiomatic rank $r_a(\boldsymbol{V})$ of any variety $\boldsymbol{V}$ of nilpotent Lie algebras of class $\leqslant c$ $(c \geqslant 3)$ over an arbitrary ring R satisfies the inequality $r_a(\boldsymbol{V}) \leqslant c$.*

The examples which follow show that the bound of Theorem 2 is, in a sense, the best possible.

EXAMPLE 1. Let $\boldsymbol{M}$ be the variety of Lie algebras considered in papers [2] and [3], the base ring being an arbitrary field of characteristic 2, and given by the laws

(i) $[x_1, x_2, [x_3, x_4]] \equiv 0$;
(ii) $[x_1, x_2, x_3, x_3] \equiv 0$;
(iii) $[x_1, x_2, x_1, x_2] \equiv 0$.

It was shown in [2] and [3] that $\boldsymbol{M}$ is nonnilpotent. Let us show that for any $c \geqslant 3$ any $(c-1)$-generator algebra in $\boldsymbol{M}$ is nilpotent of class $\leqslant c$. Just in the same way as in 34.52 from [8] one observes that it suffices to consider the cases $c = 3$ and $c = 4$. When $c = 4$ commutators of the form $[x_1, x_2, x_3, x_4, x_5]$, where only three different generators occur, should be taken into account. Using (ii) and having in mind the metabelian law (i), enabling us to interchange the variables starting from the third, we come to the commutator $[x_1, x_2, x_1, x_2, x_3]$ equal to zero by (iii). This identity, just used, plainly proves the case $c = 3$.

The preceding argument immediately shows that the identity of nilpotency (1) for no $c \geqslant 3$ follows from those depending on less than c variables, since otherwise $\boldsymbol{M}$ would be nilpotent. So the first example illustrating Theorem 2 is the variety $\boldsymbol{N}_c$, $c \geqslant 3$, over an arbitrary ring of characteristic 2. For this variety one has $r_a(\boldsymbol{N}_c) = c$.

EXAMPLE 2. Over an arbitrary ring R one has $r_a(\boldsymbol{N}_3) = 3$.

It is easily seen that the variety $\boldsymbol{N}_3^{(2)}$, that is, the variety determined by the 2-variable identities holding in $\boldsymbol{N}_3$, is in fact given by the laws

$$[x_1, x_2, x_2, x_2] \equiv 0 \quad \text{and} \quad [x_1, x_2, x_1, x_2] \equiv 0.$$

By linearization, we find the 3-variable identities of degree 4 holding in $\boldsymbol{N}_3^{(2)}$. Their multihomogeneous components of degree 1 in a, b and 2 in b have the form

(1) $[a, b, b, c] + [a, b, c, b] + [a, c, b, b] \equiv 0$;

(2) $[b, a, b, c] + [b, a, c, b] + [b, c, a, b] \equiv 0$;

(3) $[c, b, b, a] + [c, b, a, b] + [c, a, b, b] \equiv 0$;

(4) $[a, b, b, c] + [a, c, b, b] + [b, c, a, b] \equiv 0$;

(5) $[a, b, c, b] + [c, b, a, b] \equiv 0$;

(6) $[b, a, b, c] + [b, c, b, a] \equiv 0$;

(7) $[c, b, b, a] + [c, a, b, b] + [b, a, c, b] \equiv 0$.

Put $e = [a, b, b, c]$, $f = [a, b, c, b]$, $g = [a, c, b, b]$. These elements, by Lemma 1, form a basis of a corresponding multihomogeneous component, which (by using Lemma 2) enables us to rewrite identities (1)–(7)

in the form

(1) $e+f+g \equiv 0$; (2) $-4f+2g \equiv 0$; (3) $-e+3f+3g \equiv 0$;
(4) $e-f+2g \equiv 0$; (5) $2f-g \equiv 0$; (6) $-2f+g \equiv 0$;
(7) $-e+f-2g \equiv 0$.

Now one sees that the basis of the submodule of 3-variable identities of the described multidegree has the form

$$e+f+g \equiv 0 \quad \text{and} \quad 2f-g \equiv 0$$

or

$$[a, b, b, c] + [a, b, c, b] + [a, c, b, b] \equiv 0, \quad 2[a, b, c, b] - [a, c, b, b] \equiv 0.$$

This obviously gives $\boldsymbol{N}_3^{(2)} \neq \boldsymbol{N}_3$ if the characteristic of the base ring is different from 2. This case, however, has been considered in the previous example.

3. Basic rank

PROPOSITION 1. *Let $\boldsymbol{V}$ be a nilpotent Lie algebra variety all of whose members have class $\leqslant c$ over an arbitrary ring R. Then its basic rank $r_b(\boldsymbol{V})$ is not greater than c.*

We omit the proof since it is obtained, without even minor changes, from group variety theory (see [8], 35.11 and 35.12).

PROPOSITION 2. *Let S be the full symmetric group of the set $\{2, 3, \ldots, c\}$, $G_c = L_c(\boldsymbol{N}_c)$ a free algebra of $\boldsymbol{N}_c$ with free generators $a_1, a_2, \ldots, a_c$ and $G_{c-1} = L_{c-1}(\boldsymbol{N}_c)$ the same with the free generators $b_1, \ldots, b_{c-1}$. Denote by u the element*

$$u = \sum_{\sigma \in S} |\sigma| [a_1, a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(c)}] \tag{1}$$

of the algebra G_c, where $|\sigma|$ is the sign of σ. Then there exists a system of epimorphisms θ_i, δ_j, $i = 1, 2, \ldots, c-1$; $j = 1, 2, \ldots, c$ of G_c onto G_{c-1} the intersection of kernels of which belongs to the R-submodule of G_c spanned by u.

Proof. Define the epimorphisms θ_i and δ_j (see [5]) by putting

$$\theta_i(a_j) = \begin{cases} b_j, & \text{if } j \leqslant i; \\ b_{j-1}, & \text{if } j > i; \end{cases} \quad i = 1, 2, \ldots, c-1.$$

$$\delta_j(a_i) = \begin{cases} b_i, & \text{if } i < j; \\ 0, & \text{if } i = j; \\ b_{i-1}, & \text{if } i > j; \end{cases} \quad i = 1, 2, \ldots, c.$$

According to our notation, $T = \bigcap_{i=1}^{c-1} \operatorname{Ker}\theta_i \cap \bigcap_{j=1}^{c} \operatorname{Ker}\delta_j$.

Observe first that the elements from T are multilinear. Indeed, given an arbitrary element $v \in G_c$, one has

$$v = \sum a_{i_1 \ldots i_n} v_{i_1 \ldots i_n},$$

where $a_{i_1 \ldots i_n} \in R$ and $v_{i_1 \ldots i_n}$ is a linear combination of monomials each depending on each of the variables $a_{i_1}, \ldots, a_{i_n}$. If, say, $a_{i_1 \ldots i_n} \neq 0$ and $n \neq c$, there exists an $i \notin \{i_1, \ldots, i_n\}$. Apply δ_i to v. Then

$$0 = \delta_i(v) = \delta_i\Big(\sum_{\{i_1, \ldots, i_n\} \not\ni i} a_{i_1 \ldots i_n} v_{i_1 \ldots i_n}\Big).$$

But the sum in the brackets is an element of the subalgebra $\operatorname{alg}(\{a_1, \ldots \ldots, \hat{a}_i, \ldots, a_c\})$ and the restriction of δ_i to this subalgebra is injective. So far we have proved the multilinearity of $v \in T$ (the reader should keep in mind that G_c is nilpotent of class c (!)).

Now write the element $v \in T$ in the form

$$v = \sum_{\sigma \in S} a_\sigma [a_1, a_{\sigma(2)}, \ldots, a_{\sigma(c)}]. \tag{2}$$

This is possible because of Lemma 1 from the introduction. Apply θ_2 to v. By the definition of θ_2 one has $a_1 \mapsto b_1, a_2 \mapsto b_2, a_3 \mapsto b_2, \ldots, a_c \mapsto b_{c-1}$. Again using Lemma 2 (or, more precisely, its evident variant for the free nilpotent algebra), one sees that the images of all summands from (2) are basic in G_{c-1}, two different summands from (2) corresponding to σ' and $\sigma'' \in S$ mapping into the same basic monomial if and only if σ' and σ'' coincide up to a multiple of the form $(23)^s$, $s = 0, 1$. Therefore if $\sigma' = \sigma''(23)$ one has $a_{\sigma'} = -a_{\sigma''}$. Using the remaining θ_i, $i = 3, \ldots, c-1$, and the fact that any two permutations are linked by a chain of transpositions of the form $(j, j+1)$ one sees that $a_\sigma = \lambda|\sigma|$, where λ is a fixed element from R.

Before we formulate the next proposition, let us recall that by $\operatorname{var}(H)$ we denote the variety of Lie algebras generated by a Lie algebra H, that is, the least variety containing H.

PROPOSITION 3. *Let k be an integer such that $1 \leqslant k < c-1$ and G_r a free algebra of rank r in N_c, $c \geqslant 3$. Then $\operatorname{var}(G_k) \neq \operatorname{var}(G_{k+2})$.*

Proof. Make use of an identity from a paper by F. Levin [6]:

$$u_{k,c} = \sum_{\sigma \in S'} |\sigma| [x_1, x_{\sigma(2)}, \ldots, x_{\sigma(k+2)}, x_{k+3}, \ldots, x_c]. \tag{3}$$

Substituting into this identity the set of free generators among which at most k elements differ, one immediately obtains zero. But if we have $k+2$ different generators, then after the substitution

$$x_1 \mapsto y_1,\ x_2 \mapsto y_2,\ \ldots,\ x_{k+2} \to y_{k+2},\ \ldots,\ x_c \mapsto y_{k+2}$$

we obtain a linear combination of different monomials which are basic in the sense of Lemma 1, that is, we obtain a nonzero element of G_{k+2}.

From the above proposition and Proposition 1 one immediately deduces

$$c-1 \leqslant r_b(N_c) \leqslant c.$$

Using Proposition 2, one can also deduce that $r_b(c, R) = c-1$ if and only if $\varrho u \equiv 0$ is not an identical relation in $G_{c-1} = L_{c-1}(N_c)$, where u is defined by equality (1) and ϱ is an arbitrary nonzero element from R.

PROPOSITION 4. *If c is odd then $\varrho u \equiv 0$ is not identical relation in G_{c-1} for any $0 \neq \varrho \in R$.*

Proof. Induction by the degree of u plainly gives the relation

$$u = \sum_{\substack{\sigma \in S' \\ \sigma(2i) < \sigma(2i+1)}} |\sigma| \big[x_1 [x_{\sigma(2)}, x_{\sigma(3)}], [x_{\sigma(4)}, x_{\sigma(5)}], \ldots, [x_{\sigma(c-1)}, x_{\sigma(c)}]\big].$$

Put on the right $x_1 = b_1, x_2 = b_1, \ldots, x_{c-1} = b_{c-2}$, $x_c = b_{c-1}$ and order the variables $b_1, b_2, \ldots, b_{c-1}$ so that $b_1 > b_2 > \ldots > b_{c-1}$. In order to determine whether the value of u after this substitution equals zero we use Hall's usual basis. Having applied anticommutativity, we see that u is a linear combination of monomials depending on the free generators of the derived subalgebra of a free Lie algebra, exactly one of these generators having the form $[b_{\sigma(2)-1}, b_{\sigma(3)-1}, b_1]$. The monomials containing different free generators of this form being evidently linearly independent, it suffices to check up the nontriviality of a linear combination of monomials depending on some fixed group of free generators of the derived algebra, for example,

$$u_1 = [b_1, b_2, b_1], \quad u_2 = [b_3, b_4], \quad \ldots, \quad u_s = [b_{c-2}, b_{c-1}].$$

But the linear combination u' of the monomials depending on these variables has the form

$$u' = \sum_{(i_2, \ldots, i_s)} \pm [u_1, u_{i_2}, \ldots, u_{i_s}];$$

hence it is different from zero together with each its multiple $\varrho u'$, $0 \neq \varrho \in R$. This proves our proposition, for G_{c-1} is a free R-submodule of a free Lie algebra, in which all the calculations were carried out.

The case of even c is more difficult. Let d be a number such that $c = 2d$. Just as in the argument above, rewrite u in the form

$$u = \sum_{\substack{\sigma \in S' \\ \sigma(2i-1) < \sigma(2i)}} |\sigma| \big[x_1, x_{\sigma(2)}, [x_{\sigma(3)}, x_{\sigma(4)}], \ldots, [x_{\sigma(c-1)}, x_{\sigma(c)}]\big]. \tag{4}$$

Obviously the equating of any two letters from the set $x_2, \ldots, x_c$ annihilates u. Therefore, $\varrho u \equiv 0$ is an identity in G_{c-1} if and only if ϱu is annihilated by any substitution equating x_1 and one of the variables $x_2, \ldots, x_c$, say,

$$x_1 \mapsto b_1,\ x_2 \mapsto b_1,\ x_3 \mapsto b_2,\ \ldots,\ x_{c-1} \mapsto b_{c-1}.$$

As in Proposition 4, one sees that after this substitution the value of (4) may be written through the free generating system of the derived algebra. Let us order these variables so that $[b_1, b_2]$ is the largest element. We consider the summands from (4) depending only on the variables

$$[b_1, b_2],\ [b_1, b_3],\ [b_4, b_5],\ \ldots,\ [b_{c-2}, b_{c-1}],$$

which will be denoted by $u_1, u_2, u_3, \ldots, u_d$, respectively, while the sum of all monomials from (4) depending on all of them will obtain the notation u' as before. This sum is easily seen to have the form

$$(5)\qquad u' = \sum_{\mu \in S_{\{2,3,\ldots,d\}}} [u_1, u_{\mu(2)}, u_{\mu(3)}, \ldots, u_{\mu(d)}] - \sum_{\nu \in S_{\{1,3,\ldots,d\}}} [u_2, u_{\nu(1)}, u_{\nu(3)}, \ldots, u_{\nu(d)}].$$

Using Lemma 1, consider the summands of the first sum as forming a basis and try to express the second sum through this basis.

LEMMA 3. *Denote by* e_μ *the monomial of the form*

$$e_\mu = [u_1, u_{\mu(2)}, u_{\mu(3)}, \ldots, u_{\mu(d)}]$$

and put $r = \mu^{-1}(2)$. *Then* e_μ *enters into* u' *with the coefficient*

$$(6)\qquad n_r = 1 + (-1)^r \binom{d-1}{r-1}.$$

Proof. Consider an arbitrary summand

$$h_\nu = [u_2, u_{\nu(1)}, u_{\nu(2)}, \ldots, u_{\nu(d)}]$$

of the second sum in (5) and put $q = \nu^{-1}(1)$. Using Lemma 2 from the introduction, rewrite h_ν in the form

$$(7)\qquad h_\nu = -\sum (-1)^m [u_1, u_{\nu(i_1)}, u_{\nu(i_2)}, \ldots, u_{\nu(i_m)}, u_2, u_{\nu(j_1)}, \ldots \\ \ldots, u_{\nu(j_{q-1-m})}, u_{\nu(q+1)}, \ldots, u_{\nu(d)}],$$

where $i_1 > i_2 > \ldots > i_m$, $j_1 < j_2 < \ldots < j_{q-1-m}$, $\{i_1, \ldots, i_m, j_1, \ldots, j_{q-1-m}\} = \{1, 3, \ldots, q\}$. On the right-hand side of (7) each summand has form e_μ for a certain μ. It is easily seen that if e_μ occurs in some h_ν it occurs with the coefficient $(-1)^{r+1}$. Moreover, in the summand h_ν with $q < r$ the monomial e_μ evidently does not occur. If $q \geqslant r$ then the number of h_ν whose

basic expression (7) essentially depends on e_μ equals $\binom{q-2}{r-2}$. Hence the sum of coefficients at all these summands depends only on r and is equal to

$$\hat{n}_r = (-1)^r\left(\binom{r-2}{r-2} + \binom{r-1}{r-2} + \ldots + \binom{d-2}{r-2}\right) \\ = (-1)^r\left(\binom{r-1}{r-1} + \binom{r-1}{r-2} + \binom{r}{r-2} + \ldots + \binom{d-2}{r-2}\right) \\ = (-1)^r\left(\binom{r}{r-1} + \binom{r}{r-2} + \ldots + \binom{d-2}{r-2}\right) = (-1)^r\binom{d-1}{r-1}.$$

Taking into account that e_μ enters in the first sum with the coefficient 1, we obtain the promised formula (6).

Now we are in a position to prove the main theorem.

Proof of Theorem 1. The case of odd c being exhausted by Proposition 3, we suppose c even. From the argument preceding Lemma 3 we immediately observe that $\varrho u \equiv 0$ is an identity in G_{c-1} if and only if $\varrho u' = 0$ for a certain $\varrho \neq 0$. But

$$(8)\qquad u' = \sum_{r=2}^{d} n_r \sum_{\mu^{-1}(2)=r} e_\mu$$

where e_μ form a part of a free basis of the R-module G_{c-1}. Therefore, to obtain the equality $\varrho u = 0$, it is necessary and sufficient to find $0 \neq \varrho \in R$ such that $n_r \varrho = 0$ for all $r = 2, \ldots, d$. To solve this problem note first that

$$(9)\qquad n_{r+1} = 1 + (-1)^{r+1}\binom{d-1}{r} = 1 + (-1)^{r+1}\left(\binom{d}{r} - \binom{d-1}{r-1}\right) \\ = (-1)^{r+1}\binom{d}{r} + n_r.$$

(i) Assume $c/2 = d = p^s$, p being a prime. Arguing by induction on r, we prove that $p \mid n_r$. For $r = 2$ one has $n_2 = 1 + \binom{d-1}{1} = d$. Further, since $\binom{d}{r} = \binom{p^s}{r}$ is always divisible by p, the relation (9) enables us to make the induction step for any $r < d$. Show now that the greatest common divisor of all n_r, $r = 2, \ldots, d$ equals p. Its being a p-power follows from $n_2 = d$. On the other hand, for a certain r $\binom{d}{r}$ is not divisible by p: if $d = p^s$ it suffices to put $r = p^{s-1}$, in which case

$$\binom{d}{r} = \frac{(p^s)!}{(p^{s-1})!\,(p^{s-1}(p-1))!}.$$

It is well known that the power t to which p enters into the canonical decomposition of $m!$ may be found by the formula

$$t = \left[\frac{m}{p}\right]+\left[\frac{m}{p^2}\right]+\dots+\left[\frac{m}{p^v}\right]+\dots,$$

where $[a]$ is the integer part of a. Taking it into account, one sees that for the numerator this number is $(p^s-1)/(p-1)$ and for the denominator it is $(p^{s-1}-1)/(p-1)+(p^{s-1}-1)(p-1)/(p-1)$. The difference of these two numbers being equal to 1 proves that $\binom{d}{r} = \binom{p^s}{p^{s-1}}$ is not divisible by p^2. Now (9) shows that for some r also $p^2 \nmid n_r$. Therefore, in case (i), G_{c-1} satisfies the identity not holding in G_c if and only if R contains some element of the additive exponent p.

(ii) Secondly, assume that $d = c/2$ is divisible by two different primes p and q. In this case the greatest common divisor of numbers $n_2, \dots, n_d$ is trivial. Indeed, $n_2 = d$ is divisible by both p and q, and $\binom{d}{r}$ for suitable choices of r is not divisible by either (this can be proved exactly as in (i)). Hence to obtain the conclusion on the greatest common divisor of $n_2, \dots, n_d$ it remains to make use of (9). Applying formula (8), one sees that $\varrho u' \neq 0$ for any $\varrho \neq 0$ and therefore $\varrho u \equiv 0$ is not a law in G_{c-1} for any $0 \neq \varrho \in R$.

This completes the proof of the main theorem.

References

[1] K. K. Andreev, *Nilpotent groups and Lie algebras* (Russian), Algebra i Logika 7 (1969), 4–14.

[2] V. A. Artamonov, *Chain varieties of linear algebras* (Russian), Trudy Moscov. Mat. Obšč. 29 (1973), 51–77.

[3] Ju. A. Bahturin and A. Ju. Ol'sanskiĭ, *Soluble just-non-cross varieties of Lie algebras* (Russian), Mat. Sb. 100 (1976), 384–399.

[4] M. Hall, jr., *A basis for free Lie rings and higher commutators in free groups*, Proc. Amer. Math. Soc. 1 (1950), 575–581.

[5] L. G. Kovács, M. F. Newman, and P. F. Pentony, *Generating groups of nilpotent varieties*, Bull. Amer. Math. Soc. 74 (1968), 968–971.

[6] F. Levin, *On torsion free nilpotent varieties*, Comm. Pure Appl. Math. 26 (1973), 757–765.

[7] A. I. Malcev, *Algebraic systems*, Nauka, Moscow 1976.

[8] Hanna Neumann, *Varieties of groups*, Springer-Verlag, Berlin 1967.

[9] A. I. Širšov, *On free Lie rings* (Russian), Mat. Sb. 45 (1958), 113–122.

[10] M. R. Vaughan-Lee, *Generating groups of nilpotent varieties*, Bull. Austral. Math. Soc. 3 (1970), 145–154.

Presented to the Semester
Universal Algebra and Applications
(February 15 – June 9, 1978)

UNIVERSAL ALGEBRA AND APPLICATIONS
BANACH CENTER PUBLICATIONS, VOLUME 9
PWN–POLISH SCIENTIFIC PUBLISHERS
WARSAW 1982

A COMPLETENESS THEOREM IN THE MODAL LOGIC OF PROGRAMS*

KRISTER SEGERBERG

Åbo Academy, Åbo, Finland

As its name would seem to indicate, the modal logic of programs is, or can be viewed as, a generalization of classical modal logic. In spite of this fact there has been little interaction so far between the two fields. One wonders whether this is accidental, or whether there is a deeper explanation. For it may be that modal logicians and computer scientists are interested in rather different questions, or that already from the outset the modal logic of programs is headed for goals that lie beyond the limited territories of classical modal logic — the increased complexity of the former allows, even invites, such development, and application will probably demand it.

However this may be, it seems to the author that, at least in its present formative state, the modal logic of programs is truly a generalization of classical modal logic, and that the methods of the old discipline can be brought to bear on at least some of the basic problems in the emerging one. To give some substance to this claim we shall prove in this paper a completeness theorem of the kind of which there have been so many in modal logic. The theorem is interesting in its own right, but the main point is perhaps that the proof is achieved by a method that has been standard in modal logic for many years — the canonical models/filtrations technique, due originally to Dana Scott and others.

* The contents of this paper were presented in three lectures that the author delivered at the Stefan Banach International Mathematical Center in Warsaw on March 7 and 10, 1978. The author wishes to thank Professor H. Rasiowa, Dr T. Traczyk, and his other Polish hosts for a both pleasant and profitable visit to the Center, and Professor S. K. Thomason who was also there and discussed the lectures with him. He also wishes to record his thanks to Professors Rohit Parikh and, especially, Vaughan Pratt for valuable discussions and for the generous way in which they have shared with him their ideas on the modal logic of programs.

Part of the early work on the paper was supported by a grant (*stipendium för längre hunna vetenskapsidkare*) from the Academy of Finland.