

# RESIDUALLY FINITE VARIETIES OF NONASSOCIATIVE ALGEBRAS

KEITH A. KEARNES AND YOUNG JO KWAK

ABSTRACT. We prove that if  $\mathcal{V}$  is a residually finite variety of nonassociative algebras over a finite field, and the enveloping algebra of each finite member of  $\mathcal{V}$  is finitely generated as a module over its center, then  $\mathcal{V}$  is generated by a single finite algebra.

## 1. INTRODUCTION

A variety  $\mathcal{V}$  of algebraic structures has *residual character*  $\kappa$  if  $\kappa$  is the least cardinal such that  $|S| < \kappa$  for every subdirectly irreducible (= SI) member  $S \in \mathcal{V}$ . Write  $\chi_{\mathcal{V}} = \kappa$  to denote that  $\mathcal{V}$  has residual character  $\kappa$  and write  $\chi_{\mathcal{V}} = \infty$  if there is no cardinal bound on the size of the SI's in  $\mathcal{V}$ .  $\mathcal{V}$  is *residually finite* if  $\chi_{\mathcal{V}} \leq \omega$ , or equivalently if all SI members of  $\mathcal{V}$  are finite.

In [11], Olshanskii described all residually finite varieties of groups. His main result can be split into two theorems:

**Theorem I** A residually finite variety of groups is generated by a single finite group.

**Theorem II** A finite group  $G$  generates a residually finite variety if and only if  $G$  is an  $A$ -group (i.e. iff  $G$  has abelian Sylow subgroups).

Analogous theorems were proved in [12] for varieties of Lie algebras over finite fields of characteristic  $\geq 5$  by Premet and Semenov. Namely, they showed that a residually

---

1991 *Mathematics Subject Classification*. Primary: ; Secondary:  
*Key words and phrases*.

finite variety of Lie algebras over a finite field of characteristic  $\geq 5$  is generated by a single finite Lie algebra, and that a finite Lie algebra  $L$  over a finite field of characteristic  $\geq 5$  generates a residually finite variety if and only if  $L$  is an  $A$ -algebra (i.e., iff the nilpotent subalgebras of  $L$  are abelian). In this paper we prove a theorem that has as corollaries the results of Olshanskii and of Premet and Semenov, and moreover completes the results of Premet and Semenov by being applicable in characteristics 2 and 3.

The focus of this paper is the proof of a generalization of Theorem I, so we discuss the generalization of Theorem II now. McKenzie has proved that the problem of determining which finite algebraic structures generate residually finite varieties is undecidable in general (cf. [8, 9]), but, in separate collaborations with Freese and Hobby, he has shown it to be decidable in certain restricted settings. For example, if one combines the main result of [1] with Theorems 9.8 and 10.4 of [3] and with the main result from [6], then one obtains the following decidability results: if  $B$  is a finite algebraic structure and  $\mathcal{V}$  is the variety it generates, then (1) it is decidable whether there is a nontrivial lattice identity valid in the congruence lattices of all members of  $\mathcal{V}$ , and (2) if such an identity is satisfied, then it is decidable whether  $\mathcal{V}$  is residually finite. Of particular relevance to this paper is the fact that any finite algebra with underlying group structure generates a variety whose members have modular congruence lattices, so by (2) it is decidable whether such algebras generate residually finite varieties. The decision procedure, due to Freese and McKenzie, can be easily described. If  $\mathcal{V}$  is a variety whose members have modular congruence lattices, then there is an analogue of the group commutator defined on all congruence lattices of algebras in the variety (cf. [2]). The Freese-McKenzie result is that if  $B \in \mathcal{V}$  is finite, then  $B$  generates a residually finite variety iff every subalgebra  $C \leq B$  satisfies

the commutator identity

$$(C1) \quad \alpha \cap [\beta, \beta] = [\alpha \cap \beta, \beta].$$

Here the commutator is applied to congruences of the subalgebra  $C$ . Condition (C1) implies that nilpotent congruences on  $C$  are abelian (as one may deduce by taking  $\alpha = [\beta, \beta]$ ), hence if subalgebras of  $B$  satisfy (C1) then each subalgebra of  $B$  is an  $A$ -algebra. The converse does not hold for general algebraic structures, or even for nonassociative algebras over a field. For example, if we define a 3-dimensional nonassociative algebra over a finite field by specifying the multiplication on basis elements  $e, f$  and  $g$  to be

	$e$	$f$	$g$
$e$	0	0	0
$f$	0	$g$	$e$
$g$	0	$e$	$f$

then this is an  $A$ -algebra that fails (C1), hence it is a finite  $A$ -algebra that fails to generate a residually finite variety. (For a failure of (C1), let  $\alpha$  be the congruence associated to the ideal  $(e)$  and let  $\beta$  be the congruence associated to the ideal  $(e, f, g)$ . Then  $\alpha \cap [\beta, \beta] = \alpha \neq 0 = [\alpha \cap \beta, \beta]$ .) The general form of Theorem II should therefore not be stated in terms of  $A$ -algebras, but rather in terms of (C1):

**Theorem II'** ([1]) A finite algebraic structure  $B$  in a variety with modular congruence lattices generates a residually finite variety if and only if the subalgebras of  $B$  satisfy the commutator identity (C1).

Henceforth we concentrate only on an analogue of Theorem I. The algebras that interest us will be called “generalized nonassociative algebras of finite type”. Namely

$A = \langle A; +, -, 0, F_1, F_2, \dots \rangle$  will be a *generalized nonassociative algebra* if  $\langle A; +, -, 0 \rangle$  is a group (not necessarily commutative) and each additional operation  $F_i(x_1, \dots, x_n)$  is multilinear in the sense that for each  $j$  and for any elements  $a_1, \dots, a_n \in A$  the polynomial  $F_i(a_1, \dots, a_{j-1}, x, a_{j+1}, \dots, a_n)$  is an endomorphism of  $\langle A; +, -, 0 \rangle$ . A generalized nonassociative algebra has *finite type* if it is the expansion of a group by finitely many multilinear operations. Thus, groups themselves are generalized nonassociative algebras of finite type, as are ordinary nonassociative algebras over finite fields. Certain other types of algebras, like modules over finitely generated rings, may be considered to be generalized nonassociative algebras of finite type after a change of language.

Our main theorem is that if  $\mathcal{V}$  is a residually finite variety of generalized nonassociative algebras of finite type, then  $\mathcal{V}$  is generated by a single finite algebra iff the enveloping ring of any finite algebra in  $\mathcal{V}$  is a finitely generated module over its center. The condition on the enveloping rings of finite algebras will be seen to hold for varieties of groups, varieties of associative rings, and varieties of Lie algebras over a finite field of any characteristic.

## 2. PRELIMINARIES

A generalized nonassociative algebra that is a group with no additional operations will be called a *pure group*. If  $A = \langle A; +, -, 0, F_1, F_2, \dots \rangle$  is a generalized nonassociative algebra, then  $A^\circ = \langle A; +, -, 0 \rangle$  is the *underlying pure group*.

**Definition 2.1.** If  $A$  is a generalized nonassociative algebra, then an *ideal* of  $A$  is a subset  $U \subseteq A$  such that

- (i)  $U$  is a normal subgroup of  $A^\circ$ , and

(ii) if  $F$  is an additional multilinear operation of  $A$  and  $a_1, \dots, a_n \in A$ , then

$$F(a_1, \dots, a_n) \in U \text{ whenever } a_i \in U \text{ for at least one } i.$$

The ideal  $\{0\}$  may be written  $0$ .

**Lemma 2.2.** *The map  $\theta \mapsto 0/\theta$  that assigns to a congruence its 0-class is an order preserving bijection from congruences to ideals. The ideals of  $A$  form complete sublattice of the lattice of normal subgroups of  $A^\circ$ .*

*Proof.* Routine. □

Next we turn to ideal generation.

**Definition 2.3.** If  $A$  is a generalized nonassociative algebra with additional multilinear operations  $F_1, F_2, \dots$ , then a *basic translation* is a polynomial of the form

$$T_{\mathbf{c}}^{(i,j)}(x) = F_i(c_1, \dots, c_{j-1}, x, c_{j+1}, \dots, c_n)$$

where  $\mathbf{c} = (c_1, \dots, c_n) \in A^n$  and the superscripts on  $T_{\mathbf{c}}^{(i,j)}$  indicate which operation symbol and variable are involved. The *type* of a basic translation  $T_{\mathbf{c}}^{(i,j)}$  is the symbol  $T^{(i,j)}$ .

A *k-translation* is a composition of  $k$  basic translations. The identity polynomial is taken to be the only 0-translation. A *k-translate* of  $a \in A$  is an element obtained from  $a$  by applying a  $k$ -translation. A *translation* is a  $k$ -translation for some  $k$ , and a *translate* is a  $k$ -translate for some  $k$ .

Note now for later use that in a variety of generalized nonassociative algebras of finite type there are only finitely many types of basic translations.

**Lemma 2.4.** *If  $Z \subseteq A$ , then the ideal of  $A$  that is generated by  $Z$  is the normal subgroup of  $A^\circ$  that is generated by the elements obtained from  $Z$  by translation.*

*Proof.* Let  $U$  be the ideal generated by  $Z$  and let  $V$  be the the normal subgroup of  $A^\circ$  that is generated by the elements obtained from  $Z$  by translation. Ideals have been defined so that they are normal subgroups closed under translation, hence  $Z \subseteq V \subseteq U$ . Conversely, it follows from the multilinearity of the additional operations that  $V$  is closed under translation, hence is an ideal. Thus  $U = V$ .  $\square$

**Definition 2.5.** If  $U, V \subseteq A$  are ideals of  $A$ , then their *commutator* is the least ideal  $[U, V]$  of  $A$  containing all elements of the form

- (i) commutator elements of the underlying pure group,  $(-u) + (-v) + u + v$ , for  $u \in U$  and  $v \in V$ .
- (ii) Elements  $F(a_1, \dots, a_n)$  for any multilinear additional operation  $F$ , provided there exist  $i \neq j$  such that  $a_i \in U$  and  $a_j \in V$ .

**Lemma 2.6.** *The commutator of Definition 2.5 is the translation of the the modular commutator defined in [2] into the context of generalized nonassociative algebras and the language of ideals.*

*Proof.* Let  $\theta_U$  denote the congruence on  $A$  whose classes are the cosets of the ideal  $U$ . The lemma asserts that  $[\theta_U, \theta_V] = \theta_{[U, V]}$ .

We establish the inclusion  $\theta_{[U, V]} \subseteq [\theta_U, \theta_V]$  first. If  $s(x, y) = (-x) + (-y) + x + y$ ,  $t(x, y) = F(c_1, \dots, c_{i-1}, x, c_{i+1}, \dots, c_{j-1}, y, c_{j+1}, \dots, c_n)$ ,  $u \in U$  and  $v \in V$ , then the matrices

$$\begin{bmatrix} s(0, 0) & s(0, v) \\ s(u, 0) & s(u, v) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & s(u, v) \end{bmatrix}$$

and

$$\begin{bmatrix} t(0, 0) & t(0, v) \\ t(u, 0) & t(u, v) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & t(u, v) \end{bmatrix}$$

suffice to show that the generators identified in Definition 2.5 (i) & (ii) are congruent to zero modulo the commutator of congruences, so  $\theta_{[U,V]} \subseteq [\theta_U, \theta_V]$ .

Now we prove the reverse inclusion. Our commutator of ideals  $U$  and  $V$  is an ideal generated by all “products”,  $b(u, v)$ , where  $b(x, y) = s(x, y)$  or  $t(x, y)$  is a binary polynomial of a certain form, and  $u \in U, v \in V$ . This kind of definition is preserved in passing to quotients in the sense that in  $A/[U, V]$  the images of  $U$  and  $V$  have trivial commutator. The commutator of congruences is preserved and reflected by passing to quotients, so we only need to show that if  $[U, V] = 0$ , then  $[\theta_U, \theta_V] = 0$ . For this we use the criterion of Exercise 6.7 of [2]. Assume that  $[U, V] = 0$  in  $A$ . Then condition (i) of Definition 2.5 implies that the group commutator  $[U, V]$  is zero in  $A^\circ$ , while condition (ii) implies that  $F(c_1, \dots, u, \dots, v, \dots, c_n) = 0$  whenever  $F$  is an additional multilinear operation and  $u \in U, v \in V$ . Let  $A \times_u A \times_v A$  be the subalgebra of  $A^3$  consisting of tuples  $(u + w, w, v + w)$  where  $u \in U, v \in V, w \in A$ . The criterion we will use is that  $[\theta_U, \theta_V] = 0$  holds iff

$$(2.1) \quad x - y + z: A \times_u A \times_v A \rightarrow A: (u + w, w, v + w) \mapsto u + v + w$$

is a homomorphism. The fact that the group commutator  $[U, V]$  is zero in  $A^\circ$  implies that  $x - y + z$  respects the additive structure, so we only need to show that  $x - y + z$  respects each multilinear operation  $F$ .

We shall need an identity that describes the expansion by multilinearity of  $F(\mathbf{x} + \mathbf{y}) := F(x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$ . Expanding on each place from left to right we

get

$$\begin{aligned}
F(\mathbf{x} + \mathbf{y}) &= F(x_1, \mathbf{x}' + \mathbf{y}') + F(y_1, \mathbf{x}' + \mathbf{y}') \\
&= (F(x_1, x_2, \mathbf{x}'' + \mathbf{y}'') + F(x_1, y_2, \mathbf{x}'' + \mathbf{y}'')) \\
&\quad + (F(y_1, x_2, \mathbf{x}'' + \mathbf{y}'') + F(y_1, y_2, \mathbf{x}'' + \mathbf{y}'')) \\
&= \dots .
\end{aligned}$$

After this expansion is completed, assign to each summand on the right the binary number obtained by replacing each  $x_i$  with 0 and each  $y_j$  with 1. Thus, for example, when  $n = 5$ , a summand of the form  $F(x_1, y_2, y_3, x_4, x_5)$  will be assigned 01100. Every binary number of length  $n$  will occur exactly once in this way, and since we are expanding from left to right it is easy to see that all binary numbers occur in lexicographic ordering. In particular, the first summand of the completed expansion will be the one that is assigned  $00 \cdots 0$ , namely  $F(\mathbf{x}) = F(x_1, x_2, \dots, x_n)$ , and the last one will be the one that is assigned  $11 \cdots 1$ , namely  $F(\mathbf{y}) = F(y_1, y_2, \dots, y_n)$ . We write this expansion identity as

$$(2.2) \quad F(\mathbf{x} + \mathbf{y}) = \left( \sum_{\text{lex}} F(\mathbf{x}/\mathbf{y}) \right) + F(\mathbf{y}).$$

That is, we abbreviate the lexicographic sum of the first  $2^n - 1$  terms and separate out the last term.

Now we return to the problem of showing that (2.1) is a homomorphism. This requires showing that

$$F(\mathbf{u} + \mathbf{w}) - F(\mathbf{w}) + F(\mathbf{v} + \mathbf{w}) = F(\mathbf{u} + \mathbf{v} + \mathbf{w})$$



whenever  $\mathbf{u} \in U^n, \mathbf{v} \in V^n$ . This is best approached by first subtracting  $F(\mathbf{w})$  from the right of both sides:

$$(F(\mathbf{u} + \mathbf{w}) - F(\mathbf{w})) + (F(\mathbf{v} + \mathbf{w}) - F(\mathbf{w})) = (F(\mathbf{u} + \mathbf{v} + \mathbf{w}) - F(\mathbf{w})).$$

Applying expansion identity (2.2) with  $\mathbf{y} = \mathbf{w}$  we reduce our problem to that of establishing

$$\sum_{\text{lex}} F(\mathbf{u}/\mathbf{w}) + \sum_{\text{lex}} F(\mathbf{v}/\mathbf{w}) = \sum_{\text{lex}} F((\mathbf{u} + \mathbf{v})/\mathbf{w}).$$

In the multilinear expansion of  $\sum_{\text{lex}} F((\mathbf{u} + \mathbf{v})/\mathbf{w})$  the terms that involve both  $u_i$  and  $v_j$  are zero, because  $[U, V] = 0$ , so this expansion is just  $\sum_{\text{lex}} (F(\mathbf{u}/\mathbf{w}) + F(\mathbf{v}/\mathbf{w}))$ . Elements of ideal  $U$  commute with elements of ideal  $V$ , since  $[U, V] = 0$ , so we can separate this sum into two sums while preserving the lex ordering to obtain

$$\sum_{\text{lex}} F((\mathbf{u} + \mathbf{v})/\mathbf{w}) = \sum_{\text{lex}} (F(\mathbf{u}/\mathbf{w}) + F(\mathbf{v}/\mathbf{w})) = \sum_{\text{lex}} F(\mathbf{u}/\mathbf{w}) + \sum_{\text{lex}} F(\mathbf{v}/\mathbf{w}).$$

Thus,  $[U, V] = 0$  implies  $[\theta_U, \theta_V] = 0$ , as desired.  $\square$

**Lemma 2.7.** *If  $W, Z \subseteq A$  are subsets and  $U = \langle W \rangle$  and  $V = \langle Z \rangle$  are the ideals they generate, then  $[U, V] = 0$  iff*

- (i) *every conjugate of a translate of an element of  $W$  commutes with every conjugate of a translate of an element of  $Z$ , and*
- (ii) *for every  $w \in W, z \in Z$ , translations  $T_1, T_2$ , multilinear operation  $F$ , places  $i \neq j$ , and elements  $\mathbf{c} \in A^n$  it is the case that*

$$F(c_1, \dots, T_1(w), \dots, T_2(z), \dots, c_n) = 0$$

*when  $T_1(w)$  and  $T_2(z)$  are substituted in places  $i$  and  $j$ .*

*Proof.* It follows from Definition 2.5 that  $[U, V] = 0$  iff elements of  $U$  commute with elements of  $V$  and  $F(c_1, \dots, u, \dots, v, \dots, c_n) = 0$  whenever  $u \in U$  and  $v \in V$ . By Lemma 2.4,  $U$  is the subgroup of  $A^\circ$  generated by the conjugates of translates of elements of  $Z$  and  $V$  is the subgroup generated by the conjugates of translates of elements of  $W$ . Thus, item (i) of this lemma is equivalent to the statement that elements of  $U$  commute with elements of  $V$ . Since  $F$  is multilinear, item (ii) is equivalent to the statement that  $F(c_1, \dots, u, \dots, v, \dots, c_n) = 0$  whenever  $u \in U$  and  $v \in V$ .  $\square$

### 3. RESIDUALLY FINITE VARIETIES

Our goal is to prove  $\chi_{\mathcal{V}} \neq \omega$  for certain varieties of generalized nonassociative algebras of finite type. The statement that  $\chi_{\mathcal{V}} \neq \omega$  is the statement that if  $\mathcal{V}$  is residually finite ( $\chi_{\mathcal{V}} \leq \omega$ ), then there is a finite bound on the size of the SI's in  $\mathcal{V}$  ( $\chi_{\mathcal{V}} < \omega$ ). Because  $\mathcal{V}$  has finite type, a finite bound on the size of the SI's in  $\mathcal{V}$  implies that there are finitely many SI's, all finite, hence the product of these SI's will be a single finite algebra that generates  $\mathcal{V}$ .

It follows from the work of Freese and McKenzie in [1] that if  $\chi_{\mathcal{V}} \neq \infty$ , then all algebras in  $\mathcal{V}$  satisfy (C1), where this commutator identity is expressed in terms of the commutator of congruences. This commutator corresponds to the one we introduced in Definition 2.5, according to Lemma 2.6, so we may express (C1) in terms of ideals: For a generalized nonassociative algebra  $A$ , (C1) is the property that whenever  $U, V \subseteq A$  are ideals, then  $U \cap [V, V] = [U \cap V, V]$ . If  $A$  is SI with smallest nonzero ideal  $M$  (the *monolith* of  $A$ ) and  $N$  is the annihilator of  $M$ , then (C1) forces  $N$  to be abelian. For if  $[N, N] > 0$ , then  $[N, N] \geq M$ , leading to the contradiction  $M \cap [N, N] = M > 0 = [M, N] \geq [M \cap N, N]$ . Thus, in this section, where we study

residually finite varieties of generalized nonassociative algebras, any SI will have the property that the annihilator of its monolith is abelian.

For the purpose of obtaining a contradiction we assume throughout this section that  $\mathcal{V}$  is a variety of generalized nonassociative algebras of finite type for which  $\chi_{\mathcal{V}} = \omega$ . Hence all SI's in  $\mathcal{V}$  are finite, but there is no finite bound on their cardinality. Let  $A_1, A_2, \dots$  be a representative list of the SI's in  $\mathcal{V}$ , let  $M_i$  be the smallest nonzero ideal of  $A_i$ , and let  $N_i$  be the annihilator of  $M_i$ . The main task we set for ourselves in this section is to prove that the indices  $[A_i : N_i]$  are bounded by a finite number.

**Lemma 3.1.** *There is a first-order formula  $\varphi(x, y)$  that is a universally quantified conjunction of equations such that for all  $a, b \in A \in \mathcal{V}$  it is the case that  $A \models \varphi(a, b)$  iff  $[(a), (b)] = 0$  (the commutator of principal ideals is zero).*

*Proof.* Let us say that an element  $a \in A$  *annihilates* an element  $b \in A$  if every conjugate of  $a$  commutes with every conjugate of  $b$  and if

$$(3.1) \quad \forall c_1, \dots, \forall c_n (F(c_1, \dots, a, \dots, b, \dots, c_n) = 0)$$

whenever  $a$  and  $b$  are substituted into the  $i$ th and  $j$ th positions, some  $i \neq j$ , of an operation  $F$  that is one of the multilinear additional operations of  $\mathcal{V}$ . It follows from Lemma 2.7 that  $[(a), (b)] = 0$  in  $A$  iff every translate of  $a$  annihilates every translate of  $b$ .

The property that  $x$  annihilates  $y$  may be expressed by a first-order formula  $\alpha(x, y)$  that is a conjunction of universally quantified equations. We may take  $\alpha(x, y)$  to be

the conjunction of

$$(3.2) \quad \forall z_1 \forall z_2 (((-z_1) + x + z_1) + ((-z_2) + y + z_2) - ((-z_2) + y + z_2) + ((-z_1) + x + z_1) = 0)$$

with all equations of the form

$$(3.3) \quad \forall z_1, \dots, \forall z_n (F(z_1, \dots, x, \dots, y, \dots, z_n) = 0)$$

where  $F$  ranges over all additional multilinear operations of  $\mathcal{V}$  and  $x$  and  $y$  appear in all pairs of distinct places. For later reference,  $\alpha(x, y) = \forall \mathbf{z} \bigwedge (G_i(x, y, \mathbf{z}) = 0)$  where  $G_i$  is a term of the type appearing on the left side of the atomic subformula in (3.2) or (3.3).

It follows that there is a formula  $\alpha_{p,q}(x, y)$  that expresses the fact that every  $p$ -translate of  $x$  annihilates every  $q$ -translate of  $y$ . This formula will also be a conjunction of universally quantified equations. Namely,  $\alpha_{p,q}(x, y)$  may be constructed by forming the conjunction of all formulas  $\alpha(T_1(x), T_2(y))$  where  $T_1(x) = T_{\mathbf{c}_1}^{(e_1, f_1)} \circ \dots \circ T_{\mathbf{c}_p}^{(e_p, f_p)}(x)$  and  $T_2(x) = T_{\mathbf{d}_1}^{(g_1, h_1)} \circ \dots \circ T_{\mathbf{d}_q}^{(g_q, h_q)}(x)$ , then universally quantifying over the subscript  $\mathbf{c}$ 's, and  $\mathbf{d}$ 's used in the translations.

Finally let  $\alpha_{\leq p, \leq q}(x, y)$  be the conjunction of all  $\alpha_{r,s}(x, y)$  for  $r \leq p$  and  $s \leq q$ . This formula is also a universally quantified conjunction of equations, and it expresses the fact that every element obtained from  $x$  by a translation of length at most  $p$  annihilates every element obtained from  $y$  by a translation of length at most  $q$ .

**Claim 3.2.** *There is a positive integer  $\ell$  such that whenever  $a, b \in A \in \mathcal{V}$  it is the case that if  $a$  annihilates every  $k$ -translate of  $b$  for every  $k \leq \ell$ , then  $a$  annihilates every translate of  $b$ .*

We assume that the claim is false, and construct an infinite SI in  $\mathcal{V}$  from this assumption, contradicting our global assumption in this section that  $\chi_{\mathcal{V}} = \omega$ . Assume therefore that for every  $\ell \in \omega$  there exist  $B_\ell \in \mathcal{V}$  and  $a_\ell, b_\ell \in B_\ell$  that refute the statement of the claim for this value of  $\ell$ . This means that  $a_\ell$  annihilates every  $k$ -translate of  $b$  for every  $k \leq \ell$ , but  $a_\ell$  does not annihilate some  $k$ -translate of  $b_\ell$  for some  $k > \ell$ .

We describe a tree that represents all the translation types. Begin with the alphabet of symbols  $\mathcal{T} = \{T^{(i_1, j_1)}, \dots, T^{(i_\mu, j_\mu)}\}$  representing the finite set of basic translation types. Any string of length  $k$  in  $\mathcal{T}^*$  can be taken to represent the type of a  $k$ -translation; namely the empty string  $e$  represents the identity translation, a string of length 1,  $T^{(i, j)}$ , represents the translations  $T_{\mathbf{c}}^{(i, j)}(x)$  that have this type, a string of length 2,  $T^{(i_1, j_1)}T^{(i_2, j_2)}$ , represents the 2-translations  $T_{\mathbf{c}_1}^{(i_1, j_1)} \circ T_{\mathbf{c}_2}^{(i_2, j_2)}(x)$ , etc. Order the elements of  $\mathcal{T}^*$  by defining  $\sigma \leq \tau$  if  $\sigma$  is an initial segment of  $\tau$ . The resulting ordered set is a meet semilattice that is in fact a tree rooted at  $e$ . The fact that the alphabet  $\mathcal{T}$  is finite implies that the tree  $\mathcal{T}^*$  has *finite branching*, i.e. each element  $\sigma \in \mathcal{T}^*$  has finitely many successors (which are those strings obtained by adding a single symbol from  $\mathcal{T}$  to the end of  $\sigma$ ).

We will make use of several copies of the tree  $\mathcal{T}^*$ , say  $\mathcal{T}_1^*, \dots, \mathcal{T}_m^*$ , one for every conjunct of  $\alpha(x, y) = \forall \mathbf{z} \bigwedge_{i=1}^m (G_i(x, y, \mathbf{z}) = 0)$ . Call a string  $T^{(i_1, j_1)} \dots T^{(i_h, j_h)}$  a *bad node of height  $h$  in  $\mathcal{T}_i^*$*  if there exist  $a, b \in B \in \mathcal{V}$  such that

- (1)  $a$  annihilates every  $k$ -translate of  $b$  for  $k < h$  but
- (2) there exist  $\mathbf{c}_j$  such that  $a$  does not annihilate the  $h$ -translate  $b' := T_{\mathbf{c}_1}^{(i_1, j_1)} \circ \dots \circ T_{\mathbf{c}_h}^{(i_h, j_h)}(b)$  because
- (3)  $B \models \exists \mathbf{z} (G_i(a, b', \mathbf{z}) \neq 0)$ .

These conditions are intended to record minimal failures of the annihilation relation. Items (1) and (2) identify a minimal translate  $b'$  of  $b$  that fails to be annihilated by  $a$ , while item (3) indicates that  $a$  fails to annihilate  $b'$  because the  $i$ th conjunct ( $G_i(x, y, \mathbf{z}) = 0$ ) of  $\alpha(x, y)$  fails to be satisfied by  $(x, y) = (a, b')$  for some choice of  $\mathbf{z}$ . We record this information in the  $i$ th tree at the address indicated by the type of the translation taking  $b$  to  $b'$ .

Our earlier assumption about the properties of  $a_\ell, b_\ell \in B_\ell$  guarantee that for every  $\ell$  there is a bad node of height  $h$  for some  $h \geq \ell$  in at least one of the  $\mathcal{T}_i^*$ 's. Hence there are bad nodes of arbitrarily large height in at least one of the trees. On the other hand, if  $a, b \in B \in \mathcal{V}$  witness that  $T^{(i_1, j_1)} \dots T^{(i_h, j_h)}$  is a bad node of height  $h$  in  $\mathcal{T}_i^*$ , because  $a$  does not annihilate  $b' = T_{\mathbf{c}_1}^{(i_1, j_1)} \circ \dots \circ T_{\mathbf{c}_h}^{(i_h, j_h)}(b)$  in the sense that  $B \models \exists \mathbf{z}(G_i(a, b', \mathbf{z}) \neq 0)$ , then the elements  $a, T_{\mathbf{c}_h}^{(i_h, j_h)}(b) \in B$  witness that  $T^{(i_1, j_1)} \dots T^{(i_{h-1}, j_{h-1})}$  is a bad node of height  $h - 1$  in the same tree. Thus the bad nodes in each tree form an order ideal in that tree.

Combining the information so far we obtain that at least one of the trees contains an infinite order ideal of bad nodes. Kőnig's Lemma guarantees that an infinite order ideal in a rooted tree with finite branching contains an infinite branch. This means that there is some tree  $\mathcal{T}_i^*$  and some infinite sequence  $\sigma = T^{(i_1, j_1)} T^{(i_2, j_2)} T^{(i_3, j_3)} \dots$  such that every initial subsequence of  $\sigma$  is a bad node in  $\mathcal{T}_i^*$ . We use this information to build our infinite SI.

Expand the language of  $\mathcal{V}$  by adding additional constant symbols  $p, q, r_i, \mathbf{s}_i, \mathbf{t}, i \in \omega$ . Let  $\Sigma$  denote a set of first-order sentences in this language which includes

- (i) an equational basis for  $\mathcal{V}$ ,
- (ii) the sentences  $r_u = T_{\mathbf{s}_u}^{(i_u, j_u)}(r_{u+1})$  for each  $u \in \omega$ ,
- (iii)  $\alpha_{0, \leq \ell}(p, r_{\ell+1})$  for each  $\ell \in \omega$ ,

- (iv)  $G_i(p, r_0, \mathbf{t}) = q$ , and
- (v)  $q \neq 0$ .

Because of the sentences in (i), a model of  $\Sigma$  is an algebra  $S \in \mathcal{V}$  with some elements named by constants. Because of the sentences in (ii), the elements named by the  $r$ 's are related by basic translations in the following way:

$$(3.4) \quad \dots \xrightarrow{T_{\mathbf{s}_4}^{(i_4, j_4)}} r_4 \xrightarrow{T_{\mathbf{s}_3}^{(i_3, j_3)}} r_3 \xrightarrow{T_{\mathbf{s}_2}^{(i_2, j_2)}} r_2 \xrightarrow{T_{\mathbf{s}_1}^{(i_1, j_1)}} r_1 \xrightarrow{T_{\mathbf{s}_0}^{(i_0, j_0)}} r_0.$$

(Here we emphasize that the  $u$ th translation  $T_{\mathbf{s}_u}^{(i_u, j_u)}(x)$  is of type  $T^{(i_u, j_u)}$ , which is the  $u$ th symbol in the string  $\sigma$  obtained above using König's Lemma, so (3.4) reflects the structure of the sequence  $\sigma$ .) The sentences in (iii) guarantee that the element named by the constant  $p$  annihilates every  $k$ -translate of the element named by  $r_\ell$  if  $k < \ell$ . But the sentences in (iv) and (v) guarantee that the element named by  $p$  does not annihilate the element named by  $r_0$  because the  $i$ th conjunct ( $G_i(x, y, \mathbf{z}) = 0$ ) of  $\alpha(x, y)$  is not satisfied when  $(x, y, \mathbf{z}) = (p, r_0, \mathbf{t})$ . (Again, the conjunct in question is the one obtained above using König's Lemma.)

A model of  $\Sigma$  must exist, since  $\Sigma$  is finitely satisfiable, a fact that we now demonstrate. For any  $\ell \geq 0$  the  $\ell$ th initial segment of  $\sigma$ ,  $T^{(i_1, j_1)}T^{(i_2, j_2)} \dots T^{(i_\ell, j_\ell)}$ , is a bad node in some tree  $\mathcal{T}_i^*$ . This means that there exist  $a, b \in B \in \mathcal{V}$  such that  $a$  annihilates every  $k$ -translate of  $b$  for  $k < \ell$ , but there exist  $\mathbf{c}_i$  such that  $a$  does not annihilate the  $\ell$ -translate  $b' := T_{\mathbf{c}_1}^{(i_1, j_1)} \circ \dots \circ T_{\mathbf{c}_\ell}^{(i_\ell, j_\ell)}(b)$  because  $B \models (G_i(a, b', \mathbf{d}) \neq 0)$  for some  $\mathbf{d}$ . Interpret the new constant symbols  $p, q, r_i, \mathbf{s}_i, \mathbf{t}$  in  $B$  so that  $p = a, \mathbf{t} = \mathbf{d}$  and, for  $0 \leq u \leq \ell$ ,  $\mathbf{s}_u = \mathbf{c}_u$  and  $r_{\ell-u} = T_{\mathbf{c}_1}^{(i_1, j_1)} \circ \dots \circ T_{\mathbf{c}_u}^{(i_u, j_u)}(b)$ . Interpret  $r_u, \mathbf{s}_u$  arbitrarily for  $u > \ell$ . Finally, if  $b' = T_{\mathbf{c}_1}^{(i_1, j_1)} \circ \dots \circ T_{\mathbf{c}_\ell}^{(i_\ell, j_\ell)}(b)$  is the element named by  $r_0$ , let the symbol  $q$  name the element  $G_i(a, b', \mathbf{d})$ . The properties that made  $T^{(i_1, j_1)}T^{(i_2, j_2)} \dots T^{(i_\ell, j_\ell)}$

a bad node in tree  $\mathcal{T}_i^*$  guarantee that  $B$  expanded by the extra constants satisfy all sentences in  $\Sigma$  of types (i), (iii), (iv), (v), and also satisfies the first  $\ell$  sentences of type (ii). Thus, any finite subset of the sentences in  $\Sigma$  can be satisfied by some such  $B$  for  $\ell$  chosen large enough.

The Compactness Theorem guarantees that  $\Sigma$  has a model, say  $K$ . By factoring  $K$  by an ideal maximal for not containing the element denoted  $q$  we obtain an SI model of  $\Sigma$ . (The reason this factor is still a model of  $\Sigma$  is that all the universally quantified conjunctions of equations in  $\Sigma$  are preserved in passing to quotients, while we have arranged that the one inequation  $q \neq 0$  was preserved by factoring by an ideal not containing  $q$ .) Thus we may assume that  $K$  is an SI member of  $\mathcal{V}$ .  $K$  must be infinite, since the elements denoted  $r_0, r_1, \dots$  must be distinct. (If  $u < v$ , then  $\Sigma$  implies that  $q$  is an  $u$ -translate of  $r_u$  that is not annihilated by  $p$ . But since  $\alpha_{0, \leq v-1}(p, r_v)$  holds,  $p$  must annihilate all  $k$ -translates of  $r_v$  for  $k \leq v-1$ , hence  $p$  annihilates all  $u$ -translates of  $r_v$ . This implies that  $r_u \neq r_v$  for  $u < v$ .)

The existence of the infinite SI  $K \in \mathcal{V}$  is contrary to our assumption that  $\mathcal{V}$  has residual character  $\omega$ . This contradiction resulted from the assumption that Claim 3.2 was false, so that claim is true. Recall that this is the claim that associated to  $\mathcal{V}$  a positive integer  $\ell$  such that whenever  $a, b \in A \in \mathcal{V}$  it is the case that if  $a$  annihilates every  $k$ -translate of  $b$  for every  $k \leq \ell$ , then  $a$  annihilates every translate of  $b$ .

**Claim 3.3.** *The formula  $\alpha_{\leq \ell, \leq \ell}(x, y)$  defines the annihilation relation between principal ideals of algebras in  $\mathcal{V}$ . (If  $a, b \in A \in \mathcal{V}$ , then  $A \models \alpha_{\leq \ell, \leq \ell}(a, b)$  iff  $[(a), (b)] = 0$ .)*

If  $a, b \in A \in \mathcal{V}$  and  $[(a), (b)] = 0$ , then every translate of  $a$  annihilates every translate of  $b$ , so  $A \models \alpha_{\leq \ell, \leq \ell}(a, b)$ . Conversely, if  $A \models \alpha_{\leq \ell, \leq \ell}(a, b)$  and  $r, s \leq \ell$ , then every  $r$ -translate of  $a$  annihilates every  $s$ -translate of  $b$ . Hence if  $a'$  is any such



$r$ -translate of  $a$ , then it follows from Claim 3.2 that  $a'$  annihilates every translate of  $b$ . Turning the situation around, any translate  $b'$  of  $b$  annihilates every  $r$  translate of  $a$  whenever  $r \leq \ell$ . Another application of Claim 3.2 shows that every translate of  $b$  annihilates every translate of  $a$ , and therefore  $[(a), (b)] = 0$ .

We may take  $\varphi(x, y) = \alpha_{\leq \ell, \leq \ell}(x, y)$ , since this formula is a universally quantified conjunction of equations.  $\square$

**Lemma 3.4.** *The indices  $[A_i : N_i]$  are bounded by a finite number.*

*Proof.* Recall that  $A_1, A_2, \dots$  is a representative list of the SI's in  $\mathcal{V}$ , that they are finite but there is no finite bound on their size, that  $M_i$  is the least nonzero ideal in  $A_i$  and  $N_i$  is the largest ideal in  $A_i$  such that  $[N_i, M_i] = 0$ .

Assume that this lemma is false, so that there is no finite bound on the indices  $[A_i, N_i]$ . After thinning out the sequence if necessary, assume that in fact  $[A_i, N_i] \geq i$  for all  $i$ . We will find that this assumption contradicts the residual finiteness of  $\mathcal{V}$ .

**Claim 3.5.** *If the formula  $\varphi(x, y)$  from Lemma 3.1 is  $\forall \mathbf{z} \bigwedge_{i=1}^m (H_i(x, y, \mathbf{z}) = 0)$  and  $a, b \in B \in \mathcal{V}$ , then  $H_i(a, b, \mathbf{c}) \in (a)$  and  $H_i(a, b, \mathbf{c}) \in (b)$  for every  $\mathbf{c}$  and  $i$ .*

In the quotient  $B/[(a), (b)]$  the image ideals  $(\bar{a})$  and  $(\bar{b})$  annihilate one another, so  $B/[(a), (b)] \models \forall \mathbf{z} \bigwedge_{i=1}^m (H_i(\bar{a}, \bar{b}, \mathbf{z}) = 0)$ . This implies that  $H_i(\bar{a}, \bar{b}, \bar{\mathbf{c}}) = 0$  for every  $\bar{\mathbf{c}}$  and every  $i$ , hence back in  $B$  we have  $H_i(a, b, \mathbf{c}) \in [(a), (b)]$  for every  $\mathbf{c}$  and  $i$ . Since  $[(a), (b)] \subseteq (a) \cap (b)$ , this implies that  $H_i(a, b, \mathbf{c}) \in (a)$  and  $H_i(a, b, \mathbf{c}) \in (b)$  for every  $\mathbf{c}$  and  $i$ .

Claim 3.5 identifies some particular ways to generate elements of a principal ideal  $(a)$ , namely any element of the form  $H_i(a, b, \mathbf{c})$  or  $H_i(b, a, \mathbf{c})$  is such an element. We

introduce the notation  $\{a, b\} \longrightarrow \{g, h\}$  to represent that  $g - h$  belongs to the ideal  $(a - b)$  in this way. Specifically,  $\{a, b\} \longrightarrow \{g, h\}$  will mean that

$$(3.5) \quad \exists e \exists \mathbf{c} (\{g, h\} = \{0, H_i(a - b, e, \mathbf{f})\} \quad \text{or} \quad \{g, h\} = \{0, H_i(e, a - b, \mathbf{f})\}).$$

It is evident from the form of (3.5) that  $\{a, b\} \longrightarrow \{g, h\}$  is a first-order definable 4-ary relation. It follows from Claim 3.5 that  $g - h \in (a - b)$  whenever  $\{a, b\} \longrightarrow \{g, h\}$ .

**Claim 3.6.** *If  $a, b, c, d \in B \in \mathcal{V}$  and if  $[(a - b), (c - d)] \neq 0$ , then there exists  $g, h \in B$  with  $g \neq h$  such that  $\{a, b\} \longrightarrow \{g, h\}$  and  $\{c, d\} \longrightarrow \{g, h\}$ .*

If  $[(a - b), (c - d)] \neq 0$ , then there exists  $\mathbf{f}$  and  $i$  such that  $H_i(a - b, c - d, \mathbf{f}) \neq 0$ . Thus, with  $\{g, h\} = \{0, H_i(a - b, c - d, \mathbf{f})\}$  we have  $\{a, b\} \longrightarrow \{g, h\}$  and  $\{c, d\} \longrightarrow \{g, h\}$ . This proves the claim.

Extend the arrow notation in the following ways. Write  $\{a, b\} \longrightarrow_k \{g, h\}$  to mean that there exists a chain

$$\{a, b\} = \{a_1, b_1\} \longrightarrow \{a_2, b_2\} \longrightarrow \cdots \longrightarrow \{a_\ell, b_\ell\} = \{g, h\}$$

for some  $\ell \leq k$ . The relation  $\{a, b\} \longrightarrow_k \{g, h\}$  is also definable by a formula, and if the relation holds then  $g - h \in (a - b)$ . For a set  $S = \{s_1, \dots, s_k\}$  write  $S \Longrightarrow_k \{g, h\}$  to indicate that  $\{s_i, s_j\} \longrightarrow_k \{g, h\}$  for each  $i \neq j$ .

**Claim 3.7.** *Let  $A \in \mathcal{V}$  be one of the SI algebras  $A_i$ , let  $M = M_i$  and  $N = N_i$ . Suppose that  $\{a, b\} \subseteq M$  is a 2-element subset and  $S \subseteq A$  consists of  $k$  elements that are pairwise incongruent modulo  $N$ . There exists a 2-element subset  $\{g, h\} \subseteq M$  such that  $\{a, b\} \longrightarrow_{\binom{k}{2}} \{g, h\}$  and  $S \Longrightarrow_{\binom{k}{2}} \{g, h\}$ .*

Let  $\ell = \binom{k}{2}$  and let  $T_1, \dots, T_\ell$  be an enumeration of the 2-element subsets of  $S$  where  $T_1 = \{s_1, s_2\}$ . Since  $a - b \in M - \{0\}$ ,  $s_1 - s_2 \notin N$ , and  $N$  is the annihilator of  $M$  it follows that  $[(a - b), (s_1 - s_2)] \neq 0$ . From Claim 3.6 there is a 2-element set  $\{a_2, b_2\}$  such that  $\{a, b\} \longrightarrow \{a_2, b_2\}$  and  $T_1 \longrightarrow \{a_2, b_2\}$ . It follows from the definition of the arrow relation that one of the elements of  $\{a_2, b_2\}$  is zero while it follows from Claim 3.5 that  $a_2 - b_2 \in (a - b) = M$ . Hence  $\{a_2, b_2\}$  is another 2-element subset of  $M$ . We can repeat the argument with  $\{a_2, b_2\}$  and  $T_2$  replacing  $\{a, b\}$  and  $T_1$  to obtain a new doubleton  $\{a_3, b_3\} \subseteq M$  such that  $\{a_2, b_2\} \longrightarrow \{a_3, b_3\}$  and  $T_2 \longrightarrow \{a_3, b_3\}$ . Continuing to the end we get

$$\begin{array}{ccccccc}
 & & T_1 & & T_2 & & T_\ell \\
 & & \downarrow & & \downarrow & & \downarrow \\
 \{a, b\} & \longrightarrow & \{a_2, b_2\} & \longrightarrow & \{a_3, b_3\} & \longrightarrow & \cdots \longrightarrow \{a_{\ell+1}, b_{\ell+1}\} = \{g, h\}
 \end{array}$$

Each of the doubletons  $\{a, b\}, T_1, \dots, T_\ell$  is related to  $\{g, h\}$  by an  $\longrightarrow$ -path of length at most  $\ell$ , hence by  $\longrightarrow_\ell$ . This proves the claim.

**Claim 3.8.** *The algebra  $A_k$  contains subsets  $S_i \subseteq A_k$  and doubletons  $\{a_i, b_i\} \subseteq M$  for  $1 \leq i \leq k$  such that  $|S_i| = i$ ,  $\{a_{i+1}, b_{i+1}\} \longrightarrow_{\binom{i+1}{2}} \{a_i, b_i\}$  and  $S_{i+1} \implies_{\binom{i+1}{2}} \{a_i, b_i\}$  for  $1 \leq i < k$ .*

Start by choosing  $S_k$  to be a set of  $k$  elements that are pairwise incongruent modulo  $N_k$ . This is possible by our assumption that  $[A_k : N_k] \geq k$ . Next choose an arbitrary doubleton  $\{a_k, b_k\} \subseteq M_k$ . Use Claim 3.7 to find a doubleton  $\{a_{k-1}, b_{k-1}\} \subseteq M_k$  such that  $\{a_k, b_k\} \longrightarrow_{\binom{k}{2}} \{a_{k-1}, b_{k-1}\}$  and  $S_k \implies_{\binom{k}{2}} \{a_{k-1}, b_{k-1}\}$ . To continue, let  $S_{k-1} \subseteq S_k$  be a subset of size  $k - 1$ , and repeat the steps just described with  $S_{k-1}$

the doubleton  $\{a_{k-1}, b_{k-1}\}$  to produce a new doubleton  $\{a_{k-2}, b_{k-2}\}$ . Continuing to the end we get

$$\begin{array}{ccccccc} S_k & & S_{k-1} & & S_2 & & \\ \downarrow \binom{k}{2} & & \downarrow \binom{k-1}{2} & & \downarrow \binom{2}{2} & & \\ \{a_k, b_k\} & \xrightarrow{\binom{k}{2}} & \{a_{k-1}, b_{k-1}\} & \xrightarrow{\binom{k-1}{2}} & \{a_{k-2}, b_{k-2}\} & \xrightarrow{\binom{k-2}{2}} \cdots \xrightarrow{\binom{2}{2}} & \{a_1, b_1\} \end{array}$$

This proves the claim.

**Claim 3.9.** *There is some algebra  $A \in \mathcal{V}$  that contains subsets  $S_i \subseteq A$  and doubletons  $\{a_i, b_i\}$  for all positive  $i \in \omega$  such that  $|S_i| = i$ ,  $\{a_{i+1}, b_{i+1}\} \xrightarrow{\binom{i+1}{2}} \{a_i, b_i\}$  and  $S_{i+1} \xRightarrow{\binom{i+1}{2}} \{a_i, b_i\}$  for all  $i$ .*

This claim asserts that  $A$  has elements related as in

$$\begin{array}{ccccccc} S_5 & & S_4 & & S_3 & & S_2 \\ \downarrow \binom{5}{2} & & \downarrow \binom{4}{2} & & \downarrow \binom{3}{2} & & \downarrow \binom{2}{2} \\ \cdots & \xrightarrow{\binom{5}{2}} & \{a_4, b_4\} & \xrightarrow{\binom{4}{2}} & \{a_3, b_3\} & \xrightarrow{\binom{3}{2}} & \{a_2, b_2\} \xrightarrow{\binom{2}{2}} \{a_1, b_1\} \end{array}$$

where  $|S_i| = i$  for all  $i$ . This follows from the Compactness Theorem using the facts that all arrow relations are describable by formulas and that every finite fragment of this configuration of elements is realizable in some algebra in  $\mathcal{V}$ , as we proved in Claim 3.8.

Now we complete the proof of the lemma. Claim 3.9 guarantees that  $\mathcal{V}$  contains an algebra  $A$  that has subsets  $S_i \subseteq A$  and doubletons  $\{a_i, b_i\}$  for all positive  $i \in \omega$  such that  $|S_i| = i$ ,  $\{a_{i+1}, b_{i+1}\} \xrightarrow{\binom{i+1}{2}} \{a_i, b_i\}$  and  $S_{i+1} \xRightarrow{\binom{i+1}{2}} \{a_i, b_i\}$  for all  $i$ . As  $\mathcal{V}$  is a residually finite variety and  $a_1 \neq b_1$ , there must exist a homomorphism  $h: A \rightarrow B$  onto a finite algebra  $B$  such that  $a_1 - b_1 \notin \ker(h)$ . If  $k > |B|$ , then the restriction of  $h$  to  $S_k$  cannot be 1-1, since  $|S_k| = k > |B| \geq |h(S_k)|$ . Hence there exist

$s_i, s_j \in S_k$  such that  $s_i - s_j \in \ker(h)$ . There is an arrow path from  $S_k$  to  $\{a_1, b_1\}$ , hence from  $\{s_i, s_j\}$  to  $\{a_1, b_1\}$ , so it follows from Claim 3.6 and the definition of arrows that  $a_1 - b_1 \in (s_i - s_j)$ . But now we have the contradictory conclusions that  $a_1 - b_1 \in (s_i - s_j)$ ,  $(s_i - s_j) \subseteq \ker(h)$ , and  $a_1 - b_1 \notin \ker(h)$ . This shows that our initial assumption that the indices  $[A_i : N_i]$  have no finite bound is false, so the lemma is proved.  $\square$

We now have that if  $\mathcal{V}$  is a variety of generalized nonassociative algebras of finite type and  $\chi_{\mathcal{V}} = \omega$ , then there is a finite number  $\ell$  that bounds the index of the annihilator of the monolith in every SI of  $\mathcal{V}$ . If this bound  $\ell$  is equal to 1, then the annihilator of the monolith of any SI  $A_i$  is  $A_i$  itself, so by (C1) the algebra  $A_i$  is abelian. For  $[A_i, A_i] = 0$  to hold, the underlying additive group of  $A_i$  must be commutative and all additional multilinear operations of at least 2 variables must be constant zero operations. There is no restriction on the additional unary multilinear operations other than they be linear, so every SI is an abelian group equipped with finitely many unary endomorphisms. This makes  $\mathcal{V}$  is equivalent to a variety of modules over a finitely generated ring.

We have not fully reduced to the case where  $\mathcal{V}$  is equivalent to a variety of modules over a finitely generated ring, since we do not know that  $\ell = 1$ , but it is clear now that the module case is an important special case of the problem we are investigating.

#### 4. RESIDUALLY FINITE VARIETIES OF MODULES

The main goal of this section is to prove that if  $R$  is a finitely generated ring that is a finitely generated module over its center and  $\mathcal{V}$  is some variety of  $R$ -modules, then  $\chi_{\mathcal{V}} \neq \omega$ .

**Definition 4.1.** A ring  $R$  is *minimal* if  $R$  is finitely generated, infinite, and every proper homomorphic image of  $R$  is finite.

**Lemma 4.2.** *If  $R$  is a finitely generated infinite ring and  $I \triangleleft R$  is an ideal of infinite index, then  $I$  can be enlarged to an ideal  $I'$  such that  $R/I'$  is minimal.*

*Proof.* Recall that a homomorphism from a finitely generated algebraic structure onto a finitely presentable algebraic structure has finitely generated kernel. Applying this to the natural map  $R \rightarrow R/K$  where  $K \triangleleft R$  is an ideal of finite index, and using the fact that a finite algebraic structure in a finite language is finitely presentable, one obtains that  $K$  is a finitely generated ideal. In summary, ideals of finite index in finitely generated rings are finitely generated. Thus we may apply Zorn's Lemma to enlarge any ideal  $I$  of infinite index to an ideal  $I'$  that is maximal among ideals of infinite index.  $R/I'$  is minimal by the choice of  $I'$  coupled with the fact that quotients of finitely generated rings are finitely generated.  $\square$

**Corollary 4.3.** *If  $R$  is a finitely generated ring and  $\mathcal{V}$  is any variety of  $R$ -modules for which  $\chi_{\mathcal{V}} = \omega$ , then  $R$  has a quotient  $\bar{R} = R/I'$  that is minimal and has the property that the variety  $\mathcal{U}$  of all  $\bar{R}$ -modules satisfies  $\chi_{\mathcal{U}} = \omega$ .*

*Proof.* Note that we are not assuming that  $\mathcal{V}$  is the variety of *all*  $R$ -modules, but rather is a subvariety. Hence the annihilator,  $\text{Ann}(\mathcal{V})$ , may be nonzero. ( $\text{Ann}(\mathcal{V})$  is, by definition, the largest ideal of  $R$  that annihilates all members of  $\mathcal{V}$ ). Because the map from varieties of  $R$ -modules to ideals of  $R$  that assigns to a variety its annihilator is a bijection,  $\mathcal{V}$  is definitionally equivalent to the variety of all  $R/I$ -modules where  $I = \text{Ann}(\mathcal{V})$ . If  $R/I$  were finite, then it would follow from [5] that  $\chi_{\mathcal{V}} \leq |R/I| < \omega$  contrary to our assumption  $\chi_{\mathcal{V}} = \omega$ . Therefore, by Lemma 4.2 there is an ideal  $I' \supseteq I$  such that  $\bar{R} := R/I'$  is minimal.

Because  $\overline{R}$  is isomorphic to a quotient of  $R/I$ , the variety of all  $\overline{R}$ -modules,  $\mathcal{U}$ , is definitionally equivalent to a subvariety of  $\mathcal{V}$ , hence  $\chi_{\mathcal{U}} \leq \chi_{\mathcal{V}} = \omega$ . To show that  $\chi_{\mathcal{U}} = \omega$ , assume instead that  $\mathcal{U}$  contains only finitely many isomorphism types of SI's,  $S_1, \dots, S_n$ . Since this is a representative list of SI's,  $\overline{R}$  acts faithfully on the product  $\prod S_i$ , which is a finite module. This can only happen if  $\overline{R}$  is finite, which is not the case since  $\overline{R}$  is minimal. Thus  $\chi_{\mathcal{V}} = \omega$ .  $\square$

Now we know that if  $R$  is a finitely generated ring for which *some* variety of  $R$ -modules has residual character  $\omega$ , then  $R$  has a minimal quotient  $\overline{R}$  for which the variety of *all*  $\overline{R}$ -modules has residual character  $\omega$ . Let us examine the structure of such quotient rings.

**Theorem 4.4.** *Let  $R$  be a minimal ring such that the variety of all  $R$ -modules has residual character  $\omega$ .*

- (a)  *$R$  is a prime ring (i.e., if  $I, K \triangleleft R$  and  $IK = 0$ , then  $I = 0$  or  $K = 0$ ).*
- (b) *The center of  $R$  is a finite field.*

*Proof.* To prove (a), assume that  $I$  and  $K$  are nonzero ideals of  $R$  whose product is zero. Since  $R$  is minimal,  $I$  and  $K$  have finite index in  $R$ , therefore the intersection  $J := I \cap K$  is an ideal of finite index for which  $J^2 \subseteq IK = 0$ . This shows that the radical of  $R$  has finite index, and consequently the isomorphism types of simple  $R$ -modules are the same (up to definitional equivalence) as the isomorphism types of simple modules over the finite ring  $R/\text{rad}(R)$ . Since finite rings have finitely many isomorphism types of simple modules, all of which are finite, the same is true of the simple  $R$ -modules. Let  $T_1, \dots, T_m$  be a representative set of simple  $R$ -modules.

The fact that the variety of all  $R$ -modules has residual character  $\omega$  means that all SI  $R$ -modules are finite, but there is no finite bound on their size. Thus, there exists

a sequence of SI  $R$ -modules,  $S_1, S_2, \dots$  whose sizes increase without bound. Each SI has a smallest nonzero submodule, which is simple, hence is isomorphic to one of the  $T_i$ 's. Since there are only finitely many  $T_i$ 's, we may thin out the sequence  $S_1, S_2, \dots$  and henceforth assume that this is an infinite sequence of SI's whose smallest nonzero submodule is equal to a fixed finite simple  $R$ -module  $T$ .

Let  $\widehat{T}$  be the injective hull of  $T$ . The inclusion  $\iota: T \rightarrow \widehat{T}$  may be lifted to any  $S_i$ :

$$\begin{array}{ccc} & S_i & \\ & \uparrow & \searrow \bar{\iota} \\ T & \hookrightarrow & \widehat{T} \end{array}$$

The kernel of the lifted map,  $\bar{\iota}$ , is trivial, since it restricts trivially to  $T$ . Thus every  $S_i$  is embeddable in  $\widehat{T}$ . Since the  $S_i$ 's increase in size without finite bound,  $\widehat{T}$  is infinite. Since  $T$  is simple, and  $\widehat{T}$  is an essential extension of  $T$ ,  $\widehat{T}$  is an infinite SI  $R$ -module, contradicting the assumption that variety of all  $R$ -modules has residual character  $\omega$ . This concludes the proof that  $R$  is prime.

Next, as a first step toward proving (b), we argue that the center of  $R$  is a field. Choose a nonzero element  $t \in Z(R)$ . Consider the  $R$ -module  $M$  presented by generators  $v_i, i \in \omega$ , and relations  $tv_0 = 0, tv_{i+1} = v_i, i \in \omega$ . If  $v_0 \neq 0$  in this module, then let  $N \leq M$  be a submodule that is maximal for  $v_0 \notin N$ . Then  $M/N$  is SI with smallest nonzero submodule  $\langle \bar{v}_0 \rangle$ . Moreover, all elements  $\bar{v}_i$  are distinct in this SI, since if  $i < j$ , then  $t^j \bar{v}_i = 0$  and  $t^j \bar{v}_j = \bar{v}_0 \neq 0$ , forcing  $\bar{v}_i \neq \bar{v}_j$ . This proves that  $M/N$  is an infinite SI  $R$ -module when  $v_0 \neq 0$  in  $M$ , contrary to our assumption that the variety of all  $R$ -modules has residual character  $\omega$ .

Hence it must be that  $v_0 = 0$  in  $M$ . In this case, the set of sentences  $\{tv_{i+1} = v_i\} \cup \{tv_0 = 0\} \cup \{v_0 \neq 0\}$  together with the axioms of  $R$ -modules is inconsistent. By



the Compactness Theorem there is a finite inconsistent subset, which after a possible enlargement is:

$$(4.1) \quad \{tv_{i+1} = v_i, i < p\} \cup \{tv_0 = 0\} \cup \{v_0 \neq 0\}$$

together with the axioms for  $R$ -modules. If we let  $v = v_p$ , then  $v_i = t^{p-i}v$ ,  $t^p v = v_0$ , and the inconsistency of these sentences expresses that  $(t^{p+1}v = 0) \Rightarrow (t^p v = 0)$  holds in every  $R$ -module. Apply this implication to the module  $R/(t^{p+1})$ . If  $v = \bar{1}$ , then  $t^{p+1}v = 0$ . The quasi-identity forces  $t^p v = 0$ , or  $t^p \cdot 1 \in (t^{p+1})$  in  $R$ . This means that there is some  $s \in R$  such that  $t^p = st^{p+1}$ , or  $(1 - st)t^p = 0$ . Hence the ideals  $(1 - st)$  and  $(t^p) = Rt^p = (t)^p$  have product equal to zero (since  $t$  is in the center). Since we have established in (a) that  $R$  is prime, either  $(1 - st) = 0$  or  $(t) = 0$ , so either  $1 - st = 0$  or  $t = 0$ . The former must hold, since we chose  $t$  to be nonzero, so  $st = 1$  in  $R$ . Necessarily  $s \in Z(R)$ , since for any  $r \in R$  we have  $sr = sr1 = sr(st) = (st)rs = rs$ , and this proves that nonzero elements of  $Z(R)$  are invertible in  $Z(R)$ .

We conclude the proof of (b) by arguing that the subfield  $Z(R)$  is finite. Since every nonzero  $R$ -module is a  $Z(R)$ -vector space via restriction of scalars, and  $R$  must have nonzero finite modules if its variety of modules has residual character  $\omega$ , the field  $Z(R)$  must be finite.  $\square$

**Corollary 4.5.** *If  $R$  is a finitely generated ring that is a finitely generated module over its center, then no variety of  $R$ -modules has residual character  $\omega$ . Hence any residually finite variety of  $R$ -modules is generated by a single finite module.*

*Proof.* Suppose that  $R$  is a finitely generated ring that is a finitely generated module over its center, and there is a variety of  $R$ -modules satisfying  $\chi_V = \omega$ . Then according

to Corollary 4.3, some quotient  $\overline{R}$  of  $R$  is minimal and the variety of all  $\overline{R}$ -modules has residual character  $\omega$ .  $\overline{R}$  must also be a finitely generated module over its center. By Theorem 4.4 (b), the center of  $\overline{R}$  is a finite field, so in fact  $\overline{R}$  must be finite. This contradicts the fact that  $\overline{R}$  is minimal.

To prove the last claim of the corollary, observe that the first claim shows that if  $\mathcal{V}$  is a residually finite variety of  $R$ -modules, then  $\mathcal{V}$  has a finite bound on the cardinality of its SI members. Since  $R$  is finitely generated, this implies that  $\mathcal{V}$  has only finitely many SI modules, all finite. Such varieties are generated by a single finite member, as we have noted earlier.  $\square$

## 5. ENVELOPING RINGS

Exact sequences  $0 \rightarrow U \xrightarrow{\alpha} A \xrightarrow{\beta} Q \rightarrow 0$  make sense for generalized nonassociative algebras. In this section we only consider the case where  $\alpha$  is inclusion, so that  $U$  is an ideal of  $A$ . If  $U$  is abelian, it can be thought of as a “ $Q$ -module”, as we now explain. For each  $q \in Q$  let  $\hat{q} \in \beta^{-1}(q)$  be a fixed element of the preimage. Let  $\gamma_q(x) = \hat{q} + x - \hat{q}$  denote conjugation by  $\hat{q}$  considered as a polynomial function restricted to  $U$ . The subscript here is  $q$  rather than  $\hat{q}$  since the function of conjugation by an element of  $\beta^{-1}(q)$  on  $U$  is independent of the choice of the element when  $U$  is abelian. To see this, suppose that  $\hat{q}, \hat{q} + u \in \beta^{-1}(q)$ . Then for  $x \in U$  we have

$$(\hat{q} + u) + x - (\hat{q} + u) = \hat{q} + (u + x - u) - \hat{q} = \hat{q} + x - \hat{q}.$$

For each additional multilinear operation  $F_i$  and each tuple  $\mathbf{q} \in Q^n$  consider the translation  $T_{\mathbf{q}}^{(i,j)}(x) = F_i(\hat{q}_1, \dots, \hat{q}_{j-1}, x, \hat{q}_{j+1}, \dots, \hat{q}_n)$  as a polynomial function restricted to  $U$ . Our notation here is slightly in conflict with earlier use, because we are placing  $\mathbf{q}$  in the subscript instead of the proper tuple  $\hat{\mathbf{q}}$ . But again this

function does not depend on the choices of preimages, and our use of  $\mathbf{q}$  in place of  $\hat{\mathbf{q}}$  is intended to indicate that. To see why the function does not depend on choice of preimage when  $U$  is abelian, suppose that  $F_i(\hat{q}_1, \hat{q}_2, \dots, \hat{q}_{j-1}, x, \hat{q}_{j+1}, \dots, \hat{q}_n)$  and  $F_i(\hat{q}_1 + u, \hat{q}_2, \dots, \hat{q}_{j-1}, x, \hat{q}_{j+1}, \dots, \hat{q}_n)$  agree on  $U$ . The difference is the function  $F_i(u, \hat{q}_2, \dots, \hat{q}_{j-1}, x, \hat{q}_{j+1}, \dots, \hat{q}_n)$ , which is zero on  $U$  when  $[U, U] = 0$ . (We are using Definition 2.5 (ii).)

The functions of the form  $\gamma_q(x)$  and  $T_{\mathbf{q}}^{(i,j)}(x)$  are endomorphisms of the abelian group  $U^\circ = \langle U; +, -, 0 \rangle$ . The collection of these functions generates a subring  $R_{Q,U} \leq \text{End}(U^\circ)$  of the (unital) additive endomorphism ring of  $U^\circ$ . The significance of this unital ring is indicated by the following lemma.

**Lemma 5.1.** *If  $0 \rightarrow U \rightarrow A \rightarrow Q \rightarrow 0$  is exact and  $[U, U] = 0$ , then a function  $P: U^n \rightarrow U$  is the restriction from  $A$  of an algebra polynomial iff  $P$  is an  $R_{Q,U}$ -module polynomial.*

*Proof.* Since translations and conjugations are algebra polynomials, any function on  $U$  of the form  $M(x_1, \dots, x_n) + a$  for some  $R_{Q,U}$ -module polynomial  $M(x_1, \dots, x_n)$  and some element  $a \in A$  is the restriction of an algebra polynomial. We prove conversely that if  $P$  is any algebra polynomial, then restricting the domain of  $P$  to  $U^n$  yields a function  $P: U^n \rightarrow A$  that agrees with a function of the form  $M(x_1, \dots, x_n) + a$  for some  $R_{Q,U}$ -module polynomial  $M(x_1, \dots, x_n)$  and some element  $a \in A$ .

The proof is by induction. Certainly any variable or constant has the form  $M(\mathbf{x}) + a$ . Now suppose that  $P_i(x_1, \dots, x_n)$ ,  $1 \leq i \leq m$ , are  $n$ -ary algebra polynomials that agree with  $M_i(x_1, \dots, x_n) + a_i$  on  $U^n$ . For each  $i$ , let  $\hat{q}_i$  be the unique hatted element that is congruent to  $a_i$  modulo  $U$ . Then

- $-P_1$  agrees with  $-(M_1 + a_1) = -a_1 - M_1 = (-a_1 + (-M_1) + a_1) - a_1 = (-\hat{q}_1 + (-M_1) + \hat{q}_1) - a_1 = \gamma_{-q_1}(-M_1) - a_1$  on  $U^n$ . Note that  $\gamma_{-q_1}(-M_1)$  is a module polynomial and  $-a_1 \in A$  is a constant.
- $P_1 + P_2$  agrees with  $(M_1 + a_1) + (M_2 + a_2) = (M_1 + (a_1 + M_2 - a_1)) + (a_1 + a_2) = (M_1 + \gamma_{q_1} \circ M_2) + (a_1 + a_2)$  on  $U^n$ . Note that  $M_1 + \gamma_{q_1} \circ M_2$  is a module polynomial and  $a_1 + a_2 \in A$  is a constant.
- $F(P_1, \dots, P_m)$  agrees with  $F(M_1 + a_1, \dots, M_m + a_m)$  on  $U^n$ . We may expand this using identity (2.2) to obtain

$$F(\mathbf{M} + \mathbf{a}) = \left( \sum_{\text{lex}} F(\mathbf{M}/\mathbf{a}) \right) + F(\mathbf{a}).$$

Since  $F(\mathbf{a}) \in A$  is a constant, it suffices to show that the restriction of  $\sum_{\text{lex}} F(\mathbf{M}/\mathbf{a})$  to  $U^n$  is a module polynomial. If one substitutes values from  $U$  for the variables of  $\sum_{\text{lex}} F(\mathbf{M}/\mathbf{a})$ , each  $M_i$  assumes a value in  $U$ , so if in some summand  $F(\mathbf{M}/\mathbf{a})$  at least two places are occupied by  $M$ 's, then the fact that  $[U, U] = 0$  implies that the summand assumes the value 0. It is part of the notation that at least one place in each summand  $F(\mathbf{M}/\mathbf{a})$  is occupied by some  $M$ . Hence the restriction of  $\sum_{\text{lex}} F(\mathbf{M}/\mathbf{a})$  to  $U^n$  agrees with  $\sum_{i=1}^m F(a_1, \dots, a_{i-1}, M_i, a_{i+1}, \dots, a_n)$ . If  $F = F_r$ , then on  $U^n$  we have

$$\begin{aligned} \sum_{\text{lex}} F(\mathbf{M}/\mathbf{a}) &= \sum_{i=1}^m F(a_1, \dots, a_{i-1}, M_i, a_{i+1}, \dots, a_m) \\ &= \sum_{i=1}^m F_r(\hat{q}_1, \dots, \hat{q}_{i-1}, M_i, \hat{q}_{i+1}, \dots, \hat{q}_m) \\ &= \sum_{i=1}^m T_{\mathbf{q}}^{(r,i)} \circ M_i, \end{aligned}$$

which is a module polynomial.

To complete the proof, observe (by substituting 0 for all variables) that a function of the form  $M(x_1, \dots, x_n) + a$  maps  $U^n$  into  $U$  iff  $a \in U$  iff  $M(x_1, \dots, x_n) + a$  is a polynomial of the  $R_{Q,U}$ -module  $U$ .  $\square$

The enveloping ring of  $Q$  will be a ring that encodes all rings  $R_{Q,U}$  as  $U$  varies. It is defined relative to some variety containing  $Q$ , and is a specialization of the kind of ring introduced in Chapter 9 of [2].

**Definition 5.2.** Let  $\mathcal{V}$  be a variety of generalized nonassociative algebras. If  $Q \in \mathcal{V}$ , then the *enveloping ring of  $Q$  (relative to  $\mathcal{V}$ )* is the ring  $R_Q$  (or  $R_Q^{\mathcal{V}}$ ) presented by  $\langle G \mid R \rangle$  where the generators are the symbols  $\gamma_q$  and  $T_{\mathbf{q}}^{(i,j)}$  and the relations are those satisfied by all rings  $R_{Q,U}$  arising from exact sequences  $0 \rightarrow U \rightarrow A \rightarrow Q \rightarrow 0$  with  $A \in \mathcal{V}$  and  $[U, U] = 0$ .

If  $Q \in \mathcal{V} \subseteq \mathcal{W}$ , where  $\mathcal{V}$  and  $\mathcal{W}$  are varieties of generalized nonassociative algebras, then  $R_Q^{\mathcal{V}}$  has the same set of generators as  $R_Q^{\mathcal{W}}$  but more relations, hence is a quotient ring. It may be difficult to know exactly what ring  $R_Q^{\mathcal{V}}$  is, but is sometimes easy to identify rings that map onto  $R_Q^{\mathcal{V}}$  by identifying rings presented by the same generators and a subset of the most obvious relations.

**Example 5.3.** (The enveloping ring of a group) Let  $\mathcal{W}$  be the variety of pure groups and let  $Q \in \mathcal{W}$  be a member. Since there are no additional multilinear operations, the enveloping ring of  $R$  is generated by symbols  $\{\gamma_q \mid q \in Q\}$ . If  $q + r = s$  in  $Q$ , then the relation

$$(5.1) \quad \gamma_q \circ \gamma_r = \gamma_s,$$

which records the group operation, holds in any  $R_{Q,U}$ , hence is among the defining relations of  $R_Q$ . The presentation whose generators are  $\{\gamma_q \mid q \in Q\}$  and whose relations are those in (5.1) is the standard presentation of the integral group ring  $\mathbb{Z}[Q]$ . Hence  $R_Q^{\mathcal{W}}$  is a homomorphic image of  $\mathbb{Z}[Q]$ . But in fact it is an isomorphic image, since we can construct an exact sequence  $0 \rightarrow U \rightarrow A \rightarrow Q \rightarrow 0$  with  $A \in \mathcal{W}$  and  $[U, U] = 0$  showing that no other relations hold. For this, take  $U = \langle \mathbb{Z}[Q]; +, -, 0 \rangle$  to be the additive group of  $\mathbb{Z}[Q]$ , let  $Q$  act on  $U$  by left multiplication, then form the corresponding semidirect product  $A = U \rtimes Q$ . It is clear that  $U$  is an abelian ideal of  $A$ , and that the ring generated by the functions of the form  $\gamma_q$  acting on  $U$  (i.e., the left multiplications by elements of  $Q$ ) generate a ring isomorphic to  $\mathbb{Z}[Q]$ .

On the other hand, suppose that  $\mathcal{A} \subseteq \mathcal{V}$  is the subvariety of abelian groups and  $Q \in \mathcal{A}$ . While the enveloping ring of  $Q$  relative to  $\mathcal{V}$  is  $\mathbb{Z}[Q]$ , the enveloping ring of  $Q$  relative to  $\mathcal{A}$  is just  $\mathbb{Z}$ . This is because the enveloping ring is generated by the same elements, but in an abelian group each conjugation function  $\gamma_q \in R_{Q,U}$  is the identity function, so among the relations defining  $R_Q$  are the relations saying that all generators equal the identity. This much shows that  $R_Q$  is a quotient of  $\mathbb{Z}$ , but consideration of the sequence  $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z} \times Q \rightarrow Q \rightarrow 0$  shows that  $R_Q \cong \mathbb{Z}$ .

**Example 5.4.** (The enveloping ring of a nonunital associative ring) A nonunital associative ring is an abelian group expanded by a single bilinear operation  $F_1(x, y) = xy$  that is associative. If  $\mathcal{V}$  is the variety of all nonunital associative rings,  $0 \rightarrow U \rightarrow A \rightarrow Q \rightarrow 0$  is exact with  $A \in \mathcal{V}$ ,  $[U, U] = 0$ , and  $Q$  finite, then the ring  $R_{Q,U}$  is generated by the restrictions to  $U$  of the conjugations  $\gamma_q$ , and the left and right multiplications  $T_c^{(1,1)}(x) = cx$  and  $T_c^{(1,2)}(x) = xc$ . It is easily seen

that, whatever ring  $A$  is, these functions satisfy relations expressing that all conjugations equal the identity function (since the additive group of a ring is abelian), all left multiplications commute with all right multiplications (since multiplication is associative), the left multiplications and identity function generate a subring of  $R_{Q,U}$  that is a homomorphic image of  $Q^1$  (the universal unital ring of  $Q$  of the same characteristic), and the right multiplications comprise a subring of  $R_{Q,U}$  that is a homomorphic image of  $(Q^1)^{op}$ . This is enough to deduce that for any choice of exact sequence ending in  $Q$  with abelian kernel the ring  $R_{Q,U}$  is a homomorphic image of  $Q^1 \otimes_{\mathbb{Z}} (Q^1)^{op}$ . Since the relations we have identified are independent of  $U$ ,  $R_Q$  is itself a homomorphic image of  $Q^1 \otimes_{\mathbb{Z}} (Q^1)^{op}$ . This is all we shall need to know about  $R_Q$  for later application.

**Example 5.5.** (The enveloping ring of a Lie algebra) A Lie algebra over a field  $k$  is an abelian group expanded by a family of unary endomorphisms  $F_r(x)$ ,  $r \in k$ , and a single bilinear operation  $F(x, y) = [x, y]$ , such that a number of identities are satisfied. These identities state that the binary operation  $F$  is alternating and satisfies the Jacobi identity, and also that it is bilinear with respect to the unary operations:  $F(F_r(x) + F_s(y), z) = F_r(F(x, z)) + F_s(F(y, z))$ . If  $k$  is a finite field the variety  $\mathcal{V}$  of Lie algebras over  $k$  has finite type. (Note that a nontrivial variety of Lie algebras over a field  $k$  cannot be residually finite unless  $k$  is finite, since the 1-dimensional Lie algebra over  $k$  is residually finite only in this case.)

If  $0 \rightarrow U \rightarrow A \rightarrow Q \rightarrow 0$  is exact with  $A \in \mathcal{V}$ ,  $[U, U] = 0$ , and  $Q$  finite, then the ring  $R_{Q,U}$  is generated by the restrictions to  $U$  of the conjugations  $\gamma_q$ , the unary endomorphisms  $F_r$ , and the left and right multiplications  $T_c^{(1,1)}(x) = [c, x]$  and  $T_c^{(1,2)}(x) = [x, c]$ . These functions satisfy relations expressing that all conjugations

equal the identity function. The unary operations satisfy relations that encode the field structure:  $F_1 = \text{id}$ ,  $F_{r+s} = F_r + F_s$ , and  $F_{r \cdot s} = F_r \circ F_s$ . Since the binary operation is alternating,  $T_c^{(1,1)}(x) = [c, x] = \text{ad } c(x) = -[x, c] = -T_c^{(1,2)}(x)$ , and this relation allows us to eliminate the right multiplications from the generating set for  $R_{Q,U}$ , and in fact take the translations  $\text{ad } c$ ,  $c \in Q$ , as our set of generators. The bilinearity of the Lie bracket guarantees that if an element  $d$  is a linear combination of elements  $c_1, \dots, c_n$ , say  $d = \sum F_{r_i}(c_i)$ , then  $\text{ad } d = \sum F_{r_i} \circ \text{ad } c_i$ . Finally, the Jacobi identity guarantees that if  $[c, d] = e$ , then the relation  $\text{ad } e = \text{ad } c \circ \text{ad } d - \text{ad } d \circ \text{ad } c$  holds among the generators of  $R_{Q,U}$ . We have not proven that the relations discovered so far exhaust all relations satisfied by  $R_{Q,U}$ , but the relations that we have exhibited among the generators  $F_r$  and  $\text{ad } c$  suffice to prove that  $R_{Q,U}$  is a quotient of  $U(Q)$ , the usual universal enveloping algebra of  $Q$ . Since the relations we have identified are independent of the ideal  $U$ ,  $R_Q$  is itself a quotient of  $U(Q)$ .

Now we prove the main theorem of the paper.

**Theorem 5.6.** *If  $\mathcal{V}$  is a residually finite variety of generalized nonassociative algebras of finite type, then the following conditions are equivalent.*

- (1)  $\chi_{\mathcal{V}} < \omega$ .
- (2)  $\mathcal{V}$  is generated by a single finite algebra.
- (3) The enveloping ring of any finite algebra in  $\mathcal{V}$  is finite.
- (4) The enveloping ring of any finite algebra in  $\mathcal{V}$  is a finitely generated module over its center.

*Proof.* [(1) $\Rightarrow$ (2)] If  $\chi_{\mathcal{V}}$  is finite, then since  $\mathcal{V}$  is of finite type there only finitely many algebras in  $\mathcal{V}$  of cardinality  $< \chi_{\mathcal{V}}$ , so  $\mathcal{V}$  contains finitely many SI algebras, all of which are finite. Their product is a finite algebra that generates  $\mathcal{V}$ .



[(2) $\Rightarrow$ (3)] If  $\mathcal{V}$  is generated by a finite algebra, then  $\mathcal{V}$  is locally finite. If  $0 \rightarrow U \rightarrow A \rightarrow Q \rightarrow 0$  is exact with  $A \in \mathcal{V}$ ,  $[U, U] = 0$  and  $Q$  finite, then the ring  $R_{Q,U}$  is generated by (the restrictions to  $U$  of) unary polynomial functions of  $A$  which involve at most  $|Q|$  parameters. The total number of such functions is no greater than the size of the free algebra  $\mathbf{F}_{\mathcal{V}}(|Q| + 1)$ , which by local finiteness is some finite cardinal, say  $N$ . Thus,  $R_Q^{\mathcal{V}}$  satisfies all relations that hold in all rings of size  $\leq N$ , hence  $R_Q^{\mathcal{V}}$  belongs to the variety of rings generated by all rings of size  $\leq N$ . This variety of rings is a finitely generated variety, so  $R_Q^{\mathcal{V}}$  is locally finite. Since  $\mathcal{V}$  has finite type,  $R_Q^{\mathcal{V}}$  is finitely generated, hence it is finite.

[(3) $\Rightarrow$ (4)] Any finite ring is a finite module over its center.

[(4) $\Rightarrow$ (1)] We prove this implication by contradiction. Assume that (1) fails, so that  $\chi_{\mathcal{V}} = \omega$ .  $\mathcal{V}$  has infinitely many SI's, all finite; let  $A_1, A_2, \dots$  be a representative list of them. As before, let  $M_i$  denote the monolith of  $A_i$  and let  $N_i$  denote the annihilator of  $M_i$ . By Lemma 3.4, there is a finite number  $\ell$  that bounds all indices  $[A_i : N_i]$ , so the quotient algebras  $A_i/N_i$  have size  $\leq \ell$  for all  $i$ . Since  $\mathcal{V}$  is of finite type, there are only finitely many algebras of size  $\leq \ell$ , so there is one fixed algebra  $Q \in \mathcal{V}$  such that  $A_i/N_i \cong Q$  infinitely often. After thinning out the sequence  $A_1, A_2, \dots$  we may assume that  $A_i/N_i \cong Q$  for all  $i$ , and we may fix a homomorphism  $\beta_i: A_i \rightarrow Q$  that determines an exact sequence  $0 \rightarrow N_i \rightarrow A_i \xrightarrow{\beta_i} Q \rightarrow 0$  for each  $i$ . It follows from (C1) that  $[N_i, N_i] = 0$ , so each  $N_i$  is a  $Q$ -module.

The ideals of  $A_i$  that are contained in  $N_i$  are exactly the normal subgroups contained in  $N_i$  that are closed under translation. This means that they are exactly the  $R_{Q,N_i}$ -submodules of  $N_i$ . Since the interval  $[0, N_i]$  of the ideal lattice has a smallest nonzero member  $M_i$ , it follows that each  $N_i$  is an SI  $R_{Q,N_i}$ -module. The action of  $R_Q$  on  $N_i$  is obtained by restriction of scalars via the natural homomorphism

$\nu_i: R_Q \rightarrow R_{Q,U}$  guaranteed by the universal property of presentations. ( $R_Q$  has the same generators as  $R_{Q,U}$ , but only a subset of the relations.) Since  $\nu_i$  is surjective, each  $N_i$  is subdirectly irreducible as an  $R_Q$ -module.

**Claim 5.7.** *There is a submodule  $K$  of some product  $\prod N_j$  such that  $(\prod N_j)/K$  is an infinite SI  $R_Q$ -module.*

The assumption in (4) of this theorem implies that  $R_Q$  is a finitely generated module over its center. By Corollary 4.5, no variety of  $R_Q$ -modules has residual character  $\omega$ . Since the  $N_i$ 's are examples of arbitrarily large finite SI  $R_Q$ -modules, the variety  $\text{HSP}(\{N_i \mid i \in \omega\})$  must therefore contain an infinite SI  $R_Q$ -module, say  $S$ . There must exist submodules  $B \leq C \leq \prod N_j$  such that  $C/B \cong S$ . If  $K$  is a submodule of  $\prod N_j$  that is maximal with respect to the condition that  $C \cap K = B$ , then  $S \cong C/(C \cap K) \cong (C + K)/K \leq (\prod N_j)/K$ , so  $(\prod N_j)/K$  is an extension of the infinite SI module  $S$ . The maximality of  $K$  guarantees that  $(\prod N_j)/K$  is an essential extension of the SI  $S$ , so  $(\prod N_j)/K$  is SI itself.

Next we use the result of Claim 5.7 to produce an infinite SI nonassociative algebra in  $\mathcal{V}$ . In this claim we did not specify precisely which product we were considering — some  $N_i$ 's may not have appeared as factors and others may have appeared multiple times — so fix now an index set  $J$  such that  $\prod N_j = \prod_{j \in J} N_j$ . Now consider the subalgebra  $D \leq \prod_{j \in J} A_j$  consisting of all tuples  $\mathbf{d}$  such that  $\beta_i(d_i) = \beta_j(d_j)$  for all  $i, j \in J$ . Then the function  $\beta: D \rightarrow Q: \mathbf{d} \mapsto \beta_i(d_i)$  is a well-defined homomorphism, which is surjective since each  $\beta_i$  is surjective. This homomorphism determines an exact sequence  $0 \rightarrow U \rightarrow D \xrightarrow{\beta} Q \rightarrow 0$  where  $U = \ker(\beta)$  consists of all tuples  $\mathbf{d} \in \prod_{j \in J} A_j$  such that  $\beta_i(d_i) = 0$  for all  $i$ , in other words  $U = \prod_{j \in J} N_j$ . The ideal  $U \subseteq D$  is easily seen to satisfy  $[U, U] = 0$  using Definition 2.5: the tuples in  $U$

commute because they commute coordinatewise, and if  $F$  is multilinear,  $d_i \in D$ , and there exist  $i \neq k$  such that  $d_i, d_k \in U = \prod_{j \in J} N_j$ , then  $F(d_1, \dots, d_n) = 0$  because it is zero in each coordinate. (In each coordinate, then  $i$ th and  $j$ th entries are from  $U$ .)

Thus  $U$  is an  $R_Q$ -module. An examination of how conjugation and translation behave on the set  $U = \prod_{j \in J} N_j$  shows that  $U$  equals the product  $\prod_{j \in J} N_j$  as a module. In particular, the submodule  $K$  of Claim 5.7 is an ideal of  $D$  contained in  $U$ . Extend  $K$  to an ideal  $L \leq D$  that is maximal for  $U \cap L = K$ . Then  $D/L$  is SI and contains the infinite ideal  $U/(U \cap L) = U/K = (\prod_{j \in J} N_j)/K$ . This contradicts the assumption that  $\mathcal{V}$  is residually finite. The proof is complete.  $\square$

**Corollary 5.8.** *If  $\mathcal{V}$  is a locally finite and residually finite variety of generalized nonassociative algebras of finite type, then  $\mathcal{V}$  is generated by a single finite algebra.*

*Proof.* As noted in the proof of Theorem 5.6, (2) $\Rightarrow$ (3), if  $\mathcal{V}$  is locally finite and of finite type, then the enveloping ring of any finite  $Q \in \mathcal{V}$  is finite.  $\square$

**Corollary 5.9.** *(Olshanskii) Any residually finite variety of groups is generated by a single finite group.*

*Proof.* It suffices to show that the enveloping ring of a finite group  $Q$  relative to the variety of all groups is a finitely generated module over its center. We showed in example (5.3) that this ring is isomorphic to  $\mathbb{Z}[Q]$ , which is generated as a module over its center by the finite set  $Q$ .  $\square$

**Corollary 5.10.** *Any residually finite variety of nonunital associative rings is generated by a single finite ring.*

*Proof.* It suffices to show that the enveloping ring of a nonunital associative ring  $Q$  relative to the variety of all such rings is finite. We showed in example (5.4) that the enveloping ring of  $Q$  is a quotient of  $Q^1 \otimes (Q^1)^{op}$ , which is a finite ring if  $Q$  is.  $\square$

**Corollary 5.11.** (*Premet and Semenov, for characteristics  $\geq 5$* ) *Any residually finite variety of Lie algebras is generated by a single finite Lie algebra.*

*Proof.* It suffices to show that the enveloping ring of a finite Lie algebra  $Q$  over the field  $k$ , relative to the variety of all Lie algebras over  $k$ , is a finitely generated module over its center. We showed in example (5.5) that this ring  $R_Q$  is a quotient of the classical universal enveloping algebra  $U(Q)$  of  $Q$ . It suffices therefore to prove that  $U(Q)$  itself is a finitely generated module over its center since this property is inherited by quotients. But in essence this has already been done by Jacobson. In Proposition 1 of his paper [4] he shows that for any element  $\text{ad } c$ ,  $c \in Q$ , there is a polynomial  $p(x) \in k[x]$  such that  $p(\text{ad } c) \in Z(U(Q))$ . Applying this to the normal form provided by the PBW Theorem this proves that the finitely generated algebra  $U(Q)$  is generated as a module over its center by monomials of bounded total degree, hence  $U(Q)$  is a finitely generated module over its center.  $\square$

We close this paper with a remark connected to the discussion in the introduction of this paper. We stated there that for any variety  $\mathcal{V}$ , (1) it is decidable whether there is a nontrivial lattice identity valid in the congruence lattices of all members of  $\mathcal{V}$ , and (2) if such an identity is satisfied, then it is decidable whether  $\mathcal{V}$  is residually finite. From this it is natural to ask whether the result of this paper extends to the more general setting of varieties satisfying nontrivial congruence identities. It has recently been announced by R. D. Willard and the first author that it does extend. The announced extension improves upon our Theorem 5.6 by generalizing its scope,

and also by proving that the conditions in Theorem 5.6 are not merely equivalent, *but are true* (when  $\mathcal{V}$  is residually finite, as is assumed there).

## REFERENCES

- [1] R. Freese and R. McKenzie, *Residually small varieties with modular congruence lattices*. Trans. Amer. Math. Soc. **264** (1981), no. 2, 419–430.
- [2] R. Freese and R. McKenzie, *Commutator theory for congruence modular varieties*. London Mathematical Society Lecture Note Series, **125**. Cambridge University Press, Cambridge, 1987.
- [3] D. Hobby and R. McKenzie, *The structure of finite algebras*. Contemporary Mathematics, **76**. American Mathematical Society, Providence, RI, 1988.
- [4] N. Jacobson, *A note on Lie algebras of characteristic  $p$* . Amer. J. Math. **74**, (1952), 357–359.
- [5] K. A. Kearnes, *Residual bounds for varieties of modules*. Algebra Universalis **28** (1991), no. 3, 448–452.
- [6] K. A. Kearnes, *A characterization of locally finite varieties that satisfy a nontrivial congruence identity*. Algebra Universalis **42** (1999), no. 3, 195–204.
- [7] K. A. Kearnes and R. Willard, *Residually finite, congruence meet-semidistributive varieties of finite type have a finite residual bound*. Proc. Amer. Math. Soc. **127** (1999), no. 10, 2841–2850.
- [8] R. McKenzie, *The residual bound of a finite algebra is not computable*. Internat. J. Algebra Comput. **6** (1996), no. 1, 29–48.
- [9] R. McKenzie, *Recursive inseparability for residual bounds of finite algebras*. J. Symbolic Logic **65** (2000), no. 4, 1863–1880.
- [10] R. N. McKenzie, G. F. McNulty and W. F. Taylor, *Algebras, lattices, varieties. Vol. I*. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1987.
- [11] A. Ju. Olshanskii, *Varieties of finitely approximable groups*. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **33** 1969 915–927.
- [12] A. A. Premet and K. N. Semenov, *Varieties of residually finite Lie algebras*. (Russian) Mat. Sb. (N.S.) 137(179) (1988), no. 1, 103–113, 144; translation in Math. USSR-Sb. **65** (1990), no. 1, 109–118.

(Keith Kearnes) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO, BOULDER CO  
80309, USA

*E-mail address:* kearnes@euclid.colorado.edu

(Young Jo Kwak) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO, BOULDER  
CO 80309, USA

*E-mail address:* Young.Kwak@Colorado.EDU