

PRINCIPAL AND SYNTACTIC CONGRUENCES IN CONGRUENCE-DISTRIBUTIVE AND CONGRUENCE-PERMUTABLE VARIETIES

BRIAN A. DAVEY, MARCEL JACKSON[✉], MIKLÓS MARÓTI
and RALPH N. MCKENZIE

(Received 30 August 2006; accepted 23 February 2007)

Communicated by D. Easdown

Abstract

We give a new proof that a finitely generated congruence-distributive variety has finitely determined syntactic congruences (or, equivalently, term finite principal congruences), and show that the same does not hold for finitely generated congruence-permutable varieties, even under the additional assumption that the variety is residually very finite.

2000 *Mathematics subject classification*: 08B10.

Keywords and phrases: finitely determined syntactic congruences, term finite principal congruences, finite principal length, congruence distributive, congruence modular, congruence permutable.

1. Introduction

The notion of *term finite principal congruences* (TFPC) was introduced by Clark *et al.* [6] and is a natural generalisation of definable principal congruences: instead of bounding the number of different principal-congruence formulae, we bound only the set of possible terms appearing in such formulae. This property is very closely related to several other congruence conditions. For example, a variety of algebras of finite signature has TFPC if and only if it has *finite Mal'cev depth*, also known as *finite principal length*, as studied by Wang [17]. These properties have been used by Baker *et al.* [2] and by Baker and Wang [3] to establish finite basis theorems for the equations of finite algebras. More locally, an individual algebra has TFPC if and only if it has *finitely determined syntactic congruences* (FDSC), a property that arises naturally in the study of compact topological algebras [6]. For example, a Boolean

The second author was supported by ARC Discovery Project Grant DP0342459. The third author was partially supported by the Hungarian National Foundation for Scientific Research (OTKA), grant nos. T 37877 and T 48809.

© 2008 Australian Mathematical Society 1446-7887/08 \$A2.00 + 0.00

topological algebra with FDSC is topologically residually finite (see [10], [13, Lemma VI.2.7] or [6, Lemma 4.2]). Moreover, FDSC is the most general known structural property guaranteeing topological residual finiteness (algebraic residual finiteness is not sufficient in general; see Jackson [12]). The notion of FDSC arises naturally in the study of the axiomatisability of classes of Boolean topological algebras [8].

Wang [17] showed that every finitely generated congruence-distributive variety of finite signature has finite Mal'cev depth and consequently also has TFPC and FDSC. (An updated version of Wang's proof, in English, appears in Baker and Wang [3].) Thus, every finitely generated variety of lattices has TFPC and FDSC. On the other hand, Clindenbeard [9] gave an example of a Boolean topological modular lattice that is not topologically residually finite. So the variety of modular lattices (and any larger variety) has neither TFPC nor FDSC.

We present a new proof of Wang's result that avoids any assumption on the signature. To contrast this result, we construct a four-element nonassociative algebra over GF(2) that generates a variety that is congruence permutable and residually very finite (that is, has a finite bound on the size of its subdirectly irreducible algebras) but fails to have FDSC.

2. Preliminaries

Let \mathcal{V} be a variety of algebras. Let $\mathbf{A} \in \mathcal{V}$ be an algebra and $c, d \in A$. We write $\text{cg}_{\mathbf{A}}(c, d)$ to denote the smallest congruence of \mathbf{A} containing the pair (c, d) . For $m \in \omega$, let $T_x^{(m)}$ denote the set of all $(m+1)$ -variable terms $t(x, z_1, \dots, z_m)$ in the signature of \mathcal{V} , and let T_x denote the union of the sets $T_x^{(m)}$, for $m \in \omega$.

Mal'cev's lemma (see Burris and Sankappanavar [4, V.3.1], for example) states that $(a, b) \in \text{cg}_{\mathbf{A}}(c, d)$ if and only if there exist:

- (1) nonnegative integers k and m ;
- (2) elements $a = a_1, \dots, a_{k+1} = b$ in A ;
- (3) terms $t_1(x, z_1, \dots, z_m), \dots, t_k(x, z_1, \dots, z_m)$ in T_x ; and
- (4) elements $e_{1,1}, \dots, e_{1,m}, \dots, e_{k,1}, \dots, e_{k,m}$ in A ;

such that, for all $i \in \{1, \dots, k\}$,

$$\{t_i^{\mathbf{A}}(c, e_{i,1}, \dots, e_{i,m}), t_i^{\mathbf{A}}(d, e_{i,1}, \dots, e_{i,m})\} = \{a_i, a_{i+1}\}.$$

Let $F \subseteq T_x$. Given an algebra \mathbf{A} and $c, d \in A$, we say that F determines the principal congruence $\text{cg}_{\mathbf{A}}(c, d)$ if, for all $(a, b) \in \text{cg}_{\mathbf{A}}(c, d)$, the terms $t_i(x, z_1, \dots, z_m)$ in (3) above can all be chosen from F . Likewise, F determines the principal congruences on \mathbf{A} if it determines each principal congruence of \mathbf{A} , and F determines principal congruences in a class \mathcal{K} if F determines the principal congruences on each member of \mathcal{K} .

Clearly T_x determines principal congruences in any class of algebras of the appropriate signature; however, it is common that some subset of T_x suffices. The singleton $\{z_1 x z_2\}$ is sufficient to determine principal congruences in the variety of groups for example; see [6] for many other examples.

We say that a class \mathcal{K} of algebras has TFPC if there is a finite subset of T_x that determines principal congruences in \mathcal{K} .

The congruence condition TFPC is a natural generalisation of definable principal congruences: a variety \mathcal{V} has first-order *definable principal congruences* if and only if we can fix a finite bound on the length m of the chain in item (2) of Mal'cev's lemma, as well as fixing a finite set $F \subseteq T_x$ for the possible choices of terms in item (3) (see [4, Exercise V.3.5] for example). There are many interesting results that can be proved in the presence of definable principal congruences; however, it is a rather special property. For example, a finite lattice generates a variety with definable principal congruences if and only if it is a distributive lattice [15]. On the other hand, we show that every finitely generated congruence-distributive variety has TFPC.

Finite Mal'cev depth is defined by specifying the subset of T_x that should determine principal congruences in \mathcal{V} : a variety \mathcal{V} has *finite Mal'cev depth* k if principal congruences on algebras in \mathcal{V} are determined by the subset of T_x consisting of terms of nesting depth (in terms of fundamental operations) at most k .

Finally, we wish to review the notion of finitely determined syntactic congruences. Let \mathbf{A} be an algebra and θ an equivalence relation on \mathbf{A} . The largest congruence contained in θ is called the *syntactic congruence of θ* and is denoted by $\text{syn}(\theta)$. For any subset $F \subseteq T_x$ we write θ_F to denote the relation given by $(a, b) \in \theta_F$ if and only if

$$(\forall t \in F)(\forall e_0, e_1, \dots \in A)(t^{\mathbf{A}}(a, e_1, e_2, \dots), t^{\mathbf{A}}(b, e_1, e_2, \dots)) \in \theta.$$

The relation θ_F is an equivalence relation and satisfies $\text{syn}(\theta) \subseteq \theta_F$. Moreover, $\text{syn}(\theta) = \theta_{T_x}$. We say that F *determines* $\text{syn}(\theta)$ if $\theta_F = \text{syn}(\theta)$. The set F *determines syntactic congruences on \mathbf{A}* if $\theta_F = \text{syn}(\theta)$ for every equivalence relation θ on \mathbf{A} , and we say that F *determines syntactic congruences in a class \mathcal{K}* if F determines syntactic congruences on each member of \mathcal{K} . If there is a finite set $F \subseteq T_x$ that determines syntactic congruences in \mathcal{K} , then we say that \mathcal{K} has *finitely determined syntactic congruences* (FDSC).

The name syntactic congruence has its roots in the theory of formal languages (see the discussion at the start of [6, Section 2]), and the property FDSC has quite a lengthy history in relation to topological residual finiteness: see [1, 5, 6, 10, 13], for example.

The following lemma is obvious but useful.

LEMMA 2.1. *Let $F \subseteq T_x$ and let $t(x, z_1, \dots, z_k)$ and $s(x, z_1, \dots, z_k)$ be terms in T_x . If the set $F \cup \{t(x, z_1, \dots, z_k)\}$ determines principal congruences in a class \mathcal{K} that satisfies $t(x, z_1, \dots, z_k) \approx s(x, z_1, \dots, z_k)$, then the set $F \cup \{s(x, z_1, \dots, z_k)\}$ also determines principal congruences in \mathcal{K} .*

The definition of FDSC is certainly reminiscent of that of TFPC, but much more is true.

LEMMA 2.2 [6, Lemma 2.3]. *A subset F of T_x determines syntactic congruences on an algebra \mathbf{A} if and only if it determines principal congruences on \mathbf{A} .*

In particular, a class \mathcal{K} of algebras has FDSC if and only if it has TFPC. The proof of Lemma 2.2 is based on the following lemma, which is useful in its own right.

LEMMA 2.3 [6, Lemma 2.2]. *Let \mathbf{A} be an algebra and θ be an equivalence relation on \mathbf{A} . For all $a, b \in A$, we have $(a, b) \in \text{syn}(\theta)$ if and only if $\text{cg}_{\mathbf{A}}(a, b) \subseteq \theta$.*

We require the following equational characterisation of when a subset F of T_x determines syntactic congruences in a variety.

LEMMA 2.4 [6, Section 3]. *Let \mathcal{K} be a class of algebras and assume that \mathbf{W}_ω is an ω -generated \mathcal{K} -free algebra. The following are equivalent for a subset F of T_x :*

- (1) *F determines syntactic congruences in \mathcal{K} ;*
- (2) *F determines syntactic congruences on \mathbf{W}_ω ;*
- (3) *for every term $t(x, z_1, \dots, z_n)$ in T_x , there exists $\ell \in \omega$, there exist terms $s_1(x, z_1, \dots, z_m), \dots, s_\ell(x, z_1, \dots, z_m)$ in F and there exist $m\ell$ terms $w_{i,j}(x, y, z_1, \dots, z_m)$, for $1 \leq i \leq \ell$ and $1 \leq j \leq m$, such that \mathcal{K} satisfies the following equations:*

$$\begin{aligned} t(x, z_1, \dots, z_n) &\approx s_1(v_1, w_{1,1}, \dots, w_{1,m}), \\ &\vdots \\ s_i(v'_i, w_{i,1}, \dots, w_{i,m}) &\approx s_{i+1}(v_{i+1}, w_{i+1,1}, \dots, w_{i+1,m}), \\ &\vdots \\ s_\ell(v'_\ell, w_{\ell,1}, \dots, w_{\ell,m}) &\approx t(y, z_1, \dots, z_n), \end{aligned}$$

where $\{v_i, v'_i\} = \{x, y\}$, for $1 \leq i \leq \ell$.

Following [6], when a subset F of T_x and a term $t(x, z_1, \dots, z_n) \in T_x$ satisfy the conditions of this lemma, we say that F *shadows* $t(x, z_1, \dots, z_n)$. We close this section with two corollaries of Lemma 2.4.

COROLLARY 2.5. *Let \mathcal{K} be a class of algebras containing an ω -generated free algebra. Assume that F and G are subsets of T_x that determine syntactic congruences in \mathcal{K} . If G is finite, then there is a finite subset of F that determines syntactic congruences in \mathcal{K} .*

PROOF. By Lemma 2.4, the set F shadows every $t(x, z_1, \dots, z_n) \in G$. As each ‘shadowing’ of a term t in G involves only a finite subset F_t of F (the number ℓ in Lemma 2.4), the subset $\bigcup_{t \in G} F_t$ is a finite subset of F that determines syntactic congruences in \mathcal{K} . \square

COROLLARY 2.6. *Let \mathcal{V} be a variety and let F be a subset of T_x . If F determines syntactic congruences on the finitely generated \mathcal{V} -free algebras, then F determines syntactic congruences in \mathcal{V} .*

PROOF. It follows from Mal'cev's description of principal congruences that, for any algebra \mathbf{A} and elements $a, b, c, d \in A$, we have $(a, b) \in \text{cg}_{\mathbf{A}}(c, d)$ if and only if $(a, b) \in \text{cg}_{\mathbf{B}}(c, d)$, for some finitely generated subalgebra \mathbf{B} of \mathbf{A} that contains $\{a, b, c, d\}$. Hence, the class of algebras on which F determines principal congruences is closed under directed unions. As the countably generated \mathcal{V} -free algebra in \mathcal{V} is a union of a chain of finitely generated \mathcal{V} -free algebras, the result follows from Lemmas 2.2 and 2.4. \square

3. Congruence distributive varieties

Recall that a variety \mathcal{V} is congruence distributive if and only if there are terms $D_0(x, y, z), \dots, D_m(x, y, z)$, for some $m \geq 2$, such that \mathcal{V} satisfies the following Jónsson equations [14]:

$$D_0(x, y, z) \approx x; \tag{J1}$$

$$D_m(x, y, z) \approx z; \tag{J2}$$

$$D_i(x, y, x) \approx x; \tag{J3i}$$

$$D_i(x, x, y) \approx D_{i+1}(x, x, y) \text{ for } i \text{ even};$$

$$D_i(x, y, y) \approx D_{i+1}(x, y, y) \text{ for } i \text{ odd}. \tag{J4i}$$

Three-variable polynomials $d_0(x, y, z), \dots, d_m(x, y, z)$ on an algebra \mathbf{B} , for which the Jónsson equations hold, will be called *Jónsson polynomials*. Of course if \mathbf{B} lies in a congruence-distributive variety, then Jónsson terms will be Jónsson polynomials in \mathbf{B} . However, it is possible to have Jónsson polynomials on algebras that do not have Jónsson terms. This fact plays an important role in McKenzie's decidability results for finite algebras [16], which is one of the motivating reasons for presenting these ideas in this more general setting.

For an algebra \mathbf{B} and subset $F \subseteq T_x$, we use the notation $\text{Pol}_1^F(\mathbf{B})$ to denote the unary polynomials $p(x)$ on \mathbf{B} that arise as $t^{\mathbf{B}}(x, e_1, \dots, e_m)$, for some $t(x, z_1, \dots, z_m) \in F$ and $e_1, \dots, e_m \in B$. To simplify the notation, we denote finite sequences of elements or variables, of unspecified length $n \in \omega$, by \vec{c} . Note that, while c_i stands for the i th element of the sequence \vec{c} , the notation \vec{c}_i is an abbreviation for a finite sequence $c_{i,1}, c_{i,2}, \dots$.

LEMMA 3.1. *Let \mathcal{K} be a class of algebras and assume that $F \subseteq T_x$ determines syntactic congruences in \mathcal{K} . Assume that \mathbf{B} is a subdirect product of finitely many algebras from \mathcal{K} and that \mathbf{B} has Jónsson polynomials $d_0(x, y, z), \dots, d_m(x, y, z)$ built from terms $D_0(x, y, z, \vec{w}), \dots, D_m(x, y, z, \vec{w})$, for some $m \geq 2$. The subset*

$$F^+ := \{D_j(y_1, t(x, \vec{z}), y_2, \vec{w}) \mid 0 \leq j \leq m \text{ and } t(x, \vec{z}) \in F\}$$

of T_x determines syntactic congruences on \mathbf{B} .

PROOF. Assume that for some $\ell > 0$, the algebra \mathbf{B} is a subdirect product of $\mathbf{M}_1, \dots, \mathbf{M}_\ell$, with $\mathbf{M}_i \in \mathcal{K}$ for all i . Suppose, by way of contradiction, that θ is an equivalence relation on B and that F^+ does not determine the congruence $\text{syn}(\theta)$. Thus, there exists $(e, f) \in \theta_{F^+} \setminus \text{syn}(\theta)$. By the definition of θ_{F^+} and Lemma 2.3, we have $(p(e), p(f)) \in \theta$, for all $p \in \text{Pol}_1^{F^+}(\mathbf{B})$, but $\text{cg}_{\mathbf{B}}(e, f) \not\subseteq \theta$. For $u \in B$, we denote the i th coordinate on u by $u[i]$ and, for $u, v \in B$, we define

$$\llbracket u = v \rrbracket := \{i \in \{1, \dots, \ell\} \mid u[i] = v[i]\}.$$

Assume that $(a, b) \in \text{cg}_{\mathbf{B}}(e, f) \setminus \theta$ and the size of $E := \llbracket a = b \rrbracket$ is maximal over all such pairs. Without losing generality, we may assume that $a[1] \neq b[1]$, whence $1 \notin E$. We shall derive the contradiction $(a, b) \in \theta$.

We have $(a[1], b[1]) \in \text{cg}_{\mathbf{M}_1}(e[1], f[1])$. Since, by Lemma 2.2, the set F determines principal congruences on \mathbf{M}_1 , there is a chain of elements in M_1 , say $a[1] = a_1, \dots, a_{k+1} = b[1]$, such that, for all $i \in \{1, \dots, k\}$, we have $\{q_i(e[1]), q_i(f[1])\} = \{a_i, a_{i+1}\}$, where $q_i(x) = t_i^{\mathbf{M}_1}(x, \vec{c}_i)$, for some term $t_i(x, \vec{z}) \in F$ and finite sequence \vec{c}_i of elements of M_1 . As the projection from \mathbf{B} to \mathbf{M}_1 is surjective, for each $i \in \{1, \dots, k\}$, there is a finite sequence \vec{g}_i of elements of B with $g_{i,j}[1] = c_{i,j}$, for all $j = 1, 2, \dots$.

Let $p_i(x)$ denote the polynomial of \mathbf{B} given by $t_i^{\mathbf{B}}(x, \vec{g}_i)$, and fix $j \leq m$. For all $i \in \{1, \dots, k\}$, we have $d_j(a, t_i^{\mathbf{B}}(x, \vec{g}_i), b) \in \text{Pol}_1^{F^+}(\mathbf{B})$, whence

$$d_j(a, t_i^{\mathbf{B}}(e, \vec{g}_i), b) \theta d_j(a, t_i^{\mathbf{B}}(f, \vec{g}_i), b) \quad \text{for all } i \in \{1, \dots, k\}. \tag{*}$$

We now establish two claims.

CLAIM 1. For all $c, d \in B$ with $c[1] = d[1]$, we have $d_j(a, c, b) \theta d_j(a, d, b)$.

As $(a, b) \in \text{cg}_{\mathbf{B}}(e, f)$, the Jónsson equation (J3j) shows that

$$(d_j(a, c, b), d_j(a, d, b)) \in \text{cg}_{\mathbf{B}}(e, f).$$

Now $E \subseteq \llbracket d_j(a, c, b) = d_j(a, d, b) \rrbracket$, using Equation (J3j) again, while

$$1 \in \llbracket d_j(a, c, b) = d_j(a, d, b) \rrbracket$$

by assumption. As $1 \notin E$, the maximality assumption on the choice of $a, b \in B$ now shows that $d_j(a, c, b) \theta d_j(a, d, b)$.

CLAIM 2. We claim that $d_j(a, b, b) \theta d_j(a, a, b)$.

For notational convenience, we define elements $u_i, v_i \in B$, for $i \in \{1, \dots, k\}$, by

$$u_i := \begin{cases} e & \text{if } q_i(e[1]) = a_i \\ f & \text{if } q_i(f[1]) = a_i \end{cases} \quad \text{and} \quad v_i := \begin{cases} f & \text{if } q_i(f[1]) = a_{i+1} \\ e & \text{if } q_i(e[1]) = a_{i+1} \end{cases}$$

Note that, $p_i(u_i)[1] = q_i(u_i[1]) = a_i$ and $p_i(v_i)[1] = q_i(v_i[1]) = a_{i+1}$, for each $i \in \{1, \dots, k\}$. Hence, the horizontal relations in the following chain follow from Claim 1.

The vertical relations follow from (*). We show the case in which k is even, but the case where k is odd is similar and ends on the left instead of the right.

$$\begin{array}{ccc}
 d_j(a, a, b) & \theta & d_j(a, p_1(u_1), b) \\
 & & \theta \\
 d_j(a, p_2(u_2), b) & \theta & d_j(a, p_1(v_1), b) \\
 & & \theta \\
 d_j(a, p_2(v_2), b) & \theta & d_j(a, p_3(u_3), b) \\
 & & \theta \\
 \vdots & & \vdots \\
 & & \theta \\
 d_j(a, p_k(u_k), b) & \theta & d_j(a, p_{k-1}(v_{k-1}), b) \\
 & & \theta \\
 d_j(a, p_k(v_k), b) & \theta & d_j(a, b, b).
 \end{array}$$

By transitivity, we obtain $d_j(a, a, b) \theta d_j(a, b, b)$.

Now to complete the proof of the lemma. The following chain demonstrates how Claim 2 (vertically) and the Jónsson equations (J1), (J2) and (J4i) (horizontally) give the desired contradiction, namely $(a, b) \in \theta$. Here m is odd, but again the case in which m is even is similar:

$$\begin{array}{ccc}
 a = d_0(a, a, b) = d_1(a, a, b) & & \\
 & & \theta \\
 d_2(a, b, b) = d_1(a, b, b) & & \\
 & & \theta \\
 d_2(a, a, b) = d_3(a, a, b) & & \\
 & & \theta \\
 \vdots & & \vdots \\
 & & \theta \\
 d_{m-1}(a, b, b) = d_{m-2}(a, b, b) & & \\
 & & \theta \\
 d_{m-1}(a, a, b) = d_m(a, a, b) = b. & &
 \end{array}$$

This completes the proof. □

Appropriate finiteness conditions on the class \mathcal{K} in Lemma 3.1 guarantee that the set F can be chosen to be finite, in which case the set F^+ will also be finite.

LEMMA 3.2. Assume that \mathcal{K} consists of algebras of bounded finite cardinality $n \geq 1$.

- (i) The set $F = T_x^{(n)}$ determines syntactic congruences in \mathcal{K} .
- (ii) Assume that \mathcal{K} is a subset of a locally finite variety. Then there is a finite subset F of $T_x^{(n)}$ that determines syntactic congruences in \mathcal{K} .

PROOF. When Mal'cev's lemma is applied in an algebra of cardinality at most $n \in \omega$, each tuple $e_{i,0}, e_{i,1}, \dots, e_{i,m}$ in item (4) involves at most n distinct elements, and hence it suffices to choose terms in item (3) with at most $n + 1$ variables. This proves (i). If \mathcal{K} lies in a locally finite variety \mathcal{V} , then by Lemma 2.1 we need only choose one term from each equivalence class of the $(n+1)$ -generated \mathcal{V} -free algebra, whence (ii) follows. \square

Our main result now follows easily.

THEOREM 3.3. Let \mathbf{A} be a finite algebra and assume that the variety $\text{Var}(\mathbf{A})$ generated by \mathbf{A} is congruence distributive. Then $\text{Var}(\mathbf{A})$ has FDSC and TFPC.

PROOF. As \mathbf{A} is finite, by Corollary 2.6 it suffices to show that the class of finitely generated $\text{Var}(\mathbf{A})$ -free algebras has FDSC. Let \mathbf{W}_k denote the k -generated $\text{Var}(\mathbf{A})$ -free algebra.

The free algebra \mathbf{W}_k is a subdirect product of a finite set \mathcal{K} of algebras of cardinality at most $|A|$. (Indeed, \mathbf{W}_k is a subdirect product of subdirectly irreducible algebras in $\text{Var}(\mathbf{A})$, which by Jónsson's lemma [14] lie in the class $\mathbb{HS}(\mathbf{A})$. It is also a subalgebra of $\mathbf{A}^{|A|^{|X|}}$, and so is a subdirect product of algebras in $\mathbb{S}(\mathbf{A})$.) By Lemma 3.2(ii), there is a finite subset F of $T_x^{(|A|)}$ that determines syntactic congruences in \mathcal{K} . Hence, by Lemma 3.1 there is a finite subset F^+ of $T_x^{(|A|+2)}$ that determines syntactic congruences on \mathbf{W}_k . As the choice of F^+ depends only on \mathbf{A} , we conclude that F^+ determines syntactic congruences on every finitely generated $\text{Var}(\mathbf{A})$ -free algebra. Thus, $\text{Var}(\mathbf{A})$ has FDSC by Corollary 2.6, and so has TFPC by Lemma 2.2. \square

To get a bound on the number of terms required to determine syntactic congruences in $\text{Var}(\mathbf{A})$, let \mathbf{W}_k denote the k -generated $\text{Var}(\mathbf{A})$ -free algebra and let $|A| = n$. Note that $|W_k| \leq n^{n^k}$. When forming the subset F of $T_x^{(n)}$ used in the proof of Theorem 3.3, we need only pick one term $t(x, z_1, \dots, z_n)$ for each element of \mathbf{W}_{n+1} . Since the terms in F should depend on x , an upper bound for the number of terms required is $|W_{n+1}| - |W_n| \leq n^{n^{n+1}}$. Thus, if there are $m + 1$ Jónsson terms D_0, \dots, D_m , then

$$|F^+| = (m - 1)|F| \leq (m - 1)n^{n^{n+1}}.$$

If we do not know the number of Jónsson terms, then working in W_{n+3} gives $|F^+| \leq n^{n^{n+3}}$. One can also obtain an upper bound for the nesting depth of the terms required. Easy observations show that every term in F^+ is equivalent to one of nesting depth at most $n^{n^{n+3}}$. (Essentially, if t is represented in shortest fashion then no subterms of t can be equivalent in $\text{Var}(\mathbf{A})$ to a term of smaller depth. So the depth of t is bounded by the size of \mathbf{W}_{n+3} .) All of these bounds are probably excessive.

+	0	a	b	$a + b$	·	0	a	b	$a + b$
0	0	a	b	$a + b$	0	0	0	0	0
a	a	0	$a + b$	b	a	0	0	a	a
b	b	$a + b$	0	a	b	0	0	0	0
$a + b$	$a + b$	b	a	0	$a + b$	0	0	a	a

FIGURE 1.

4. Congruence permutable varieties

The variety of lattices is congruence distributive and, as we pointed out earlier, fails to have FDSC. However, the varieties of groups and of rings are congruence permutable and do have FDSC. This suggests some possible variants of Theorem 3.3. The proof of Theorem 3.3 does not make it clear precisely what role is played by the finite residual bound of a finitely generated congruence-distributive variety. (Having a finite residual bound is not a property shared by finitely generated congruence-permutable varieties.)

In this section we show that one obvious variant of Theorem 3.3 does not extend to congruence-permutable varieties. We find a four-element algebra \mathbf{A} generating a residually very finite congruence-permutable variety that fails to have FDSC.

Define $\mathbf{A} = \langle \{0, a, b, a + b\}; +, \cdot, 0 \rangle$, where $+$ and \cdot are given in Figure 1. The additive reduct of \mathbf{A} is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ and it is easy to check that the left and right distributive law holds. Hence we may view \mathbf{A} as a nonassociative algebra over $\text{GF}(2)$, where the word *algebra* is used in the more classical sense.

We shall use Lemma 2.4 to prove that $\text{Var}(\mathbf{A})$ does not have FDSC. For this we need to develop a detailed understanding of the equational properties of \mathbf{A} . Let Σ denote the set consisting of the following three equations:

- (a) $x(yz) \approx 0$;
- (b) $(xy)y \approx xy$;
- (c) $(xy)z \approx (xz)y$.

We write $x_{i_0}x_{i_1} \dots x_{i_{n-1}}x_{i_n}$ to abbreviate the left-bracketed multiplicative term $((\dots(x_{i_0} \cdot x_{i_1}) \cdot \dots) \cdot x_{i_{n-1}}) \cdot x_{i_n}$. We also refer to x_{i_0} as the *first variable* in such a term. More generally, if u_1, \dots, u_n are terms, then $u_1 \cdot u_2 \cdot \dots \cdot u_n$ is assumed to be left bracketed and so stands for $(\dots((u_1 \cdot u_2) \cdot \dots) \cdot u_n$.

LEMMA 4.1. *Every multiplicative term $t(x_0, \dots, x_n)$ in which each of the variables x_0, \dots, x_n occurs is equivalent modulo Σ and the usual multiplicative properties of 0 to either 0 or a term $x_{i_0}x_{i_1} \dots x_{i_{m-1}}x_{i_m}$, with $m \in \{n, n + 1\}$, such that $i_1 < i_2 < \dots < i_m$, and $\{i_0, \dots, i_m\} = \{0, \dots, n\}$.*

PROOF. Certainly law (a) ensures that if t contains a right bracketing then we can derive $t(x_0, \dots, x_n) \approx 0$. Otherwise, $t(x_0, \dots, x_n)$ contains only left bracketing, and laws (b) and (c) can be used to rearrange and remove repetitions amongst the variables appearing to the right of the first variable. \square

We refer to a term of the form $x_{i_0}x_{i_1} \dots x_{i_{m-1}}x_{i_m}$, with $i_1 < i_2 < \dots < i_m$, as a *reduced multiplicative term*. It is clear that we are able to rewrite every nonzero term as a sum $w_1 + \dots + w_n$ of multiplicative terms. Lemma 4.1 shows that we may further assume that each multiplicative term in such a sum is in reduced form.

LEMMA 4.2. *Let $n \geq 1$ and let w_1, \dots, w_n be pairwise distinct reduced multiplicative terms. Then the equation $w_1 + \dots + w_n \approx 0$ fails in \mathbf{A} .*

PROOF. Assume without loss of generality that $w_1 = x_{i_0}x_{i_1} \dots x_{i_m}$ and that m is minimal amongst the w_i . Let \mathbf{W}_ω denote the $\text{Var}(\mathbf{A})$ -free algebra with free generating set $\{x_i \mid i \in \omega\}$.

CASE 1. We have $i_0 \neq i_j$, for all $j \in \{1, \dots, m\}$.

Define $\varphi : \mathbf{W}_\omega \rightarrow \mathbf{A}$ by $\varphi(x_{i_0}) = a$, $\varphi(x_{i_j}) = b$ for $1 \leq j \leq m$, and $\varphi(x_i) = 0$ for all other generators. Now $\varphi(w_1) = a$, but by minimality and the fact that the w_i are pairwise distinct, we have $\varphi(w_i) = 0$, for $i \neq 1$. Hence, $\sum_{i=1}^m \varphi(w_i) = a \neq \varphi(0)$, showing that $w_1 + \dots + w_n \approx 0$ fails in \mathbf{A} .

CASE 2. We have $i_0 = i_j$, for some $j \in \{1, \dots, m\}$.

The idea is the same, but we define φ by $\varphi(x_{i_0}) = a + b$, $\varphi(x_{i_j}) = b$ for $1 \leq j \leq m$, and $\varphi(x_i) = 0$ for all other generators. \square

Lemmas 4.1 and 4.2 show that Σ is a basis for the equational theory of \mathbf{A} within the variety of all algebras over $\text{GF}(2)$, as the following argument shows. Lemma 4.1 and the axioms for an algebra over $\text{GF}(2)$ imply that every term reduces to either 0 or one of the form $w_1 + \dots + w_n$, for some reduced multiplicative terms w_1, \dots, w_n . However, Lemma 4.2 implies that no two distinct terms of this form, with their multiplicative terms in lexicographic order, induce the same term function on \mathbf{A} . Indeed, if the equation $w_1 + \dots + w_n \approx v_1 + \dots + v_m$ holds, then $w_1 + \dots + w_n + v_1 + \dots + v_m \approx 0$ also holds. After removing repeats (using $x + x \approx 0$), Lemma 4.2 implies that the left-hand side must reduce to 0, showing that $\{w_1, \dots, w_n\} = \{v_1, \dots, v_m\}$. (Lemma 4.2 also shows that the reduced multiplicative terms over an alphabet X form a vector basis for the $\text{Var}(\mathbf{A})$ -free algebra freely generated by X .) Let us say that a sum of distinct reduced multiplicative terms appearing lexicographically in the sum is a *normal form*. We have just argued that every term reduces to a unique normal form.

For $n \in \omega$, define terms f_n and g_n by

$$\begin{aligned} f_n(x, z_1, \dots, z_n) &:= xz_1z_2 \dots z_{n-1} + z_n, \\ g_n(x, z_1, \dots, z_n) &:= z_1xz_2 \dots z_{n-1} + z_n, \end{aligned}$$

and note that $f_0 = g_0 = x$.

LEMMA 4.3. *The set $F := \{f_n(x, \vec{z}) \mid n \in \omega\} \cup \{g_n(x, \vec{z}) \mid n \in \omega\}$ determines syntactic congruences in $\text{Var}(\mathbf{A})$.*

PROOF. Let $t(x, z_1, \dots, z_n)$ be a term. We shall prove that F shadows t . If the variable x does not appear in t , there is nothing to do (choose $\ell = 0$ in the definition of shadowing: see Lemma 2.4). We can assume that t is written in the form $w_1 + \dots + w_m$ with each multiplicative subterm w_i in reduced form, and that these subterms have been arranged so that x appears in w_1 . So w_1 can be written in one of the forms $xy_1 \dots y_k$ or $y_0 \dots y_{j-1}xy_{j+1} \dots y_k$, where $\{y_0, \dots, y_k\} \subseteq \{x, z_1, z_2, \dots\}$. If w_1 can be written in the form $xy_1 \dots y_k$, then

$$\begin{aligned} w_1 + \dots + w_m &\approx xy_1 \dots y_k + w_2 + \dots + w_m \\ &\approx f_{k+1}(x, y_1, \dots, y_k, w_2 + \dots + w_m) \end{aligned}$$

and

$$f_{k+1}(y, y_1, \dots, y_k, w_2 + \dots + w_m) \approx yy_1 \dots y_k + w_2 + \dots + w_m.$$

If w_1 is of the form $y_0 \dots y_{j-1}xy_{j+1} \dots y_k$, then

$$\begin{aligned} w_1 + \dots + w_m &\approx y_0 \dots y_{j-1}xy_{j+1} \dots y_k + w_2 + \dots + w_m \\ &\approx g_{k-j+1}(x, y_0 \dots y_{j-1}, y_{j+1}, \dots, y_k, w_2 + \dots + w_m) \end{aligned}$$

and

$$\begin{aligned} g_{k-j+1}(y, y_0 \dots y_{j-1}, y_{j+1}, \dots, y_k, w_2 + \dots + w_m) \\ \approx y_0 \dots y_{j-1}yy_{j+1} \dots y_k + w_2 + \dots + w_m. \end{aligned}$$

By moving each multiplicative term w_i involving x to the front, in turn, and repeating this process we can replace each occurrence of x in the term t by y and thereby show that F shadows t . □

This lemma and Corollary 2.5 show that in order to prove that $\text{Var}(\mathbf{A})$ does not have FDSC it suffices to prove that, for every $n \in \omega$, the set

$$F_n := \{f_k(x, \vec{x}) \mid k \leq n\} \cup \{g_k(x, \vec{x}) \mid k \leq n\}$$

fails to determine syntactic congruences in $\text{Var}(\mathbf{A})$. We shall show that F_n does not shadow the term

$$p_n(x, z_1, \dots, z_n) := xz_1 \dots z_n.$$

By Lemma 2.4 it will follow that F_n does not determine syntactic congruences in $\text{Var}(\mathbf{A})$.

Let us say that a term t is *near* p_n if p_n appears as a multiplicative term when t is written in normal form. (It does not count if p_n appears as a proper subterm of a multiplicative term in the normal form of t .) Trivially, $p_n(x, z_1, \dots, z_n)$ is near p_n

and $p_n(y, z_1, \dots, z_n)$ is not. Suppose that F_n shadows p_n . Then there exists $\ell \in \omega$, terms

$$s_1(x, z_1, \dots, z_m), \dots, s_\ell(x, z_1, \dots, z_m)$$

in F_n and $m\ell$ terms $w_{i,j}(x, y, z_1, \dots, z_m)$, for $1 \leq i \leq \ell$ and $1 \leq j \leq m$, such that \mathcal{K} satisfies the following equations:

$$p_n(x, z_1, \dots, z_n) \approx s_1(v_1, w_{1,1}, \dots, w_{1,m}), \tag{A}$$

$$s_i(v'_i, w_{i,1}, \dots, w_{i,m}) \approx s_{i+1}(v_{i+1}, w_{i+1,1}, \dots, w_{i+1,m}) \tag{B}$$

$$s_\ell(v'_\ell, w_{\ell,1}, \dots, w_{\ell,m}) \approx p_n(y, z_1, \dots, z_n), \tag{C}$$

where $\{v_i, v'_i\} = \{x, y\}$, for $1 \leq i \leq \ell$. We shall prove that, for $1 \leq i \leq \ell$, and for $z \in \{x, y\}$, the term $s_i(z, w_{i,1}, \dots, w_{i,m})$ is near p_n .

LEMMA 4.4. *Let $0 \leq m \leq n$, let $z \in \{x, y\}$ and let w_1, \dots, w_m be terms in the variables $\{x, y, z_1, z_2, \dots\}$. The term $f_m(z, w_1, \dots, w_m)$ is near p_n if and only if w_m is near p_n .*

PROOF. Note that

$$f_m(z, w_1, \dots, w_m) = zw_1w_2 \dots w_{m-1} + w_m.$$

We show that the term $zw_1w_2 \dots w_{m-1}$ is not near p_n .

If $zw_1w_2 \dots w_{m-1}$ has normal form 0, then we are done. Otherwise, the law $x(yz) \approx 0$ allows us to assume that, for $1 \leq i < m$, each term w_i is a single variable. So the normal form of $zw_1w_2 \dots w_{m-1}$ cannot be the multiplicative term p_n because it has too few variables. Hence, $f_m(z, w_1, \dots, w_m)$ is near p_n if and only if w_m is. \square

LEMMA 4.5. *Let $0 \leq m \leq n$, let $z \in \{x, y\}$ and let w_1, \dots, w_m be terms in the variables $\{x, y, z_1, \dots\}$. The term $g_m(z, w_1, \dots, w_m)$ is near p_n if and only if w_m is near p_n .*

PROOF. Note that $g_m(z, w_1, \dots, w_m) = w_1zw_2 \dots w_{m-1} + w_m$. We show that the term $w_1zw_2 \dots w_{m-1}$ is not near p_n .

If $w_1zw_2 \dots w_{m-1}$ has normal form 0, then we are done. Otherwise, the law $x(yz) \approx 0$ allows us to assume that, for $1 < i < m$, each term w_i is a single variable. Assume that w_1 has normal form $v_1 + \dots + v_k$. So

$$w_1zw_2 \dots w_{m-1} \approx v_1zw_2 \dots w_{m-1} + \dots + v_kzw_2 \dots w_{m-1}.$$

The normal form for such an expression can include the multiplicative term p_n if and only if an odd number of the multiplicative terms $v_izw_2 \dots w_{m-1}$ reduce to p_n . However, each such multiplicative term either contains a y or an x that is not the first variable, and hence cannot reduce to p_n . So $w_1zw_2 \dots w_{m-1}$ is not near p_n . Hence, $g_m(z, w_1, \dots, w_m)$ is near p_n if and only if w_m is. \square

Lemmas 4.4 and 4.5 allow us to complete the proof. As $p_n(x, z_1, \dots, z_n)$ is near p_n , Equation (A) shows that $w_{1,m}$ is near p_n . However, then a trivial induction shows that, for $z \in \{x, y\}$, each term $s_i(z, w_{i,1}, \dots, w_{i,m})$ is near p_n , as required. Now Equation (C) implies that $p_n(y, z_1, \dots, z_n)$ is near p_n , which is a contradiction. This shows that $\text{Var}(\mathbf{A})$ fails to have FDSC (and therefore fails to have TFPC).

Now we show that this variety is residually very finite. As the algebra \mathbf{A} has a group reduct it certainly generates a congruence-permutable variety. Consequently, we may use commutator theory for congruence modular varieties; see Freese and McKenzie [11]. In particular [11, Theorem 10.15] shows that $\text{Var}(\mathbf{A})$ is residually very finite if and only if the implication

$$\nu \leq [\mu, \mu] \Rightarrow \nu = [\mu, \nu] \tag{RF}$$

holds, for every pair of congruences μ, ν on every subalgebra \mathbf{B} of \mathbf{A} .

Up to isomorphism, there are two proper subalgebras of \mathbf{A} : one is the trivial subalgebra, and the other is the two-element 0-ring \mathbf{Z} . On these algebras the implication (RF) holds trivially, so we concentrate on calculating the commutator on \mathbf{A} .

We first observe that the only congruence of \mathbf{A} that is neither the diagonal Δ nor the universal relation ∇ is the congruence α corresponding to the two-block partition $\{0, a \mid b, a + b\}$. The quotient \mathbf{A}/α is again isomorphic to \mathbf{Z} . Let $f : \mathbf{A} \rightarrow \mathbf{Z}$ be the natural map.

As \mathbf{Z} is a 0-ring, it is abelian and so $[\beta, \gamma] = \Delta_{\mathbf{Z}}$, for all $\beta, \gamma \in \text{Con}(\mathbf{Z})$. Now

$$f^{-1}[f(\nabla \vee \alpha), f(\nabla \vee \alpha)] = [\nabla, \nabla] \vee \alpha, \tag{\dagger}$$

by properties of the commutator [11, Proposition 4.4]. However, as \mathbf{Z} is abelian, the left-hand side of (\dagger) becomes $f^{-1}(\Delta_{\mathbf{Z}})$ which is α . Hence, (\dagger) yields $[\nabla, \nabla] \leq \alpha$.

Now we show that $[\nabla, \alpha] = \alpha$. Recall [11, Definition 4.7] that the algebra $\mathbf{A}(\nabla, \alpha)$ is the subalgebra of \mathbf{A}^4 (thought of as 2×2 matrices over A) consisting of all matrices whose columns belong to $\nabla = A^2$ and rows belong to α . Also, $\Delta_{\nabla, \alpha}$ denotes the congruence on \mathbf{A}^2 (written as columns) generated by the elements of $\mathbf{A}(\nabla, \alpha)$ of the form

$$\begin{pmatrix} u & v \\ u & v \end{pmatrix} \equiv \left(\begin{pmatrix} u \\ u \end{pmatrix}, \begin{pmatrix} v \\ v \end{pmatrix} \right).$$

As

$$\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix} \in \mathbf{A}(\nabla, \alpha),$$

right multiplication by $\begin{pmatrix} b \\ 0 \end{pmatrix}$ gives

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in \Delta_{\nabla, \alpha}.$$

By [11, Theorem 4.9], we find that $(a, 0) \in [\nabla, \alpha]$, showing that $\alpha \leq [\nabla, \alpha]$.

Now, using the order-preserving properties of the commutator,

$$\alpha \leq [\alpha, \nabla] = [\nabla, \alpha] \leq [\nabla, \nabla] \leq \alpha,$$

giving equality throughout. As Δ is an absorbing element with respect to the commutator product $[\ , \]$, we obtain the following partial table of commutators:

$[\ , \]$	Δ	α	∇
Δ	Δ	Δ	Δ
α	Δ	?	α
∇	Δ	α	α ,

where the question mark is either α or Δ . We do not need to calculate $[\alpha, \alpha]$. In both of the possible cases, the reader will easily verify that the implication (RF) must hold.

By [11, Theorem 10.15], we have shown that (up to isomorphism) the variety $\text{Var}(\mathbf{A})$ contains only finitely many subdirectly irreducible algebras all of which are finite (in fact of size at most $4 + 4(4^4)^!$).

Summarising, we have proved the following result.

THEOREM 4.6. *The four-element algebra \mathbf{A} generates a residually very finite, congruence-permutable variety that does not have finitely determined syntactic congruences.*

Let $\{\mathbf{A}_1, \dots, \mathbf{A}_n\}$ be a transversal of the isomorphism classes of the subdirectly irreducible algebras in $\text{Var}(\mathbf{A})$ and define $\mathbf{B} := \mathbf{A}_1 \times \dots \times \mathbf{A}_n$. Then

$$\text{Var}(\mathbf{B}) = \text{Var}(\mathbf{A}) = \mathbb{ISP}(\mathbf{B}).$$

Thus, \mathbf{B} is a finite algebra such that the quasivariety generated by \mathbf{B} is a variety that fails to have FDSC. The existence of such an example was alluded to in [6, p. 373]. The original example referred to in [6] is the three-element multiplicative subreduct of \mathbf{A} on the set $\{0, a, b\}$. Denote this algebra by \mathbf{C} . While \mathbf{C} does not generate a congruence-permutable variety, one can show that $\text{Var}(\mathbf{C})$ fails to have FDSC, via a proof similar to but easier than that we gave for \mathbf{A} . We can also prove that $\text{Var}(\mathbf{C}) = \mathbb{ISP}(\mathbf{C})$, via a proof very different from that which we gave for $\text{Var}(\mathbf{B})$. The Equations (a)–(c) given for \mathbf{A} along with the extra law $xx \approx 0$ (and other standard multiplicative properties for 0) form an equational basis for $\text{Var}(\mathbf{C})$.

Most of the interest in the example \mathbf{C} is superseded by Theorem 4.6 above; however, we observe that every two-element algebra has FDSC: cofinitely many of these are covered by Theorem 3.3 above, while the remaining are easy exercises. (A graduate student of the first and second authors, Claire Edwards, has verified this and used it to prove that all two-element algebras are standard in the sense of [7].)

We also observe that there are finite algebras that generate congruence meet semi-distributive varieties without FDSC [6, Example 7.7]. So the congruence distributivity condition in Theorem 3.3 cannot be replaced by congruence meet semi-distributivity. On the other hand, the examples given in [6] generate varieties that are not residually

very finite, and there are no known examples of congruence meet semi-distributive varieties without FDSC that are finitely generated and contain only finitely many subdirectly irreducibles. As observed in [6, (after Problem 9.3)], if no such example exists, then the problem of deciding whether FDSC holds for a finitely generated variety is undecidable.

References

- [1] J. Almeida and P. Weil, ‘Relatively free profinite monoids: an introduction and examples’, in: *Semigroups, Formal Languages and Groups*, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 466 (ed. J. Fountain) (Kluwer, Dordrecht, 1995), pp. 73–117.
- [2] K. A. Baker, G. F. McNulty and J. Wang, ‘An extension of Willard’s finite basis theorem: congruence meet-semidistributive varieties of finite critical depth’, *Algebra Universalis* **52** (2005), 289–302.
- [3] K. A. Baker and J. Wang, ‘Approximate distributive laws and finite equational bases for finite algebras in congruence-distributive varieties’, *Algebra Universalis* **54** (2005), 385–396.
- [4] S. Burris and H. P. Sankappanavar, *A Course in Universal Algebra*, Graduate Texts in Mathematics, 78 (Springer, Berlin, 1980).
- [5] T. H. Choe, ‘Zero-dimensional compact associative distributive universal algebras’, *Proc. Amer. Math. Soc.* **42** (1974), 607–613.
- [6] D. M. Clark, B. A. Davey, R. S. Freese and M. Jackson, ‘Standard topological algebras: syntactic and principal congruences and profiniteness’, *Algebra Universalis* **52** (2004), 343–376.
- [7] D. M. Clark, B. A. Davey, M. Haviar, J. G. Pitkethly and M. R. Talukder, ‘Standard topological quasi-varieties’, *Houston J. Math.* **29** (2003), 859–887.
- [8] D. M. Clark, B. A. Davey, M. Jackson and J. G. Pitkethly, ‘The axiomatizability of topological prevarieties’, *Adv. Math.* **218** (2008), 1604–1653.
- [9] D. J. Clinkenbeard, ‘Simple compact topological lattices’, *Algebra Universalis* **9** (1979), 322–328.
- [10] B. J. Day, ‘On profiniteness of compact totally disconnected algebras’, *Bull. Austral. Math. Soc.* **20** (1970), 71–76.
- [11] R. Freese and R. McKenzie, *Commutator Theory for Congruence Modular Varieties*, London Mathematical Society Lecture Note Series, 125 (Cambridge University Press, Cambridge, 1987).
- [12] M. Jackson, ‘Residual bounds for compact totally disconnected algebras’, *Houston J. Math.* **34** (2008), 33–67.
- [13] P. Johnstone, *Stone Spaces* (Cambridge University Press, Cambridge, 1982).
- [14] B. Jónsson, ‘Algebras whose congruence lattices are distributive’, *Math. Scand.* **21** (1967), 110–121.
- [15] R. McKenzie, ‘Para primal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties’, *Algebra Universalis* **8** (1978), 336–348.
- [16] ———, ‘The residual bound of a finite algebra is not computable’, *Internat. J. Algebra Comput.* **6** (1996), 29–48.
- [17] J. Wang, ‘A proof of the Baker conjecture’, *Acta Math. Sin.* **33** (1990), 626–633 (in Chinese).

BRIAN A. DAVEY, Department of Mathematics, La Trobe University, Victoria, Australia

e-mail: b.davey@latrobe.edu.au

MARCEL JACKSON, Department of Mathematics, La Trobe University, Victoria, Australia

e-mail: m.g.jackson@latrobe.edu.au

MIKLÓS MARÓTI, János Bolyai Mathematical Institute, University of Szeged,
Szeged, Hungary

e-mail: mmaroti@math.u-szeged.hu

RALPH N. MCKENZIE, Department of Mathematics, Vanderbilt University,
Nashville, TN, USA

e-mail: mckenzie@math.vanderbilt.edu