TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 350, Number 1, January 1998, Pages 1–41
S 0002-9947(98)01594-3

MINIMAL SETS AND VARIETIES

KEITH A. KEARNES, EMIL W. KISS, AND MATTHEW A. VALERIOTE

Abstract. The aim of this paper is twofold. First some machinery is established to reveal the structure of abelian congruences. Then we describe all minimal, locally finite, locally solvable varieties. For locally solvable varieties, this solves problems 9 and 10 of Hobby and McKenzie. We generalize part of this result by proving that all locally finite varieties generated by nilpotent algebras that have a trivial locally strongly solvable subvariety are congruence permutable.

1. Introduction

This paper is an outgrowth of our study of locally solvable locally finite varieties. Our purpose is to describe tools that have been developed to better deal with finite solvable algebras. We refer to these tools as "coordinatization theory" and "the theory of minimal sets in subdirect powers". Although these tools were originally developed to deal with solvable algebras, we present them in greater generality here. After spending the early sections of this paper building theory, we then present one of the firstfruits of coordinatization theory: we characterize the locally finite minimal varieties generated by an abelian algebra.

In Section 2 we present all technical results on centrality and type **2** minimal sets that we use later. There are some new observations here, too, like Theorem 2.12 and its corollary.

Our first section devoted to theory building is Section 3. In this section we describe coordinatization results. We approach the subject in a general way, explaining how a subset of an algebra may be coordinatizable by E–traces, but we quickly get to the most interesting case: we consider when a subset of an algebra is coordinatizable by traces. Such a subset might be called a "higher dimensional trace". We analyze the algebra induced on a coordinatizable subset of an α–class, where α is a minimal congruence on a finite algebra $\mathbf{A}$ and $\mathrm{typ}(0_a, \alpha) \in \{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$. We now describe what this means and why it is interesting. To minimize the prerequisites for this discussion we assume that $\mathbf{A}$ is a finite simple algebra. In this setting, $\alpha = 1_{\mathbf{A}}$, and minimal sets and traces are the same thing. We will use the word "trace" in the next few paragraphs since that is the accurate choice when looking at algebras which are not simple.

The fundamental concept of tame congruence theory is that an algebra can be locally approximated by induced algebras. One proceeds as follows. Choose a

Received by the editors October 14, 1994 and, in revised form, August 18, 1995.
1991 *Mathematics Subject Classification.* Primary 08A05; Secondary 08A40, 08B15.
This research was partially supported by a fellowship from the Alexander von Humboldt Stiftung (to the first author), by the Hungarian National Foundation for Scientific Research, grant no. 1903 (to the second author), and by the NSERC of Canada (third author).

nonconstant idempotent unary polynomial e of $\mathbf{A}$ with minimal range. Let $N = e(A)$. Then N is a $\langle 0,1\rangle$–minimal set of $\mathbf{A}$ and also a $\langle 0,1\rangle$–trace. Define $\mathbf{A}|_N$ to be the algebra whose universe is N and whose basic operations are the polynomials of $\mathbf{A}$ under which N is closed. These are the $f \in \mathrm{Pol}(\mathbf{A})$ such that $f(N^k) \subseteq N$. What makes this a powerful approach to the study of finite algebras can be summarized by four words: Isomorphism, Density, Separation and Classification. The word Isomorphism refers to the fact that, up to polynomial equivalence, the algebra $\mathbf{A}|_N$ is independent of the choice of e. Hence, the polynomial equivalence class of $\mathbf{A}|_N$ is an invariant of $\mathbf{A}$. The word Density refers to the fact that any two elements of $\mathbf{A}$ can be connected by a chain of overlapping traces. The word Separation reflects the fact that if $a, b \in A$ are distinct, then there is a polynomial $p \in \mathrm{Pol}_1(\mathbf{A})$ such that $p(A) = N$ and $p(a) \neq p(b)$. The word Classification refers to the fact that, up to polynomial equivalence, the structure of $\mathbf{A}|_N$ is known. Namely, $\mathbf{A}|_N$ is one of the following algebras:

1. a simple G–set (for a group G),
2. a 1–dimensional vector space,
3. a 2–element Boolean algebra,
4. a 2–element lattice, or
5. a 2–element semilattice.

The number **1** – **5** is called the *type* of $\mathbf{A}|_N$ and also the *type* of $\mathbf{A}$.

When a finite algebra $\mathbf{A}$ offers a puzzle, analysis of the puzzle often can be reduced to the consideration of a certain "configuration" of elements and operations. We do not intend to define "configuration" here, but roughly what we mean by this term is a set of first order sentences in the language of $\mathbf{A}_A$ which are either atomic or negated atomic. Now, one can use separation to map any configuration of $\mathbf{A}$ into N in a way that preserves at least one negated atomic sentence. This transforms the puzzle about $\mathbf{A}$ into a related puzzle about the induced algebra $\mathbf{A}|_N$. Because of the isomorphism between induced algebras it doesn't matter which you choose. Using the classification of induced algebras, one solves the puzzle "locally". Then one uses density to transfer the solution back to the original algebra. Of course, the success of this strategy depends on how closely $\mathbf{A}$ is approximated by its induced algebras.

In Figure 1 we have indicated what might be called the "geometry" of an 8–element simple algebra $\mathbf{A}$. The black dots represent elements of A. These are the "points" of the geometry. The set $N = \{0,1\}$ is one of the ten traces of $\mathbf{A}$. The traces are the "lines" of the geometry. It would be highly desirable to understand how all the operations of $\mathbf{A}$ compose, but tame congruence theory won't tell us that much; the theory only tells us what is happening "on a line". That is, if $p \in \mathrm{Pol}_k(\mathbf{A})$ and $p(N^k) \subseteq N$, then $p|_N \in \mathrm{Pol}_k(\mathbf{A}|_N)$. If, for example, $\mathbf{A}$ is of type **2**, then $p|_N$ is a vector space polynomial. This tells us that a fragment of the Cayley table for p is described by an operation on N of the form $a_1x_1 + \cdots + a_kx_k$. Tame congruence theory does not tell us more about the Cayley table of p, nor does it tell us anything about other polynomials $q \in \mathrm{Pol}_m(\mathbf{A})$ unless it happens that $q(N^m) \subseteq N$ (or at the very least one must have $q(N_1 \times \cdots \times N_m) \subseteq N_0$, where all N_i are traces).

In Section 3 we go a step further. We show that often there are subsets $T \subseteq A$ larger than a trace which share the basic properties of traces and which may be thought of as higher dimensional traces. The sets we consider are those subsets of A

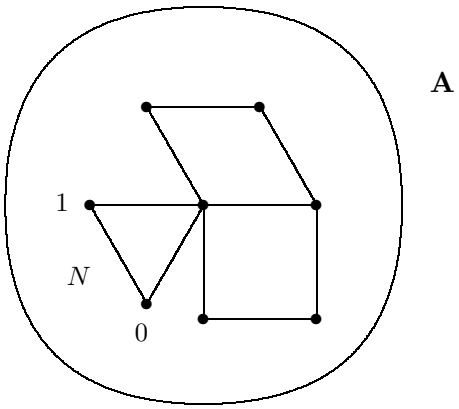

FIGURE 1. The geometry of **A**

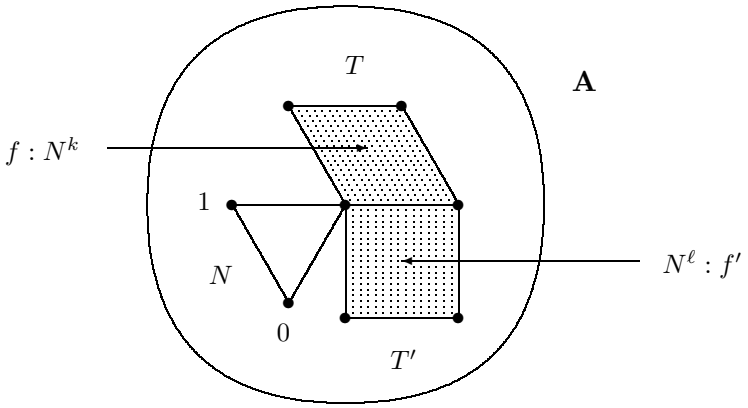

FIGURE 2. Multitraces T and T'

of the form $T = f(N, \dots, N)$, where N is a trace and $f \in \mathrm{Pol}(\mathbf{A})$. We call these sets *multitraces*. In Figure 2 there are two multitraces which are not just traces.

The multitrace T might be thought of as a "hyperplane" of the geometry. A classification of algebras of the form $\mathbf{A}|_T$, where T is a multitrace, would tell us what is happening on a hyperplane rather than just what is happening on a line. The structure of $\mathbf{A}|_T$ when $\mathbf{A}$ is abelian follows fairly directly from coordinatization theory. We are also able to determine the structure of $\mathbf{A}|_T$ when $\mathbf{A}$ has type **3**. Unfortunately, the notion of a multitrace is not well–behaved in types **4** and **5**.

The class of multitraces of our simple algebra $\mathbf{A}$ contains the traces, so we still have the properties of separation and density with respect to multitraces. In Section 3, we classify the algebra induced on a multitrace for types **1**, **2** and **3**. With respect to the isomorphism property which traces enjoy, it is not true that any two

multitraces are polynomially isomorphic. However, any polynomial image of a multitrace is again a multitrace and, in types **1**, **2** and **3**, the structure that $\mathbf{A}$ induces on a multitrace is determined up to polynomial equivalence by the cardinality of the multitrace. These two properties may serve as substitutes for the isomorphism property of traces.

It turns out that there is another realization of the intuitive notion of a higher dimensional trace which works well in all types. This new notion, called a *generalized trace*, will be developed in a subsequent paper. Here we will only say that the definition of a generalized trace is a little more complicated than that of a multitrace, but in types **1**, **2**, and **3** these concepts coincide.

Section 4 is our other section devoted to theory building. In this section we investigate minimal sets in subdirect powers. Generally, our goal is to better understand the connection between local and global properties in a locally finite variety. Specifically, our goal is to analyze the relationship between minimal sets in $\mathbf{A}$ and minimal sets in an arbitrarily chosen finite algebra $\mathbf{B} \in \mathcal{V}(\mathbf{A})$. This seems to be a difficult problem. For example, say that a finite algebra satisfies the *empty tails condition* if all of its minimal sets have empty tail. It is known (see [11]) that a locally finite variety is congruence modular if and only if all finite members satisfy the empty tails condition. The empty tails condition is not sufficient (nor necessary) to prove congruence modularity for a single algebra; but the empty tails condition for every finite subalgebra of a power of $\mathbf{A}$ is strong enough to prove that $\mathbf{A}$ is congruence modular, and moreover it is strong enough to prove that the variety generated by $\mathbf{A}$ is congruence modular. In particular, this shows that the empty tails condition holding for all subalgebras of powers of $\mathbf{A}$ implies that $\mathrm{typ}\{\mathbf{B}\} \subseteq \{\mathbf{2}, \mathbf{3}, \mathbf{4}\}$ whenever $\mathbf{B}$ is a subalgebra of a power of $\mathbf{A}$. However, this implication does not hold on the level of single algebras; $\mathbf{A}$ may satisfy the empty tails condition even when $\mathrm{typ}\{\mathbf{A}\} \not\subseteq \{\mathbf{2}, \mathbf{3}, \mathbf{4}\}$. What is needed, clearly, is a better understanding of the consequences of asserting that all minimal sets of subalgebras of powers satisfy a specified condition (like the empty tails condition). In Section 4 we consider a finite algebra $\mathbf{A}$ which has a type **2** prime quotient $\langle \alpha, \beta \rangle$. We describe the minimal sets corresponding to certain type **2** intervals in subdirect powers of $\mathbf{A}$. In the case where $\mathbf{A}$ is a simple algebra of type **2**, our description of minimal sets in subdirect powers applies to all type **2** prime quotients in all subalgebras of powers of $\mathbf{A}$.

In Section 5 we use the tools developed in the earlier part of the paper to classify the minimal, locally finite varieties generated by abelian algebras. Any locally finite variety generated by abelian algebras is locally solvable. Any locally finite minimal variety is generated by a *strictly simple algebra*—by which we mean a finite simple algebra with no nontrivial proper subalgebras. Hence, a minimal locally finite variety generated by abelian algebras is generated by an abelian strictly simple algebra. The main idea behind the classification theorem is that this strictly simple abelian generating algebra must be coordinatizable by traces. The connection between the theory of coordinatization and matrix powers allows one to deduce that a minimal, locally finite variety generated by a simple algebra of type **1** is term equivalent to a matrix power of the variety of sets or the variety of pointed sets. It also allows one to deduce that a minimal, locally finite variety generated by a simple algebra of type **2** is an affine variety. We give two proofs of the latter result in Section 5.

In Section 6 we give yet a third proof that a minimal locally finite variety generated by a simple algebra of type **2** is affine. We then extend this result to non–minimal varieties generated by nilpotent algebras. The main result in this section

is that a locally finite variety generated by nilpotent algebras either is congruence permutable or else has a nontrivial strongly abelian subvariety. This section can be read independently of Sections 3–5.

The reader is assumed to be familiar with the book [6] on tame congruence theory, and also with the book [2] containing the basics of universal algebra. The notation used in the paper is mostly the same as that used in [6]. In particular, algebras are denoted by boldface capital letters, and A is the underlying set of $\mathbf{A}$. Boldface lower case letters, like $\mathbf{b}$, denote sequences of elements, and b_i stands for the i–th component of $\mathbf{b}$. Thus $\mathbf{b}$ typically denotes $(b_1, \dots, b_n)$ for some integer n if these are arguments of a function, and the corresponding column vector, if this is an element of a cartesian product. If R is a binary relation, then by $\mathbf{a}\ R\ \mathbf{b}$ we mean $a_i\ R\ b_i$ for all i.

Acknowledgements

The first and second authors are greatly indebted to Matthew Valeriote for inviting them to Hamilton to work on the topic of this paper. The second author would also like to thank Joel Berman for inviting him to Chicago for the same purpose.

2. Centrality

First we recall the concepts of centrality and of the commutator (defined in Chapter 3 of [6]) in a slightly more general form.

Definition 2.1. Let $\mathbf{A}$ be an algebra, L and R binary relations on A, and $\delta \in \mathrm{Con}(\mathbf{A})$. We say that L *centralizes* R *modulo* δ, or that *the* $\langle L, R\rangle$*–term condition holds modulo* δ (in notation: $C(L, R; \delta)$) if for all polynomials f of $\mathbf{A}$ and elements $a\ L\ b$ and $\mathbf{c}\ R\ \mathbf{d}$ of A,

$$\begin{array}{ccc} f(a, \mathbf{c}) & \delta & f(a, \mathbf{d}) \\ & \Updownarrow & \\ f(b, \mathbf{c}) & \delta & f(b, \mathbf{d})\,. \end{array}$$

The *commutator* of L and R is defined to be the smallest congruence δ of $\mathbf{A}$ with $C(L, R; \delta)$, and it is denoted $[L, R]$. The largest congruence α of $\mathbf{A}$ satisfying $C(\alpha, R; \delta)$ is denoted by $(\delta : R)$. We write $\mathrm{ann}(R)$ for $(0_{\mathbf{A}} : R)$; this is the *annihilator* of R.

We have to make several remarks to justify this definition. First note that if $\overline{R}$ denotes the tolerance of $\mathbf{A}$ generated by R, then $C(L, R; \delta)$ is equivalent to $C(L, \overline{R}; \delta)$. If R itself is reflexive, then it is sufficient to assume $f(a, \mathbf{c})\ \delta\ f(a, \mathbf{d}) \iff f(b, \mathbf{c})\ \delta\ f(b, \mathbf{d})$ for all terms f (rather than polynomials).

It is easy to see that the set of all congruences δ satisfying $C(L, R; \delta)$ is closed under intersection, so the commutator $[L, R]$ indeed exists. However, this set of congruences is not necessarily a filter in $\mathbf{Con}(\mathbf{A})$. The polynomials $f(x, \mathbf{c})$ and $f(x, \mathbf{d})$ in Definition 2.1 are called R*–twins* because they are derived from the same polynomial with different parameter sequences which are R–related componentwise. More generally and more precisely, when $S \subseteq A^k$ is a k–ary relation on A and $t(x, \overline{y})$ is a polynomial, then we say that a sequence of unary polynomials, $(t_1^{\mathbf{A}}(x, \mathbf{s}^1), \dots, t_k^{\mathbf{A}}(x, \mathbf{s}^k))$, where the tuples $(s_i^1, \dots, s_i^k)$ each belong to S, is a sequence of (*simultaneous*) S*–twins*. The statement that the $\langle L, R\rangle$–term condition holds is simply this: *any pair of* R*–twins which agree modulo* δ *at the value* a *also agree modulo* δ *at any value* L*–related to* a. As one can see, the relations L and R

do not play symmetric roles. We have described the $\langle L, R\rangle$–term condition in such a way that L refers to the relation in the leftmost position in $[L, R]$ and $C(L, R; \delta)$, while R refers to the relation which occupies the position to the right of L.

It is not difficult to show that the set of all pairs (a, b) for which $C(\{(a, b)\}, R; \delta)$ holds is a congruence relation of $\mathbf{A}$. This congruence is of course $(\delta : R)$, so the definition of $(\delta : R)$ is meaningful. We should really speak of a left annihilator here, but this will cause no trouble, since there is no natural definition for a right annihilator. Thus, if $\overline{L}$ denotes the congruence generated by L, then $C(L, R; \delta)$ and $C(\overline{L}, R; \delta)$ are also equivalent.

An important consequence of the existence of the annihilator is the fact that

$$C(\alpha_i, R; \delta) \text{ for all } i \in I \quad \Longleftrightarrow \quad C(\bigvee_{i\in I} \alpha_i, R; \delta),$$

where $\alpha_i \in \mathrm{Con}(\mathbf{A})$ for $i \in I$. This does not imply, however, that the commutator is left distributive over join.

Definition 2.2. If $\mathbf{A}$ is an algebra and R is a compatible, reflexive, binary relation on $\mathbf{A}$, then the subalgebra of $\mathbf{A}^2$ with underlying set R (that is, all R–related pairs) will often be denoted by $\mathbf{A}(R)$. If L is any binary relation on A, then $\Delta_{L,R}$ denotes the congruence on $\mathbf{A}(R)$ generated by

$$\{\langle (x, x), (y, y)\rangle \;\Big|\; x \; L \; y\}.$$

Let π_i denote the coordinate projections of $\mathbf{A}(R)$ onto $\mathbf{A}$. If $\gamma \neq 0$ is a congruence of $\mathbf{A}$, then we denote by γ_i the congruence $\pi_i^{-1}(\gamma)$, and write η_i for $\pi_i^{-1}(0_{\mathbf{A}})$. If R is a congruence β, then $\beta_1 = \beta_2$ is denoted by $\overline{\beta}$.

It is easy to check that $[L, R] = 0$ is equivalent to the statement that the diagonal subuniverse of $\mathbf{A}(R)$ is a union of $\Delta_{L,R}$–classes. This observation leads to an alternative definition of the commutator. It also shows that we can replace L with the congruence it generates in $\mathbf{A}$ in the definition of $\Delta_{L,R}$ and also in the definition of $[L, R]$. (We point out that what we write as $\Delta_{L,R}$ has unfortunately been expressed as $\Delta_{R,L}$ in several places in the literature. Because of the connection between $\Delta_{L,R}$ and the commutator of L and R, we choose to arrange our notation so that the left subscript of $\Delta_{L,R}$ corresponds to the left position of $[-, -]$. So remember: the right subscript of $\Delta_{L,R}$ is considered as a subalgebra, the left subscript is put on the diagonal.)

Next we recall some definitions concerning nilpotence, partially contained in Definition 3.5 of [6].

Definition 2.3. Let $\mathbf{A}$ be any algebra and $\beta \in \mathrm{Con}(\mathbf{A})$. We define $(\beta]^1 = [\beta)^1 = [\beta]^1 = \beta$, and inductively $(\beta]^{n+1} = [\beta, (\beta^n]]$, also $[\beta)^{n+1} = [[\beta)^n, \beta]$, and $[\beta]^{n+1} = [[\beta]^n, [\beta]^n]$. The congruence β is called *left* or *right nilpotent*, or *solvable*, iff for some n we have $(\beta]^n = 0_{\mathbf{A}}$, or $[\beta)^n = 0_{\mathbf{A}}$, or $[\beta]^n = 0_{\mathbf{A}}$. The algebra $\mathbf{A}$ is *left (right) nilpotent*, or *solvable*, if the congruence $1_{\mathbf{A}}$ is.

Thus, β is left nilpotent if

$$[\beta, [\beta, [\beta, [\dots, [\beta, \beta]\dots]]]] = 0_a$$

(for a sufficiently long expression). As proved in [7], the hypothesis of left nilpotence is weaker than any other notion of nilpotence. For example, if $\mathbf{A}$ is a finite algebra satisfying $[1)^{k+1} = 0$ ($\mathbf{A}$ is k–step right nilpotent), then $\mathbf{A}$ is left nilpotent although

possibly of higher nilpotence class. Sometimes, when we refer just to nilpotence, we shall mean the weakest form: left nilpotence. We will need some other results and definitions of [7], so we reproduce them here.

Definition 2.4. If $\mathbf{A}$ is a finite algebra, $\beta \in \mathrm{Con}(\mathbf{A})$, $\delta \prec \theta$ in $\mathbf{Con}(\mathbf{A})$ and N is a $\langle \delta, \theta \rangle$–trace, then the congruence quotient $\langle \delta, \theta \rangle$ is said to be *β–coherent* if the implication

$$C(\beta, N^2; \delta) \Longrightarrow C(\beta, \theta; \delta)$$

holds. If every prime quotient of $\mathbf{Con}(\mathbf{A})$ is β–coherent for every β, then $\mathbf{A}$ is said to be *coherent*.

Note that, as all $\langle \delta, \theta \rangle$–traces are polynomially isomorphic, if we have $C(\beta, N^2; \delta)$ for one trace N, then $C(\beta, N^2; \delta)$ holds for all traces N.

Recall that a group is said to act regularly on a set if whenever a group element stabilizes a point, it acts as the identity map. (Sometimes this concept is called semiregularity.)

Definition 2.5. Assume that $\mathbf{A}$ is a finite algebra, $\beta \in \mathrm{Con}(\mathbf{A})$, $\delta \prec \theta$ in $\mathbf{Con}(\mathbf{A})$, N is a $\langle \delta, \theta \rangle$–trace and H is the group of polynomial permutations of $\mathbf{A}|_N$ which are β–twins of id_N. We say that the congruence quotient $\langle \delta, \theta \rangle$ is *β–regular* if $\mathrm{typ}(\delta, \theta) \neq \mathbf{1}$, or $\mathrm{typ}(\delta, \theta) = \mathbf{1}$ and H acts regularly on N modulo δ. When $\mathrm{typ}(\delta, \theta) = \mathbf{1}$ this states that $\langle \delta, \theta \rangle$ is β–regular iff for all $p \in H$ the implication

$$(\forall u, x \in N)\ (p(u)\ \delta\ u \Longrightarrow p(x)\ \delta\ x)$$

holds.

We record in the following theorem and corollary the facts from [7] that we will need concerning β–coherent and β–regular prime quotients.

Theorem 2.6. *Let $\mathbf{A}$ be a finite algebra, with $\beta \in \mathrm{Con}(\mathbf{A})$ and $\delta \prec \theta$ in $\mathbf{Con}(\mathbf{A})$. Choose $U \in \mathrm{M}_{\mathbf{A}}(\delta, \theta)$ and denote by B and T the body and tail of U respectively. The following are true.*

1. *If $[\beta, \beta] \wedge \theta \leq \delta$, then $\langle \delta, \theta \rangle$ is β–regular.*
2. *If $\langle \delta, \theta \rangle$ is β–regular, then it is β–coherent.*
3. *Every homomorphic image of $\mathbf{A}$ is left nilpotent iff $\mathbf{A}$ is left nilpotent and coherent.*
4. *If $\langle \delta, \theta \rangle$ is β–regular, then for the conditions listed below $(i) \Longrightarrow (ii) \Longrightarrow (iii) \Longleftrightarrow (iv)$ holds.*
   - *(i) $C(\beta, \theta; \delta)$.*
   - *(ii) $[\beta, \theta] \leq \delta$.*
   - *(iii) $C(\theta, \beta; \delta)$.*
   - *(iv) $[\theta, \beta] \leq \delta$.*

   If $(\beta]^k|_U \subseteq B^2 \cup T^2$ for some k, then all conditions are equivalent. If $[\beta]^k|_U \subseteq B^2 \cup T^2$ for some k and $\mathrm{typ}(\delta, \theta) \neq \mathbf{1}$, then all conditions are equivalent.

Proof. For the case when $\mathrm{typ}(\delta, \theta) = \mathbf{1}$, statement (2) follows from Lemma 4.13 of [7]. In all other cases we always have β–coherence by Lemma 4.2 of [7], and also β–regularity by the definition (so β–regularity and β–coherence are only interesting when $\mathrm{typ}(\delta, \theta) = \mathbf{1}$). Statement (1) is Theorem 4.20 of [7], (3) is Corollary 4.4 of [7], and, finally, (4) is a combination of Lemmas 3.1, 3.2, and 4.14 of [7], depending on the type of $\langle \delta, \theta \rangle$. □

Corollary 2.7. *Any locally finite variety generated by abelian algebras is locally left nilpotent.*

The concept of an E–trace plays an important role in [6] (see Lemma 2.4 or the second part of Chapter 6). The name E–trace was coined later.

Definition 2.8. Let $\mathbf{A}$ be an algebra, e an idempotent unary polynomial, α a congruence, and a an element of $\mathbf{A}$. We say that a subset S of $\mathbf{A}$ is an *E–trace* of $\mathbf{A}$ with respect to e (or with respect to α, or a/α), if $S = e(A) \cap a/\alpha$.

The following notation and easy–to–check observation is from [1]; see Sections 5 and 7 of that paper for a more detailed analysis.

Definition 2.9. Let $\alpha < \beta \in \mathrm{Con}(\mathbf{A})$ for some algebra $\mathbf{A}$. Set

$$\mathrm{Sep}(\alpha, \beta) = \{ f \in \mathrm{Pol}_1(\mathbf{A}) \;\big|\; f(\beta) \not\subseteq \alpha \}.$$

Lemma 2.10. *Let $\langle \alpha, \beta \rangle$ be a tame quotient of a finite algebra $\mathbf{A}$. Then for all $\gamma \in \mathrm{Con}(\mathbf{A})$ with $\alpha < \gamma < \beta$ we have*

1. $\mathrm{Sep}(\alpha, \gamma) = \mathrm{Sep}(\alpha, \beta)$, *and*
2. $\mathrm{Sep}(\gamma, \beta) = \mathrm{Sep}(\alpha, \beta)$.

Next we summarize some basic facts on type **2** minimal sets.

Lemma 2.11. *Let $\mathbf{A}$ be a finite algebra, $\langle \delta, \theta \rangle$ a type **2** prime quotient of $\mathbf{A}$ and $\gamma = (\delta : \theta)$. Choose any $\langle \delta, \theta \rangle$–minimal set U. Let B be the body and T the tail of U, and N a $\langle \delta, \theta \rangle$–trace in B. Then the following hold.*

1. *The induced algebra on N/δ (in the algebra $\mathbf{A}/\delta$) is polynomially equivalent to a vector space of dimension one over a finite field $\mathbf{K}$.*
2. *The induced algebra $\mathbf{A}|_B$ is Mal'cev, nilpotent, and is an E–minimal algebra of type **2**.*
3. *If $\beta \in \mathrm{Con}(\mathbf{A})$ and $\beta \overset{s}{\sim} \beta \wedge \gamma$, then $\beta|_U \subseteq B^2 \cup T^2$.*
4. *$C(\theta, \gamma; \delta)$ holds in $\mathbf{A}$.*
5. *We have $\gamma = (\delta : S^2)$ for every subset S of A contained in a θ–block, and containing a $\langle \delta, \theta \rangle$–trace. Such subsets include, in particular, the E–traces of $\mathbf{A}$ with respect to θ that are not contained in δ.*
6. *The set B is the intersection of a γ–class of $\mathbf{A}$ with U, and is therefore an E–trace of $\mathbf{A}$.*
7. *If U is a minimal set for some other tame quotient, then the type of this quotient is **2** and B is the body of U with respect to this quotient.*

Proof. Statement (1) is the definition of a type **2** quotient, (2) follows from Theorem 4.31 and Lemma 4.36 of [6]. Theorem 2.6 shows that $\langle \delta, \theta \rangle$ is γ–regular and γ–coherent. By the definition of γ we have $C(\gamma, \theta; \delta)$, so (4) follows from Theorem 2.6 (4).

To prove (5) let $\beta \in \mathrm{Con}(\mathbf{A})$. Clearly, $C(\beta, S^2; \delta)$ is equivalent to $C(\beta, \theta; \delta)$ by coherence. This proves the first statement in (5). Now let $S = e(A) \cap a/\theta$ for some idempotent polynomial e of $\mathbf{A}$, and elements $a, b \in S$ such that $(a, b) \notin \delta$. Connect a and b by a sequence of $\langle \delta, \theta \rangle$–traces N_i. Then one of the sets $e(N_i)$ is not contained in a δ–block, so it is also a $\langle \delta, \theta \rangle$–trace, which is contained in S. Thus, (5) is proved.

Let N be a $\langle \delta, \theta \rangle$–trace contained in B. From (1) we get that $\theta|_N$ covers $\delta|_N$. As all $\langle \delta, \theta \rangle$–traces of U are polynomially isomorphic by Lemma 4.20 (5) of [6], we have

that $\theta|_B$ covers $\delta|_B$. Combining this with the fact that modulo $\delta|_B$, $\mathbf{A}|_B$ is nilpotent (by applying (2) to the algebra $\mathbf{A}/\delta$ and the prime quotient $\langle 0_{A/\delta}, \theta/\delta\rangle$), we have that $C(B^2, \theta|_B, \delta)$. Then we have $C(B^2, N^2; \delta)$, so $B^2 \subseteq (\delta : N^2) = \gamma$. On the other hand, $\gamma|_U$ is clearly contained in the congruence β defined in Lemma 4.27 (1) of [6], implying that $\gamma|_U \subseteq B^2 \cup T^2$. This proves (6). Also, in view of Lemma 4.27 (4) (ii) of [6], $\gamma|_U \subseteq B^2 \cup T^2$ and $\beta \overset{s}{\sim} \beta \wedge \gamma$ imply that $\beta|_U \subseteq B^2 \cup T^2$. This proves (3).

Finally, (7) is proved in Section 5 of [10]. □

We conclude this section by proving one more statement. In the following theorem, C^2 denotes the *binary centrality relation*. Its definition is similar to Definition 2.1, but here c and d must be elements, and not vectors (hence f is a binary polynomial). Clearly, binary centrality is weaker than centrality.

Theorem 2.12. *Let* $\mathbf{A}$ *be a finite algebra,* $\sigma_0, \sigma, \tau, \rho$ *congruences, and* L *a binary relation of* $\mathbf{A}$*. Suppose that*

- (i) $\sigma_0 \leq \sigma < \rho$*, and* σ *can be connected to* ρ *by a chain of prime quotients of type* **2**.
- (ii) $\tau \vee \rho \overset{s}{\sim} \rho$.

Then we have

$$C(\tau, L; \rho) \;\&\; C^2(L, \tau; \sigma_0) \Longrightarrow C(\tau, L; \sigma)\,.$$

Proof. Suppose that $C(\tau, L; \sigma)$ fails. As $C(\tau, L; \rho)$ holds, there is a prime quotient $\langle \delta, \theta\rangle$ of type **2** between σ and ρ such that $C(\tau, L; \delta)$ fails, but $C(\tau, L; \theta)$ holds. Thus, there exists a polynomial f, and elements and vectors $a\ \tau\ b$ and $\mathbf{c}\ L\ \mathbf{d}$ of $\mathbf{A}$ such that

$$\begin{array}{llll} s = f(a, \mathbf{c}) & \delta & t = f(a, \mathbf{d}), \\ u = f(b, \mathbf{c}) & \theta - \delta & v = f(b, \mathbf{d}) \end{array}$$

($u\ \theta\ v$ follows from $C(\tau, L; \theta)$). By tame congruence theory, there exists a unary polynomial h such that $(h(u), h(v)) \in \theta - \delta$, and $U = h(A)$ is a $\langle \delta, \theta\rangle$–minimal set. Then $h(u)$ and $h(v)$ are contained in the body B of U. We show that $h(s)$ and $h(t)$ are also in B.

Indeed, we show that the conditions of Lemma 2.11 (3) are satisfied with $\beta = \tau \vee \rho$. By our assumptions, $\beta \overset{s}{\sim} \rho \overset{s}{\sim} \delta$. On the other hand, $\gamma = (\delta : \theta) \geq \delta$ obviously holds, so $\delta \leq \beta \wedge \gamma \leq \beta$ and therefore $\beta \overset{s}{\sim} \beta \wedge \gamma$. Thus Lemma 2.11 (3) implies that $\beta|_U \subseteq B^2 \cup T^2$. On the other hand, $h(s)\ \beta\ h(u)$ and $h(t)\ \beta\ h(v)$, since $a\ \tau\ b$, so we have proved that $h(s)$ and $h(t)$ are in B.

Now let d be a pseudo–Mal'cev operation on U. Then Lemma 2.9 of [10] shows that $h(s)\ \delta\ h(t)$ implies $h(u)\ \delta\ h(v)$, and this contradiction proves the theorem. □

Corollary 2.13. *Let* α *and* β *be congruences of a finite algebra* $\mathbf{A}$*. Suppose that* $\mathrm{typ}\{\beta, \alpha \vee \beta\} = \{\mathbf{2}\}$*. Then* $[\alpha, \alpha] \leq \beta$ *implies that* $(\alpha \vee \beta)/\beta$ *is an abelian congruence, hence* $[\alpha \vee \beta, \alpha \vee \beta] \leq \beta$*.*

Proof. Apply Theorem 2.12 with $\sigma = \beta$ and $\rho = \alpha \vee \beta$. Then (i), (ii), and $C(\tau, L; \rho)$ are satisfied for every congruence $\tau \leq \alpha \vee \beta$ and for every binary relation L. So for every congruence $\sigma_0 \leq \beta$ we have that

$$C(L, \tau; \sigma_0) \Longrightarrow C(\tau, L; \beta)\,.$$

We apply this observation twice. First let $L = \tau = \alpha$ and $\sigma_0 = [\alpha, \alpha]$. Then $C(L, \tau; \sigma_0) = C(\alpha, \alpha; [\alpha, \alpha])$ obviously holds, so we get $C(\alpha, \alpha; \beta)$. Together with $C(\beta, \alpha; \beta)$ this implies $C(\alpha \vee \beta, \alpha; \beta)$ by the properties of the centrality relation

mentioned at the beginning of this section. Now apply the above implication again with $L = \alpha \vee \beta$, $\tau = \alpha$, and $\sigma_0 = \beta$. We get that $C(\alpha, \alpha \vee \beta; \beta)$ holds. But $C(\beta, \alpha \vee \beta; \beta)$ also holds, so finally we get $C(\alpha \vee \beta, \alpha \vee \beta; \beta)$, as desired. □

3. Coordinatization

Let α be a minimal abelian congruence of a finite algebra $\mathbf{A}$. As shown by tame congruence theory, the induced algebras on the $\langle 0_{\mathbf{A}}, \alpha\rangle$–traces have a very tight structure. In this section we show the same for subsets of the form $T = f(N, \dots, N)$, where N is a $\langle 0_{\mathbf{A}}, \alpha\rangle$–trace, and f is a polynomial of $\mathbf{A}$. We call such a set T a $\langle 0_{\mathbf{A}}, \alpha\rangle$–*multitrace*. Similar terminology will be used when $\langle 0_{\mathbf{A}}, \alpha\rangle$ is replaced with an arbitrary tame quotient. We shall learn that T is an E–trace of A with respect to α, and $\mathbf{A}|_T$ is term equivalent (or more precisely, isomorphic to an algebra which is term equivalent) to a matrix power of $\mathbf{A}|_N$ (see Theorem 3.10). We shall say that T is a *coordinatizable* subset of $\mathbf{A}$ (or, more specifically, that T is *coordinatizable by traces*). Thus, before starting our discussion, we have to summarize some facts on non–indexed products and matrix powers. The two main references are [13] and [20].

Definition 3.1. Let $\mathbf{A}_1, \dots, \mathbf{A}_k$ be algebras, and f_i an n–ary function on A_i for $1 \leq i \leq k$. Define the n–ary function $f_1 \times \cdots \times f_k$ on $A_1 \times \cdots \times A_k$ to act as f_i in the i–th component for $1 \leq i \leq k$, that is,

$$(f_1 \times \cdots \times f_k)(\mathbf{x}^1, \dots, \mathbf{x}^n) = \begin{pmatrix} f_1(x_1^1, \dots, x_1^n) \\ \vdots \\ f_k(x_k^1, \dots, x_k^n) \end{pmatrix},$$

where $\mathbf{x}^j \in A_1 \times \cdots \times A_k$ for $1 \leq j \leq n$, thought of as column vectors. We sometimes call this function the product of $f_1, \dots, f_n$. If f_i is the i–th projection for $1 \leq i \leq k$, then the resulting product is called the *diagonal operation* on $A_1 \times \cdots \times A_n$. The *non–indexed product* $\mathbf{A}_1 \otimes \cdots \otimes \mathbf{A}_k$ is defined to have underlying set $A_1 \times \cdots \times A_k$, and basic operations, for each non–negative integer n, of the form $f_1 \times \cdots \times f_k$, where f_i runs over all n–ary terms of $\mathbf{A}_i$ for $1 \leq i \leq k$.

Definition 3.2. Let $\mathbf{A}$ be an algebra and $k \geq 0$ an integer. The k*–th matrix power* of $\mathbf{A}$, denoted by $\mathbf{A}^{[k]}$, is defined to have underlying set A^k, and basic operations, for each non–negative integer n, of the form

$$f(\mathbf{x}^1, \dots, \mathbf{x}^n) = \begin{pmatrix} f_1(x_1^1, \dots, x_1^k, \dots, x_k^n) \\ \vdots \\ f_k(x_1^1, \dots, x_1^k, \dots, x_k^n) \end{pmatrix},$$

where $\mathbf{x}^j \in A^k$ for $1 \leq j \leq n$, thought of as column vectors, and f_i runs over all nk–ary term operations of $\mathbf{A}$ for $1 \leq i \leq k$.

The non–indexed product and the matrix power are considered non–indexed algebras, although we will see in the next theorem how to regard them as indexed algebras. The difference between the two types of operations is that, although both take as input a matrix of n columns and k rows, the component maps in the case of a matrix power can depend on all elements of this matrix, while in the case of a non–indexed product the i–th component map depends only on the i–th row. To get the clone (all terms) of the direct product $\mathbf{A}_1 \times \cdots \times \mathbf{A}_k$ (this makes sense only

if these algebras are of the same similarity type), one has to consider the reduct of $\mathbf{A}_1 \otimes \cdots \otimes \mathbf{A}_k$ consisting of the functions $f^{\mathbf{A}_1} \times \cdots \times f^{\mathbf{A}_k}$, where f is a term in the language of the algebras $\mathbf{A}_i$. We shall need one more special type of operation of a matrix power.

Definition 3.3. Let S be any set. The unary *shift operation* on S^k is defined by

$$s\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix} = \begin{pmatrix} x_n \\ x_1 \\ x_2 \\ \vdots \\ x_{n-1} \end{pmatrix}.$$

The following, easy–to–verify theorem collects some well–known facts concerning the concepts just defined. Statement (5) explains the name 'matrix power'.

Theorem 3.4. *Let $\mathbf{A}$ and $\mathbf{A}_1, \ldots, \mathbf{A}_k$ be algebras and $\mathbf{B} = \mathbf{A}_1 \otimes \cdots \otimes \mathbf{A}_k$. Let $\mathcal{V}$ be a variety with similarity type τ. Then the following hold.*

(1) *Every congruence of $\mathbf{B}$ is a product congruence (see [2], Definition 11.4), so $\mathbf{Con}(\mathbf{B})$ is isomorphic to the direct product $\mathbf{Con}(\mathbf{A}_1) \times \cdots \times \mathbf{Con}(\mathbf{A}_k)$.*

(2) *Every congruence of $\mathbf{A}^{[k]}$ is a product congruence of the form $\theta \times \cdots \times \theta$, where θ is a congruence of $\mathbf{A}$, so $\mathbf{Con}(\mathbf{A}^{[k]})$ is isomorphic to $\mathbf{Con}(\mathbf{A})$. This isomorphism preserves the notions defined in tame congruence theory (like centrality, type labeling, tameness).*

(3) *If the algebras $\mathbf{A}_1, \ldots, \mathbf{A}_k$ are of the same similarity type, τ, then the clone of $\mathbf{B}$ is generated by the clone of $\mathbf{A}_1 \times \cdots \times \mathbf{A}_k$, together with the diagonal operation. Thus we can regard $\mathbf{B}$ as an indexed algebra over the similarity type obtained by expanding τ by a new k-ary operation symbol.*

(4) *The clone of $\mathbf{A}^{[k]}$ is generated by all the operations in the (k–fold) non–indexed product $\mathbf{A} \otimes \cdots \otimes \mathbf{A}$, together with the shift operation. Thus, if $\mathbf{A}$ has similarity type τ, then we may regard $\mathbf{A}^{[k]}$ as an indexed algebra over the similarity type $\tau^{[k]}$, obtained by expanding τ by a new k-ary and a new unary operation symbol.*

(5) *Let $\mathbf{R}$ be an associative ring and $\mathbf{M}$ an $\mathbf{R}$–module. Then $\mathbf{M}^{[k]}$ is term equivalent to the module M^k considered over the $n \times n$ matrix ring over $\mathbf{R}$ in the usual way.*

(6) *The collection of all algebras of similarity type $\tau^{[k]}$ isomorphic to k–th matrix powers of algebras in $\mathcal{V}$ is a variety. It is denoted by $\mathcal{V}^{[k]}$ and called the k–th matrix power of $\mathcal{V}$. Every subvariety of $\mathcal{V}^{[k]}$ is of the form $\mathcal{U}^{[k]}$ for some subvariety $\mathcal{U} \subseteq \mathcal{V}$. In particular, $\mathcal{V}(\mathbf{A}^{[k]}) = (\mathcal{V}(\mathbf{A}))^{[k]}$.*

Now let us see what a coordinatizable subset is.

Definition 3.5. Let $\mathbf{A}$ be an algebra, n a positive integer, f an n–ary polynomial of $\mathbf{A}$, and $S_1, \ldots, S_n$ non–empty subsets of $\mathbf{A}$. We say that the set $T = f(S_1, \ldots, S_n)$ *can be coordinatized* (with respect to f and $S_1 \times \cdots \times S_n$), if there exist unary polynomials $g_1, \ldots, g_n$ of $\mathbf{A}$ satisfying

$$g_i(f(x_1, \ldots, x_n)) = x_i \qquad (x_1 \in S_1, \ldots, x_n \in S_n,\ 1 \leq i \leq n).$$

The g_i are called the coordinate maps (with respect to f and T).

First we investigate a weaker form of this condition.

Lemma 3.6. *Let $\mathbf{A}$ be a finite algebra, $S_1, \dots, S_n$ and T non–empty subsets of $\mathbf{A}$, and $g_1, \dots, g_n \in \mathrm{Pol}_1(\mathbf{A})$, $f \in \mathrm{Pol}_n(\mathbf{A})$ such that*

(i) $f(S_1, \dots, S_n) \subseteq T$;
(ii) $g_i(T) \subseteq S_i$ *for* $1 \leq i \leq n$;
(iii) $f(g_1(x), \dots, g_n(x)) = x$ *for all* $x \in T$.

Let $G : T \to S_1 \times \cdots \times S_n$ *be defined by*

$$G(x) = (g_1(x), \dots, g_n(x)),$$

and let $\mathsf{S} = G(T)$. *Then the following hold.*

(1) *The induced algebra* $(\mathbf{A}|_{S_1} \otimes \cdots \otimes \mathbf{A}|_{S_n})|_{\mathsf{S}}$ *is term equivalent to a reduct of* $\mathbf{A}|_T$.
(2) *If the sets* $S_1, \dots, S_n$ *are all equal, then* S *is the range of an idempotent unary polynomial of the algebra* $\mathbf{P} = (\mathbf{A}|_{S_1})^{[n]}$, *and* $\mathbf{A}|_T$ *is term equivalent to* $\mathbf{P}|_{\mathsf{S}}$.
(3) *If* α *is an arbitrary congruence of* $\mathbf{A}$, *and all the* S_i *are E–traces with respect to* α, *then* T *is an E–trace with respect to* α.

Proof. Let $F = f|_{\mathsf{S}} : \mathsf{S} \to T$. Then F and G are inverse bijections between S and T by *(iii)*. For a function $t : T^k \to T$ define $\overline{G}(t) : (S_1 \times \cdots \times S_n)^k \to \mathsf{S}$ by

$$\overline{G}(t)(\mathbf{x}^1, \dots, \mathbf{x}^k) = G(t(f(\mathbf{x}^1), \dots, f(\mathbf{x}^k))).$$

Similarly, to any $h : \mathsf{S}^k \to \mathsf{S}$ we can assign $\overline{F}(h)$ by composing it with G inside and F outside. This way we have set up inverse bijections between the set of all finitary functions on T and the set of all finitary functions on S. Let

$$\mathcal{C} = \{(\overline{G}(t))|_{\mathsf{S}} \;\Big|\; t \in \mathrm{Pol}(\mathbf{A}|_T)\}.$$

Clearly, G and F establish an isomorphism between the algebras $\mathbf{A}|_T$ and $(\mathsf{S}, \mathcal{C})$.

To prove (1), let h be a k–ary polynomial of $\mathbf{A}|_{S_1} \otimes \cdots \otimes \mathbf{A}|_{S_n}$ that can be restricted to S. Then $h = h_1|_{S_1} \times \cdots \times h_n|_{S_n}$, where the h_i are k–ary polynomials of $\mathbf{A}$ that can be restricted to S_i for $1 \leq i \leq n$. Define

$$t(x_1, \dots, x_k) = f(h_1(g_1(x_1), \dots, g_1(x_k)), \dots, h_n(g_n(x_1), \dots, g_n(x_k))).$$

Then t is a k–ary polynomial of $\mathbf{A}$ that can be restricted to T, and an easy calculation shows that $(\overline{G}(t|_T))|_{\mathsf{S}} = h|_{\mathsf{S}}$, proving (1).

To prove (2), assume $S_1 = \cdots = S_n$. To show that $\mathcal{C}$ is the clone of $\mathbf{P}|_{\mathsf{S}}$ let s be the unary shift operation of $\mathbf{P}$. Define $s'(x) = f(g_n(x), g_1(x), \dots, g_{n-1}(x))$. It is easy to check that $(\overline{G}(s'|_T))|_{\mathsf{S}} = s|_{\mathsf{S}}$ (in particular, the set S is closed under s). Thus, (1) and Theorem 3.4 (4) show that $\mathcal{C} \supseteq \mathrm{Clo}(\mathbf{P}|_{\mathsf{S}})$. For the converse inclusion, assume that $t \in \mathrm{Pol}_k(\mathbf{A})$ can be restricted to T. Then the definition of $h = \overline{G}(t|_T)$ clearly implies that its component maps are nk–ary polynomials of $\mathbf{A}$ that can be restricted to S_i, and that h preserves S, so indeed $h|_{\mathsf{S}} \in \mathrm{Clo}(\mathbf{P}|_{\mathsf{S}})$. Finally, $e = \overline{G}(id_T)$ is clearly an idempotent polynomial of $\mathbf{P}$ with range S. Thus (2) is proved.

To prove (3), let $S_i = e_i(A) \cap a_i/\alpha$ for some idempotent polynomials e_i of $\mathbf{A}$ and $a_i \in S_i$. Let

$$h(x) = f(e_1 g_1(x), \dots, e_n g_n(x)),$$

and let h^k be an idempotent power of h. We prove that $T = h^k(A) \cap a/\alpha$ for any $a \in T$. First we show that $h(a/\alpha) \subseteq T$. Indeed, if $b \in a/\alpha$, then $e_i g_i(b)\ \alpha\ e_i g_i(a) \in S_i$ by condition *(ii)*, so $e_i g_i(b) \in e_i(A) \cap a_i/\alpha = S_i$; hence $h(b) \in T$ by condition *(i)*. Thus, $h(a/\alpha) \subseteq T$. On the other hand, h acts on T as the identity map by

condition (*iii*), and by the same condition, T is contained in a single α–block. Hence, h is already idempotent on a/α, with range T. Therefore $e = h^k$ still has range T on a/α, but e is idempotent on A. If $e(c) \in a/\alpha$, then $e(c) = e(e(c)) \in T$, so indeed $T = e(A) \cap a/\alpha$, as stated. □

When we have a coordinatizable subset, we get a full matrix power, and not just an induced algebra on an E–trace.

Corollary 3.7. *Let* $\mathbf{A}$ *be a finite algebra,* f *an* n*–ary polynomial, and* $S_1, \ldots, S_n$ *non–empty subsets of* $\mathbf{A}$ *such that* $T = f(S_1, \ldots, S_n)$ *is coordinatizable with respect to* f *and* $S_1 \times \cdots \times S_n$*, with coordinate maps* $g_1, \ldots, g_n$*. Then the following hold.*

1. *If* α *is an arbitrary congruence of* $\mathbf{A}$*, then* T *is an E–trace with respect to* α *if and only if all the* S_i *are E–traces with respect to* α*.*
2. *If the sets* $S_1, \ldots, S_n$ *are polynomially isomorphic, then* $\mathbf{A}|_T$ *is term equivalent to the full matrix power* $(\mathbf{A}|_{S_i})^{[n]}$ *for all* $1 \leq i \leq n$*.*

Proof. First note that coordinatizable subsets satisfy conditions (*i*)–(*iii*) of Lemma 3.6 (to verify condition (*iii*), substitute a general element $x = f(x_1, \ldots, x_n)$ of T, where $x_i \in S_i$). In this case, however, we get that $\mathsf{S} = S_1 \times \cdots \times S_n$.

To show (2), let $h_i : S_i \to S_1$ be a polynomial isomorphism with polynomial inverse $k_i : S_1 \to S_i$. Set $g_i' = h_i \circ g_i$ and

$$f'(x_1, \ldots, x_n) = f(k_1(x_1), \ldots, k_n(x_n)) .$$

Clearly, T satisfies (*i*)–(*iii*) of Lemma 3.6 with respect to f', S_1^n, and g_i'. Thus, statement (2) of that lemma immediately implies (2).

To prove (1), first assume that the sets S_i are E–traces of $\mathbf{A}$ for $1 \leq i \leq n$. Then Lemma 3.6 (3) clearly implies that T is an E–trace with respect to α. For the converse we apply the same lemma, but with a different selection of subsets and polynomials. So assuming that T is an E–trace with respect to α, we want to show that S_i is also an E–trace. Let $n' = 1$, $T' = S_i$, $S_1' = T$, $f' = g_i$ and $g_1'(x) = f(c_1, \ldots, c_{i-1}, x, c_{i+1}, \ldots, c_n)$, where $c_j \in S_j$ are arbitrary, but fixed elements. It is straightforward to check that the conditions of Lemma 3.6 (3) are satisfied. Thus, the corollary is proved. □

Lemma 3.8. *Let* $\mathbf{A}$ *be a finite algebra,* S *a subset of* $\mathbf{A}$*, and* $T = f(S, \ldots, S)$ *for some* n*–ary polynomial* f *of* $\mathbf{A}$*. Suppose that* T *has more than one element, and*:

1. *The induced algebra* $\mathbf{A}|_S$ *is polynomially equivalent to a vector space over a finite field* $\mathbf{K}$ *with addition* $+$ *and zero element* 0*.*
2. *For any two elements* $a \neq b \in T$ *there exists a unary polynomial* g *of* $\mathbf{A}$ *that separates* a *and* b*, and maps* T *into* S*.*

Then T *is a coordinatizable subset of* $\mathbf{A}$ *with respect to* S^k *and a* k*–ary polynomial* f' *for some integer* $k \leq n$*.*

Proof. Let $0' = f(0, \ldots, 0) \in T$ and

$$\mathcal{G} = \{ g|_T \;\big|\; g \in \mathrm{Pol}_1(\mathbf{A}), g(T) \subseteq S, g(0') = 0 \} .$$

This is a finite dimensional vector space over $\mathbf{K}$ under pointwise operations. Let $g_1, \ldots, g_k$ be a basis. Since $g_i \circ f$ can be restricted to S, and maps 0 to 0, we can write

$$g_i(f(x_1, \ldots, x_n)) = \lambda_1^i x_1 + \cdots + \lambda_n^i x_n \qquad (x_j \in S,\, \lambda_j^i \in K,\, 1 \leq i \leq k,\, 1 \leq j \leq n).$$

As the mappings $g_1, \dots, g_k$ are linearly independent, so are the rows of the matrix

$$M = \begin{pmatrix} \lambda_1^1 & \dots & \lambda_n^1 \\ \vdots & & \vdots \\ \lambda_1^k & \dots & \lambda_n^k \end{pmatrix}.$$

This matrix induces a linear map $L : \mathbf{K}^n \to \mathbf{K}^k$, which is therefore onto. Thus $k \leq n$, and there exists a linear map $L' : \mathbf{K}^k \to \mathbf{K}^n$ satisfying $LL'(v) = v$ for all $v \in K^k$. Thus, the matrix M' of L' is such that MM' is the $k \times k$ identity matrix. Let

$$M' = \begin{pmatrix} \mu_1^1 & \dots & \mu_k^1 \\ \vdots & & \vdots \\ \mu_1^n & \dots & \mu_k^n \end{pmatrix},$$

and choose k–ary polynomials $\ell_j \in \mathrm{Pol}_k(\mathbf{A})$ satisfying

$$\ell_j(x_1, \dots, x_k) = \mu_1^j x_1 + \dots + \mu_k^j x_k \qquad (x_i \in S,\ 1 \leq i \leq k,\ 1 \leq j \leq n).$$

Finally, let

$$f'(x_1, \dots, x_k) = f(\ell_1(x_1, \dots, x_k), \dots, \ell_n(x_1, \dots, x_k)).$$

Then we have

$$g_i(f'(x_1, \dots, x_k)) = x_i \qquad (x_1, \dots, x_k \in S,\ 1 \leq i \leq k).$$

This is a simple calculation based on MM' being the identity matrix. So to finish the proof it is sufficient to show that $T = f'(S, \dots, S)$.

Clearly, $T \supseteq f'(S, \dots, S)$. To prove the converse inclusion, we first show that if $a \neq b \in T$, then there exists an i such that $g_i(a) \neq g_i(b)$. By condition (2), there is a $g \in \mathrm{Pol}_1(\mathbf{A})$ with $g(T) \subseteq S$ and $g(a) \neq g(b)$. Then $g(x) - g(0')$ still separates a and b, and this new function is an element of the vector space $\mathcal{G}$. As $g_1, \dots, g_k$ is a basis for this vector space, $g(x) - g(0')$ can be written as a linear combination of the maps g_i. Therefore $g_i(a) = g_i(b)$ indeed cannot happen for all i.

Now let $a \in T$ and $b = f'(g_1(a), \dots, g_k(a))$. It is sufficient to show that $a = b$, since $b \in f'(S, \dots, S)$. By the result of the previous paragraph, we have to show that $g_i(a) = g_i(b)$ for all $1 \leq i \leq k$. But this is clear, since the g_i are coordinate maps for f'. □

Lemma 3.9. *Let* $\mathbf{A}$ *be a finite algebra,* S *a subset of* $\mathbf{A}$*, and* $T = f(S, \dots, S)$ *for some* n*–ary polynomial* f *of* $\mathbf{A}$*. Suppose that* T *has more than one element, and*:

(*i*) *The induced algebra* $\mathbf{A}|_S$ *is permutational (that is, it is essentially unary, and every unary polynomial is either a permutation or constant).*

(*ii*) *For any two elements* $a \neq b \in T$ *there exists a unary polynomial* g *of* $\mathbf{A}$ *that separates* a *and* b*, and maps* T *into* S*.*

Then T *is a coordinatizable subset of* $\mathbf{A}$ *with respect to* S^k *and a* k*–ary polynomial* f' *for some integer* $k \leq n$*.*

Proof. If f does not depend on, say, its n–th variable on S, then let $f'(x_1, \dots, x_{n-1}) = f(x_1, \dots, x_{n-1}, c)$, where c is an arbitrary, but fixed element of S. Clearly, $T = f'(S, \dots, S)$. Hence, we may assume that f depends on all of its variables on S. We shall prove in this case that T is coordinatizable with respect to f. (Note that having f depend on several variables does not contradict condition (*i*). Condition (*i*) only asserts that if $h \in \mathrm{Pol}_k(\mathbf{A})$ has the property that $h(S^k) \subseteq S$, then $h|_S$ depends on at most one variable.)

To simplify notation, we shall construct the coordinate map g_1. As f depends on its first variable, there exist elements $a, b \in S$ and $\mathbf{c} \in S^{n-1}$ such that $f(a, \mathbf{c}) \neq f(b, \mathbf{c})$. Choose, by condition (ii), a unary polynomial g that maps T to S and separates $f(a, \mathbf{c})$ and $f(b, \mathbf{c})$. Hence, the polynomial

$$gf(x_1, \ldots, x_n)$$

depends on its first variable on S. This polynomial can be restricted to S. As the induced algebra $\mathbf{A}|_S$ is permutational, this polynomial does not depend on any other variable on S, and is a permutation in its first variable on S. Denote by m the order of this permutation, and let $h(x) = gf(x, \ldots, x)$. Then $h(x_1) = gf(x_1, x_2, \ldots, x_n)$, and hence

$$h^{m-1}gf(x_1, \ldots, x_n) = h^m(x_1) = x_1 \qquad (x_1, \ldots, x_n \in S).$$

Thus, $g_1 = h^{m-1} \circ g$ is the required coordinate map. □

Theorem 3.10. *Let α be an abelian congruence on a finite algebra $\mathbf{A}$ such that $\langle 0_{\mathbf{A}}, \alpha \rangle$ is tame, and let T be a $\langle 0_{\mathbf{A}}, \alpha \rangle$–multitrace. Then T is an E–trace with respect to α, it is coordinatizable by traces, and $\mathbf{A}|_T$ is term equivalent to $(\mathbf{A}|_N)^{[k]}$, where N is a $\langle 0_{\mathbf{A}}, \alpha \rangle$–trace.*

Proof. Depending on the type of $\langle 0, \alpha \rangle$, apply Lemma 3.8 or Lemma 3.9. Note that if $T = f(N, \ldots, N)$ for some n–ary polynomial f, then the resulting number k is at most n, but it is not necessarily equal to n. □

The conclusion of Theorem 3.10 (that T is an E–trace which is coordinatizable with respect to N^k) is false when α is nonabelian. However, in the type **3** case we still have the weaker conditions assumed in Lemma 3.6. Recall that an algebra is *primal* if every finitary operation on the universe of the algebra is a term operation of the algebra.

Lemma 3.11. *Let $\mathbf{A}$ be a finite algebra, S a subset of $\mathbf{A}$, and $T = f(S, \ldots, S)$ for some n–ary polynomial f of $\mathbf{A}$. Suppose that T has more than one element, and:*

- (i) *The induced algebra $\mathbf{A}|_S$ is primal.*
- (ii) *For any two elements $a \neq b \in T$ there exists a unary polynomial g of $\mathbf{A}$ that separates a and b, and maps T into S.*

Then there exist $g_1, \ldots, g_n \in \mathrm{Pol}_1(\mathbf{A})$ satisfying conditions (i)–(iii) of Lemma 3.6 (with $S_i = S$).

Proof. By the second hypothesis, we can choose unary polynomials $p_i(x)$ of $\mathbf{A}$, where $1 \leq i \leq k$ for some k, which map T into S and which separate the elements of T. For every $y \in T$ pick a vector $(x_1^y, \ldots, x_n^y)$ in S^n such that $f(x_1^y, \ldots, x_n^y) = y$. For $1 \leq i \leq n$ let h_i be a k–ary polynomial of $\mathbf{A}$ mapping S^k to S, and satisfying, for every $y \in T$,

$$h_i(p_1(y), \ldots, p_k(y)) = x_i^y \,.$$

Why do we have such polynomials? As the mapping that sends every $y \in T$ to the k–tuple $(p_1(y), \ldots, p_k(y)) \in S^k$ is one to one, there certainly exists a function h_i satisfying the above equation. But $\mathbf{A}|_S$ is primal, so the desired polynomials indeed exist. Now set

$$g_i(x) = h_i(p_1(x), \ldots, p_k(x)) \,.$$

Then the polynomials g_i clearly satisfy the conditions. □

Theorem 3.12. *Let $0 \prec \alpha$ be a type* **3** *minimal congruence on a finite algebra* $\mathbf{A}$ *and let T be a $\langle 0, \alpha\rangle$–multitrace. Then T is an E–trace with respect to α and $\mathbf{A}|_T$ is a primal algebra.*

Proof. The statement follows from Lemma 3.6 (2) and from Lemma 3.11, since a matrix power of a primal algebra is clearly primal and the algebra induced on any subset of a primal algebra is again primal. □

A second proof of the fact that $\mathbf{A}|_T$ is primal when the type is **3** can be obtained from Rosenberg's primal algebra classification. One can arrange things so that T is a maximal set of the form $f(N, \dots, N)$, where $N \subseteq T$ is a $\langle 0_{\mathbf{a}}, \alpha\rangle$–trace. These conditions imply that T is closed under f and therefore f is an operation of $\mathbf{A}|_T$. One can also arrange it so that $\mathbf{A}|_T$ has operations which restrict to give all Boolean operations on N. These Boolean operations together with f are incompatible with all Rosenberg–type relations.

It is not true in general that we can get coordinatization in the type **3** case. Indeed, consider any three–element primal algebra $\mathbf{A}$ and any two–element subset N of $\mathbf{A}$. Then there is a binary polynomial of $\mathbf{A}$ satisfying $f(N, N) = A$, but $\mathbf{A}$ is not coordinatizable, because its cardinality is not a power of 2.

Multitraces in the type **4** and **5** cases are even less well–behaved. Their behavior with respect to coordinatization will be discussed in a subsequent paper.

4. Minimal sets in subdirect powers

In this section, $\mathbf{A}$ will be a finite algebra and $\mathbf{C}$ will be a finite subdirect power of $\mathbf{A}$. We shall compare the structure of certain minimal sets in $\mathbf{C}$ to minimal sets in $\mathbf{A}$. We fix the following notation concerning $\mathbf{A}$: $\alpha, \beta, \gamma \in \mathrm{Con}(\mathbf{A})$, $\alpha \prec \beta$, $\mathrm{typ}(\alpha, \beta) = \mathbf{2}$ and $\beta \leq \gamma \leq (\alpha : \beta)$. If N is an $\langle \alpha, \beta\rangle$–trace, then $\mathbf{A}|_N/\alpha|_N$ is polynomially equivalent to a 1–dimensional vector space over a finite field. Let $\mathbf{K}$ denote that field. We assume that $\mathbf{C}$ is a subdirect subalgebra of $\mathbf{A}^k$, $k < \omega$, which satisfies $C \subseteq \gamma^{(k)}$. The condition $C \subseteq \gamma^{(k)}$ means that if $(c_1, \dots, c_k) \in C$, then $(c_i, c_j) \in \gamma$ for all $1 \leq i, j \leq k$. We fix the following notation for $\mathbf{C}$: $\alpha' = (\alpha^k)|_{\mathbf{C}}$, $\beta' = (\beta^k)|_{\mathbf{C}}$, and $\gamma' = (\gamma^k)|_{\mathbf{C}}$.

It can happen that the algebra $\mathbf{C}$ is very 'thin'. The results below are empty if $\alpha' = \beta'$. Let us call a coordinate i (with $1 \leq i \leq k$) *bad*, if $\mathbf{a}\ \beta'\ \mathbf{b}$ implies $a_i\ \alpha\ b_i$ for all elements $\mathbf{a}, \mathbf{b}$ of C; otherwise i is called a *good* coordinate. In other words, the good coordinates are those for which α' and β' map to different congruences under the i–th projection. We have $\alpha' < \beta'$ if and only if there exists at least one good coordinate. In 'normal' subalgebras of $\mathbf{A}^k$, for example when C contains the diagonal, every coordinate is automatically good. Throughout this section, we assume that there is at least one good coordinate.

The minimal sets in $\mathbf{C}$ that will concern us correspond to prime quotients which we call "centralized". We define $\langle \delta, \theta\rangle$ to be *centralized* if

(1) $\alpha' \leq \delta \prec \theta \leq \beta'$,
(2) $\mathrm{typ}(\delta, \theta) = \mathbf{2}$, and
(3) $C(\gamma', \theta; \delta)$ holds.

Of course, it is condition (3) which suggests the name "centralized". We want to describe the minimal sets corresponding to centralized quotients in $\mathbf{C}$. For this purpose, we let $\mathcal{M}$ denote the collection of all subsets of C which are minimal with respect to at least one centralized quotient.

Theorem 4.1. *If* $\mathbf{A}$, α, β, γ, $\mathbf{K}$, k, $\mathbf{C}$, α', β', γ' *and* $\mathcal{M}$ *are as above, then the following hold.*

1. *There exists a centralized quotient.*
2. *If* $\gamma \overset{s}{\sim} \beta$ *in* $\mathbf{Con}(\mathbf{A})$*, then all type* $\mathbf{2}$ *prime quotients in the interval* $I[\alpha', \beta']$ *are centralized.*
3. *Every member* U *of* $\mathcal{M}$ *is a minimal set with respect to each centralized quotient. The body and the tail of* U *are the same with respect to all centralized quotients.*
4. *If* $U \in \mathcal{M}$ *and* f *is a unary polynomial of* $\mathbf{C}$ *satisfying* $f(\beta'|_U) \not\subseteq \alpha'$*, then* $f(U) \in \mathcal{M}$ *and* f *is a polynomial isomorphism of* U *onto* $f(U)$*.*
5. *Let* $U \in \mathcal{M}$*,* M *the intersection of the body of* U *with a class of* β'*,* $\overline{\mathbf{C}} = \mathbf{C}/\alpha'$*, and* $\overline{M}$ *the image of* M *in this factor. Then* $\overline{\mathbf{C}}|_{\overline{M}}$ *is polynomially equivalent to a vector space over* $\mathbf{K}$ *of dimension at most* k*. For every* n*–ary polynomial* f *of* $\overline{\mathbf{C}}$*, the set* $f(\overline{M}, \dots, \overline{M})$ *is a coordinatizable* E*–trace of* $\overline{\mathbf{C}}$ *with respect to* $\overline{M}^{\ell}$ *for some* $\ell \leq n$*.*
6. *The elements of* $\mathcal{M}$ *are exactly the sets* $U = C \cap (e_1(A) \times \cdots \times e_k(A))$*, where* $(e_1, \dots, e_k)$ *is a sequence of simultaneous* C*–twins and each* e_i *is an idempotent polynomial of* $\mathbf{A}$ *with* $e_i(A) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$*. The body and tail of* U *are of the form* $C \cap (B_1 \times \cdots \times B_k)$ *and* $C \cap (T_1 \times \cdots \times T_k)$*, respectively, where* B_i *and* T_i *are the* $\langle \alpha, \beta \rangle$*–body and tail of* $e_i(A)$*.*

The six parts of Theorem 4.1 are proved in Lemmas 4.3, 4.6, 4.8, and 4.10. These lemmas depend on intermediate results.

We introduce the following notation for certain congruences of $\mathbf{C}$. For $1 \leq i \leq k$, let η_i be the i–th projection kernel restricted to $\mathbf{C}$, and

$$\begin{aligned} \alpha_i &= (1_{\mathbf{A}} \times \cdots \times 1_{\mathbf{A}} \times \alpha \times 1_{\mathbf{A}} \times \cdots \times 1_{\mathbf{A}})|_{\mathbf{C}}, \\ \beta_i &= (1_{\mathbf{A}} \times \cdots \times 1_{\mathbf{A}} \times \beta \times 1_{\mathbf{A}} \times \cdots \times 1_{\mathbf{A}})|_{\mathbf{C}}, \\ \rho_i &= (\beta \times \cdots \times \beta \times \alpha \times \beta \times \cdots \times \beta)|_{\mathbf{C}}, \end{aligned}$$

where α, β, and α occur in the i–th component of α_i, β_i, and ρ_i, respectively.

Lemma 4.2. *The following are true.*

1. $\alpha_i \prec \beta_i$ *and* $\mathrm{typ}(\alpha_i, \beta_i) = \mathbf{2}$ *for all* i*.*
2. $\alpha_i \wedge \beta' = \rho_i$ *for all* i*.*
3. i *is a good coordinate if and only if* $\beta' \not\leq \alpha_i$ *if and only if* $\alpha_i \vee \beta' = \beta_i$ *if and only if* $\rho_i < \beta'$ *if and only if* β_i/α_i *and* β'/ρ_i *are perspective quotients. If* i *is bad, then* $\rho_i = \beta'$*.*
4. *The intersection of all* ρ_i *for* $1 \leq i \leq k$ *is* α'*.*

Proof. (1) follows from the fact that $\mathbf{C}/\eta_i$ is isomorphic to $\mathbf{A}$, and β_i/η_i corresponds to β and α_i/η_i corresponds to α under this isomorphism. We get (2), (3), and (4) as straightforward consequences of the definitions and of (1). □

We prove Theorem 4.1 (1) and (2) immediately, to make it clear that the rest of the results in this section have content.

Lemma 4.3. *Assume the hypotheses of Theorem 4.1.*

1. *There exists a centralized quotient. In fact, if* $\alpha' = \delta \prec \theta \leq \beta'$*, then* $\langle \delta, \theta \rangle$ *is centralized.*
2. *If* $\gamma \overset{s}{\sim} \beta$ *in* $\mathbf{Con}(\mathbf{A})$*, then all type* $\mathbf{2}$ *prime quotients in the interval* $I[\alpha', \beta']$ *are centralized.*

Proof. For part (1), choose $\langle \delta, \theta \rangle$ so that $\alpha' = \delta \prec \theta \leq \beta'$. The quotient $\langle \delta, \theta \rangle$ is prime by choice. Since $\gamma \leq (\alpha : \beta)$ in $\mathbf{A}$, we get

$$\gamma' \leq (\alpha' : \beta') \leq (\alpha' : \theta) = (\delta : \theta)$$

in $\mathbf{C}$. Hence, $C(\gamma', \theta; \delta)$. What remains to be shown is that $\mathrm{typ}(\delta, \theta) = \mathbf{2}$.

Choose $(\mathbf{a}, \mathbf{b}) \in \theta - \delta$. We have $(\mathbf{a}, \mathbf{b}) \in \beta' - \alpha'$, so we have $(a_i, b_i) \in \beta - \alpha$ for some i. For this i we have $(\mathbf{a}, \mathbf{b}) \in \beta_i - \alpha_i$. Thus, we have

$$\alpha_i = \alpha_i \vee \delta < \alpha_i \vee \theta \leq \beta_i.$$

By Lemma 4.2, $\alpha_i \prec \beta_i$, so we conclude that $\langle \delta, \theta \rangle$ and $\langle \alpha_i, \beta_i \rangle$ are perspective. Hence, $\mathrm{typ}(\delta, \theta) = \mathrm{typ}(\alpha_i, \beta_i) = \mathbf{2}$.

To prove (2), first observe that $[\gamma, \beta] \leq \alpha$, so $[\gamma', \beta'] \leq \alpha'$. Now let $\langle \delta, \theta \rangle$ be an arbitrary type $\mathbf{2}$ prime quotient in $I[\alpha', \beta']$. We have

$$[\gamma', \theta] \leq [\gamma', \beta'] \leq \alpha' \leq \delta.$$

Since $\gamma \overset{s}{\sim} \beta$ in $\mathbf{Con}(\mathbf{A})$, we get that $\gamma' \overset{s}{\sim} \beta'$ in $\mathbf{Con}(\mathbf{C})$. This means that there is a k such that $[\gamma']^k \leq \beta'$. But $[\beta, \beta] \leq \alpha$, so $[\beta', \beta'] \leq \alpha'$ and therefore $[\gamma']^{k+1} \leq \alpha' \leq \theta$. Now Theorem 2.6 (4) applies to show that $[\gamma', \theta] \leq \delta$ (which holds) is equivalent to $C(\gamma', \theta; \delta)$. Hence $\langle \delta, \theta \rangle$ is centralized. □

Lemma 4.4. *For every congruence ρ of $\mathbf{C}$ with $\alpha' < \rho \leq \beta'$ and for each good i we have that*

$$\mathrm{Sep}(\alpha', \rho) = \mathrm{Sep}(\alpha', \beta') = \mathrm{Sep}(\alpha_i, \beta_i).$$

Proof. We first show that $\mathrm{Sep}(\alpha', \rho) = \mathrm{Sep}(\alpha', \beta')$. Let $f \in \mathrm{Pol}_1(\mathbf{C})$. Since $\mathrm{Sep}(\alpha', \rho) \subseteq \mathrm{Sep}(\alpha', \beta')$, clearly, we have to show that if $f(\rho) \subseteq \alpha'$, then $f(\beta') \subseteq \alpha'$. Assume that $f(\rho) \subseteq \alpha'$ and let the components of f be $f_1, \ldots, f_k$. Set

$$\psi_i = \{(x, y) \in \beta \mid (\forall g \in \mathrm{Pol}_1(\mathbf{A}))\ (f_i g(x)\ \alpha\ f_i g(y))\}.$$

It is easy to see that this is a congruence of $\mathbf{A}$ for every i, and $\alpha \leq \psi_i \leq \beta$. As $\mathbf{C}$ is a subdirect power of $\mathbf{A}$, for every $g \in \mathrm{Pol}_1(\mathbf{A})$ and any given $1 \leq i \leq k$ there exists a unary polynomial $\hat{g}$ of $\mathbf{C}$ that acts as g in the i–th component. This implies that if

$$\mathbf{a} = (a_1, \ldots, a_n)\ \rho\ (b_1, \ldots, b_n) = \mathbf{b},$$

then $a_i\ \psi_i\ b_i$ for all i (as f collapses ρ to α'). Now $\rho \neq \alpha'$, so we can choose $\mathbf{a}$, $\mathbf{b}$, and i so that $(a_i, b_i) \notin \alpha$. Then $a_i\ \psi_i\ b_i$ implies that $\psi_i \neq \alpha$, so by $\alpha \prec \beta$ we have that $\psi_i = \beta$. Setting g to be the identity map of $\mathbf{A}$, we see that $f_i(x)\ \alpha\ f_i(y)$ holds for all $x\ \beta\ y$; that is, f_i collapses β into α. Now we use the fact that $C \subseteq \gamma^{(k)}$. As the polynomials f_i are C–twins, they are $(\alpha : \beta)$–twins also. If one collapses β to α, then so do all the others. Thus, we indeed have $f(\beta') \subseteq \alpha'$.

The argument that $\mathrm{Sep}(\alpha', \beta') \subseteq \mathrm{Sep}(\alpha_i, \beta_i)$ is not very different from the above. Using the fact that $\mathbf{C}$ is a subdirect power of $\mathbf{A}$, one gets that any polynomial f for which $f(\beta_i) \subseteq \alpha_i$ has i–th component f_i such that $f_i(\beta) \subseteq \alpha$. As argued above, every component of f collapses β into α, and so $f(\beta') \subseteq \alpha'$.

Now we argue that $\mathrm{Sep}(\alpha_i, \beta_i) \subseteq \mathrm{Sep}(\alpha', \beta')$. Since i is good, Lemma 4.2 (3) proves that β'/ρ_i is perspective with β_i/α_i. Hence, $\mathrm{Sep}(\alpha_i, \beta_i) = \mathrm{Sep}(\rho_i, \beta')$. Since $\alpha' \leq \rho_i < \beta'$, we get $\mathrm{Sep}(\rho_i, \beta') \subseteq \mathrm{Sep}(\alpha', \beta')$. These last two sentences give the desired conclusion. □

Lemma 4.5. *Let $\langle \delta, \theta \rangle$ be a centralized quotient, choose $U \in \mathrm{M}_{\mathbf{C}}(\delta, \theta)$ and denote the body of U by B.*

(1) $\beta_i \leq (\delta : \theta)$ *for each* i.
(2) *The lattice interval between* $\alpha'|_B$ *and* $\beta'|_B$ *in* $\mathbf{Con}(\mathbf{C}|_B)$ *is a complemented modular lattice.*
(3) $\mathrm{Sep}(\delta, \theta) = \mathrm{Sep}(\alpha', \beta')$.

Proof. Since $C \subseteq \gamma^{(k)}$ and $\beta \leq \gamma$, we get that $\beta_i \leq \gamma'$ for all i. Since $\langle \delta, \theta \rangle$ is centralized, we get that $\beta_i \leq \gamma' \leq (\delta : \theta)$. This proves (1).

Since B is an E–trace with respect to $(\delta : \theta)$, the restriction map is a homomorphism from the interval $I[0, (\delta : \theta)]$ of $\mathbf{Con}(\mathbf{C})$ onto $\mathbf{Con}(\mathbf{C}|_B)$. Since $\beta_i \leq (\delta : \theta)$, by (1), and $\alpha_i \prec \beta_i$, by Lemma 4.2 (1), we get that $\alpha_i|_B = \beta_i|_B$ or $\alpha_i|_B \prec \beta_i|_B$ in $\mathbf{Con}(\mathbf{C}|_B)$. The induced algebra $\mathbf{C}|_B$ is Mal'cev, so the lattice $\mathbf{Con}(\mathbf{C}|_B)$ is modular. Using Lemma 4.2 and the modularity of $\mathbf{Con}(\mathbf{C}|_B)$, we get that $\rho_i|_B = \beta'|_B$ or $\rho_i|_B \prec \beta'|_B$ for all i. Since $\alpha' = \bigcap_{i=1}^k \rho_i$, then by restriction to B we find that $\alpha'|_B$ is a meet of lower covers of $\beta'|_B$. This is enough to force the lattice interval $I[\alpha'|_B, \beta'|_B]$ to be a complemented modular lattice. This proves (2).

By Lemma 4.4, we have $\mathrm{Sep}(\alpha', \beta') = \mathrm{Sep}(\alpha_i, \beta_i)$ for any good i. To prove (3), we will show that $\mathrm{Sep}(\alpha_i, \beta_i) = \mathrm{Sep}(\delta, \theta)$ for some good i. Since $I[\alpha'|_B, \beta'|_B]$ is a complemented modular lattice for which $\rho_i|_B = \beta'|_B$ or $\rho_i|_B \prec \beta'|_B$ for each i and $\alpha'|_B = \bigcap_{i=1}^k \rho_i|_B$, then the prime quotient $\langle \delta|_B, \theta|_B \rangle$ is projective to some prime quotient $\langle \rho_i|_B, \beta'|_B \rangle$. Since $I[\alpha'|_B, \beta'|_B]$ is complemented and modular, we can project in two steps from $\theta|_B/\delta|_B$ to $\beta'|_B/\rho_i|_B$:

$$\theta|_B/\delta|_B \searrow \mu/\nu \nearrow \beta'|_B/\rho_i|_B$$

for some congruences $\mu, \nu \in \mathrm{Con}(\mathbf{C}|_B)$. Necessarily i is good, so Lemma 4.2 (3) proves that $\beta'/\rho_i \nearrow \beta_i/\alpha_i$. Therefore, we even have that

$$\theta|_B/\delta|_B \searrow \mu/\nu \nearrow \beta_i|_B/\alpha_i|_B.$$

Set $\hat{\mu} = \mathrm{Cg}^{\mathbf{C}}(\mu)$ and let $\hat{\nu}$ be the largest congruence on $\mathbf{C}$ for which $\hat{\nu} \leq \hat{\mu}$ and $\hat{\nu}|_B = \nu$. Then, since $\delta \prec \theta$, $\alpha_i \prec \beta_i$ and restriction to B is a lattice homomorphism, we get that

$$\theta/\delta \searrow \hat{\mu}/\hat{\nu} \nearrow \beta_i/\alpha_i$$

in $\mathbf{Con}(\mathbf{C})$. This forces

$$\mathrm{Sep}(\delta, \theta) = \mathrm{Sep}(\hat{\nu}, \hat{\mu}) = \mathrm{Sep}(\alpha_i, \beta_i)$$

and finishes the proof of (3). □

Now we prove part (3) of Theorem 4.1.

Lemma 4.6. *Assume the hypotheses of Theorem 4.1.*

(3) *Every member* U *of* $\mathcal{M}$ *is a minimal set with respect to each centralized quotient. The body and the tail of* U *are the same with respect to all centralized quotients.*

Proof. We proved in Lemma 4.5 that $\mathrm{Sep}(\delta, \theta) = \mathrm{Sep}(\alpha', \beta')$ when $\langle \delta, \theta \rangle$ is centralized. It follows that $\mathrm{M}_{\mathbf{C}}(\delta, \theta) = \mathrm{M}_{\mathbf{C}}(\alpha', \beta')$; therefore, a set is a minimal set for one centralized quotient if and only if it is a minimal set for all centralized quotients. It follows that $\mathrm{M}_{\mathbf{C}}(\delta, \theta) = \mathcal{M}$. The second part of this lemma follows from Lemma 2.11 (7). □

We are at a point where it is possible to identify exactly which quotients are centralized and which are not. In the next lemma, let ρ' be the congruence on $\mathbf{C}$ which is the join of all congruences ρ such that $\alpha' \prec \rho \leq \beta'$.

Lemma 4.7. *The following are true of ρ'.*

(1) *$\langle \alpha', \rho' \rangle$ is tame of type $\mathbf{2}$.*
(2) *$\mathrm{M}_{\mathbf{C}}(\alpha', \rho') = \mathcal{M}$.*
(3) *The $\langle \alpha', \rho' \rangle$–body of any $U \in \mathcal{M}$ is the same as the $\langle \delta, \theta \rangle$–body for any centralized quotient $\langle \delta, \theta \rangle$.*
(4) *$\rho'|_U = \beta'|_U$ for all $U \in \mathcal{M}$.*
(5) *Every type $\mathbf{2}$ prime quotient in the interval $I[\alpha', \rho']$ is centralized. Every centralized quotient is perspective with one in the interval $I[\alpha', \rho']$. No centralized quotient is contained in $I[\rho', \beta']$.*

Proof. The following observation will be useful in this proof.

Claim 1. For any $U \in \mathcal{M}$, the mappings $\rho \mapsto \rho|_U$ and $\sigma \mapsto \mathrm{Cg}^{\mathbf{C}}(\alpha' \cup \sigma)$ are inverse bijections between $\{\rho \in \mathrm{Con}(\mathbf{C}) \;\big|\; \alpha' \prec \rho \leq \beta'\}$ and $\{\sigma \in \mathrm{Con}(\mathbf{C}|_U) \;\big|\; \alpha'|_U \prec \sigma \leq \beta'|_U\}$.

Proof of Claim 1. Choose a congruence ρ such that $\alpha' \prec \rho \leq \beta'$ and a $U \in \mathcal{M}$. By Lemma 4.3 (1), the quotient $\langle \alpha', \rho \rangle$ is centralized. Hence $U \in \mathrm{M}_{\mathbf{C}}(\alpha', \rho)$, and so $\alpha'|_U < \rho|_U$. This implies that $\alpha'|_U \prec \rho|_U$. Since restriction to U is a lattice homomorphism of $I[\alpha', \beta']$ onto $I[\alpha'|_U, \beta'|_U]$, we must have that distinct covers of α' restrict to distinct covers of $\alpha'|_U$. It is clear that $\alpha' < \mathrm{Cg}^{\mathbf{C}}(\alpha' \cup \rho|_U) \leq \rho$, so $\mathrm{Cg}^{\mathbf{C}}(\alpha' \cup \rho|_U) = \rho$ since $\alpha' \prec \rho$.

To finish, we must show that any cover of $\alpha'|_U$ in $I[\alpha'|_U, \beta'|_U]$ is the restriction of a cover of α' in $I[\alpha', \beta']$. Choose σ so that $\alpha'|_U \prec \sigma \leq \beta'|_U$. For $\tau = \mathrm{Cg}^{\mathbf{C}}(\alpha' \cup \sigma)$, we clearly have $\alpha' < \tau \leq \beta'$. Choose some congruence λ with $\alpha' \prec \lambda \leq \tau$. Then

$$\alpha'|_U \prec \lambda|_U \leq \tau|_U = \sigma,$$

since we have shown that covers of α' restrict to covers of $\alpha'|_U$. But then $\lambda|_U = \sigma$, since σ covers $\alpha'|_U$. Claim 1 is proven. □

Lemmas 4.4 and 4.5 (3) prove that

$$\mathrm{Sep}(\alpha', \rho') = \mathrm{Sep}(\alpha', \beta') = \mathrm{Sep}(\delta, \theta)$$

for any centralized $\langle \delta, \theta \rangle$. Hence, $\mathrm{M}_{\mathbf{C}}(\alpha', \rho') = \mathrm{M}_{\mathbf{C}}(\delta, \theta) = \mathcal{M}$, proving (2). It now follows that any member of $\mathrm{M}_{\mathbf{C}}(\alpha', \rho')$ is the image of an idempotent polynomial. To prove that $\langle \alpha', \rho' \rangle$ is tame we must verify that the restriction map from $I[\alpha', \rho']$ to $I[\alpha'|_U, \rho'|_U]$ is 0,1–separating for any $U \in \mathcal{M}$.

If restriction were not 0–separating, then we would have $\alpha'|_U = \rho|_U$ for some ρ satisfying $\alpha' \prec \rho \leq \beta'$. Claim 1 shows that this does not happen, so restriction is 0–separating. Choose σ such that $\alpha' \leq \sigma \prec \rho'$. From the definition of ρ', there is a congruence ρ such that $\alpha \prec \rho \leq \rho'$, where $\rho \not\leq \sigma$. We get that $\rho/\alpha' \nearrow \rho'/\sigma$. Hence, if $\sigma|_U = \rho'|_U$, we also have $\alpha'|_U = \rho|_U$, which is false. Thus, $\sigma|_U \neq \rho'|_U$ for any lower cover of ρ' in $I[\alpha', \rho']$. This proves that restriction is 1–separating. We get that $\langle \alpha', \rho' \rangle$ is tame. Since $I[\alpha', \beta']$ is a solvable interval containing ρ', it must be that $\mathrm{typ}(\alpha', \rho') \in \{\mathbf{1}, \mathbf{2}\}$. But, we showed in Lemma 4.3 that for any ρ such that $\alpha' \prec \rho \leq \rho'$ we have $\mathrm{typ}(\alpha', \rho) = \mathbf{2}$. Hence, $I[\alpha', \rho']$ is not strongly solvable. We infer that $\mathrm{typ}(\alpha', \rho') = \mathbf{2}$. This proves (1).

Parts (1) and (2) of this lemma combine with part (7) of 2.11 to establish (3).

We now prove (5). Let $\langle \delta, \theta \rangle$ be an arbitrary centralized quotient, choose $U \in \mathcal{M}$ and let B be the body of U. By Lemma 4.5 (2), the interval $I[\alpha'|_B, \beta'|_B]$ is a complemented modular lattice. We have $\delta|_B < \theta|_B$, since $U \in \mathrm{M}_{\mathbf{C}}(\delta, \theta)$. Hence,

there is a congruence $\sigma \in \mathrm{Con}(\mathbf{C}|_B)$ which is a complement to $\delta|_B$ in $I[\alpha'|_B, \theta|_B]$. By Claim 1, σ is the restriction to B of some $\rho \in \mathrm{Con}(\mathbf{C})$ with $\alpha' \prec \rho \leq \beta'$. It follows that $\rho/\alpha' \nearrow \theta/\delta$. This proves the part of (5) which asserts that every centralized quotient is perspective with one in the interval $I[\alpha', \rho']$. It also proves that no centralized quotient is contained in $I[\rho', \beta']$, since no prime quotient in this interval is perspective with any ρ/α' when $\alpha' \prec \rho \leq \beta'$. To finish the proof of (5) we must explain why every type **2** prime quotient in the interval $I[\alpha', \rho']$ is centralized.

Theorem 7.7 (4) of [6] shows that $I[\alpha', \rho']/\overset{ss}{\sim}$ is a modular lattice. Since the atoms of this lattice join to the top element, then every element of this lattice is a join of atoms. This implies that every prime quotient in $I[\alpha', \rho']/\overset{ss}{\sim}$ is perspective with one of the form $(\rho/\overset{ss}{\sim})/(\alpha'/\overset{ss}{\sim})$ for some ρ satisfying $\alpha' \prec \rho \leq \beta'$. It then follows from Lemma 6.5 of [6] that any type **2** prime quotient in the interval $I[\alpha', \rho']$ is perspective with a centralized quotient of the form $\langle \alpha', \rho \rangle$. If $\langle \delta, \theta \rangle$ is a type **2** prime quotient in the interval $\langle \alpha', \rho' \rangle$ and $U \in \mathrm{M}_{\mathbf{C}}(\delta, \theta) = \mathcal{M}$, then as noted earlier the $\langle \delta, \theta \rangle$–body and tail of U are the same as they would be for any centralized quotient. It follows from Lemma 2.11 (6) that $\gamma'|_U \subseteq B^2 \cup T^2$ for this body and tail, and so to prove that $C(\gamma', \theta; \delta)$ it suffices, by Lemma 2.6, to observe that

$$[\gamma', \theta] \leq [\gamma', \beta'] \leq \alpha' \leq \delta.$$

This finishes the proof of (5).

Claim 2. Whenever $\alpha' \leq \delta \prec \theta \leq \beta'$ and $\delta|_U < \theta|_U$ for some $U \in \mathcal{M}$, then $\langle \delta, \theta \rangle$ is centralized.

Proof of Claim 2. To see this, we argue first that $U \in \mathrm{M}_{\mathbf{C}}(\delta, \theta)$. Since $\delta|_U < \theta|_U$, it is clear that U contains a $\langle \delta, \theta \rangle$–minimal set. (In more detail, if $e \in E(\mathbf{C})$ is such that $e(C) = U$, then $e(\theta) \not\subseteq \delta$, so $U = e(C)$ contains a $\langle \delta, \theta \rangle$–minimal set.) However, if $V \subset U$ is a $\langle \delta, \theta \rangle$–minimal set properly contained in U and $f \in E(\mathbf{C})$ is such that $f(C) = V$, then $f \notin \mathrm{Sep}(\alpha', \rho') = \mathrm{Sep}(\alpha', \beta')$. Hence $f \notin \mathrm{Sep}(\delta, \theta)$. But this is impossible since $f(\theta|_V) \not\subseteq \delta$. We conclude that $U \in \mathrm{M}_{\mathbf{C}}(\delta, \theta)$. Since U is already known to be minimal with respect to some centralized quotient, it follows that $\mathrm{typ}(\delta, \theta) = \mathbf{2}$ and that the $\langle \delta, \theta \rangle$–body and tail are the same as they would be for any centralized quotient. Hence, $\gamma'|_U \subseteq B^2 \cup T^2$ for this body and tail. The proof that $C(\gamma', \theta; \delta)$ holds is the same as in the paragraph preceding the statement of Claim 2. □

Now (4) follows from Claim 2 and the part of (5) which states that no centralized quotient is contained in $I[\rho', \beta']$. This finishes the proof of the lemma. □

Parts (4) and (5) of Theorem 4.1 are now easy to prove.

Lemma 4.8. *Assume the hypotheses of Theorem 4.1.*

(4) *If $U \in \mathcal{M}$ and f is a unary polynomial of $\mathbf{C}$ satisfying $f(\beta'|_U) \not\subseteq \alpha'$, then $f(U) \in \mathcal{M}$, and f is a polynomial isomorphism of U onto $f(U)$.*

(5) *Let $U \in \mathcal{M}$, M the intersection of the body of U with a class of β', $\overline{\mathbf{C}} = \mathbf{C}/\alpha'$, and $\overline{M}$ the image of M in this factor. Then $\overline{\mathbf{C}}|_{\overline{M}}$ is polynomially equivalent to a vector space over $\mathbf{K}$ of dimension at most k. For every n–ary polynomial f of $\overline{\mathbf{C}}$, the set $f(\overline{M}, \ldots, \overline{M})$ is a coordinatizable E–trace of $\overline{\mathbf{C}}$ with respect to $\overline{M}^{\ell}$ for some $\ell \leq n$.*

Proof. By Lemma 4.7, $\beta'|_U = \rho'|_U$; so (4) is simply a restatement of Theorem 2.8 (3) of [6] for the tame quotient $\langle \alpha', \rho' \rangle$.

Now we prove (5). Since $\beta'|_U = \rho'|_U$, the set M is simply an $\langle \alpha', \rho' \rangle$–trace of U. Clearly, $\overline{\mathbf{C}}|_{\overline{M}}$ is isomorphic to $(\mathbf{C}|_M)/(\alpha'|_M)$, which is polynomially equivalent to a vector space since $\langle \alpha', \rho' \rangle$ is tame of type **2**. The dimension of this vector space is the same as the height of the lattice $I[\alpha'|_M, \rho'|_M] = I[\alpha'|_M, \beta'|_M]$. But the latter lattice is a homomorphic image of $I[\alpha'|_B, \beta'|_B]$ by Lemma 2.4 of [6]. We proved in Lemma 4.5 that $I[\alpha'|_B, \beta'|_B]$ is a complemented modular lattice, where $\alpha'|_B = \bigcap_{i=1}^k \rho_i|_B$. Since each $\rho_i|_B$ is either equal to $\beta'|_B$ or a coatom in $I[\alpha'|_B, \beta'|_B]$, we get that $\alpha'|_B$ is a meet of at most k coatoms in $I[\alpha'|_B, \beta'|_B]$. This proves that the height of $I[\alpha'|_B, \beta'|_B]$ (and therefore of $I[\alpha'|_M, \beta'|_M]$) is at most k.

Let $\mathbf{K}'$ denote the field over which $(\mathbf{C}|_M)/(\alpha'|_M)$ is a vector space. If i is good, then $\rho_i|_B \prec \beta'|_B = \rho'|_B$. Since M is an $\langle \alpha', \rho' \rangle$–trace, and all traces are polynomially isomorphic, $\rho_i|_M \prec \rho'|_M$ in $\mathrm{Con}(\mathbf{C}|_M)$. Let M' denote the $\beta_i|_U$–class containing M and let e be an idempotent polynomial of $\mathbf{C}$ with range U. Clearly, M'/α_i is an E–trace of $\mathbf{C}/\alpha_i$ with respect to (β_i/α_i) and $e(x)/\alpha_i$, since M' is an E–trace of $\mathbf{C}$ with respect to β_i ($> \alpha_i$) and $e(x)$. Since $\beta_i \leq \gamma'$, we get $\beta_i|_U \subseteq B^2 \cup T^2$, and so $M' \subseteq B$. The fact that $\mathbf{C}|_B$ is Mal'cev implies that

$$\beta'|_B \circ \alpha_i|_B = \beta'|_B \vee \alpha_i|_B = (\beta' \vee \alpha_i)|_B = \beta_i|_B,$$

so $M \subseteq M'$ and each element of M' is α_i–related to an element of M. We conclude that $M/\alpha_i = M'/\alpha_i$. In particular, M/α_i is an E–trace of $\mathbf{C}/\alpha_i$ with respect to (β_i/α_i) and $e(x)/\alpha_i$.

Now, $(\mathbf{C}|_M)/(\alpha'|_M)$ is a $\mathbf{K}'$–space and $\rho_i|_M = \alpha_i|_M$ is a maximal congruence of $\mathbf{C}|_M$ above $\alpha'|_M$, and so it follows that the algebra $(\mathbf{C}|_M)/(\alpha_i|_M)$ is polynomially equivalent to a 1–dimensional $\mathbf{K}'$–space. At the same time M/α_i is an E–trace with respect to (β_i/α_i) in $\mathbf{C}/\alpha_i$, which forces it to be a $\langle 0_{C/\alpha_i}, (\beta_i/\alpha_i) \rangle$–trace. But $\mathbf{C}/\alpha_i \cong \mathbf{A}/\alpha$, and (β_i/α_i) corresponds to (β/α) under this isomorphism. The field associated with any $\langle \alpha, \beta \rangle$–trace is $\mathbf{K}$, so we have $\mathbf{K}' = \mathbf{K}$.

The coordinatizability of sets of the form $f(\overline{M}, \ldots, \overline{M})$ follows directly from Lemma 3.8. This finishes the proof of (5). □

Centralized quotients will play almost no role in the rest of this section, so now seems a good time to present an example to justify the amount of attention we have paid them.

The structure of minimal sets of type **2** in subdirect powers would be easier to describe if all type **2** prime quotients in the interval $I[\alpha', \beta']$ were centralized. Unfortunately, as the next example witnesses, that is not always the case (however, recall Lemma 4.3 (2)).

Example. (Some quotients may not be centralized.) Our example has universe $\{0, 1, 2\}$ and a single basic operation, which is binary, and has the table

$\circ$	0	1	2
0	0	1	1
1	1	0	0
2	1	0	2

$\mathbf{A}$ is the algebra $\langle \{0, 1, 2\}; \circ \rangle$. The only congruences of $\mathbf{A}$ are $\alpha = 0_{\mathbf{A}}$, $\beta = \mathrm{Cg}(0, 1)$, and $\gamma = 1_{\mathbf{A}}$. It is not hard to check by hand or computer that $C(\gamma, \beta; \alpha)$ holds. Furthermore, $\mathrm{typ}(\alpha, \beta) = \mathbf{2}$, and the unique member of $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ is the set $N = \{0, 1\}$. We choose $\mathbf{C}$ to equal $\mathbf{A}^2$. In this example, $\alpha' = 0_{\mathbf{C}}$, $\beta' = \beta \times \beta$ and $\gamma' = 1_{\mathbf{C}}$. $\mathbf{C}$ has twenty-four congruences, so we will not try to display them all.

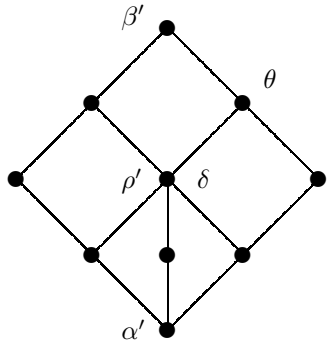

FIGURE 3. $I[\alpha', \beta]$.

What interests us are the ten congruences in the interval $I[\alpha', \beta']$. Their relative positions are shown in Figure 3. All prime quotients shown in this picture are of type **2**. In Figure 3, $\rho' = \delta \prec \theta \prec \beta'$.

From Lemma 4.7 (5) we see that neither $\langle \delta, \theta \rangle$ nor $\langle \theta, \beta' \rangle$ is centralized even though they both are prime quotients of type **2** which lie between α' and β'. To see that the minimal sets corresponding to non–centralized quotients must be handled in a different way, we note that $\mathrm{M}_{\mathbf{C}}(\alpha', \rho') = \mathcal{M} = \{N \times N\}$, $\mathrm{M}_{\mathbf{C}}(\delta, \theta) = \{N \times A\}$, and $\mathrm{M}_{\mathbf{C}}(\theta, \beta') = \{A \times N\}$.

Now we resume the main line of our argument. Fix an element $U \in \mathcal{M}$ and let B and T be the $\langle \alpha', \rho' \rangle$–body and tail, respectively. B is an E–trace of $\mathbf{C}$, and $\mathbf{C}|_B$ is Mal'cev and E–minimal. Choose an idempotent polynomial e of $\mathbf{C}$ such that $e(C) = U$, denote the components of e by $e_1, \ldots, e_k$, and let $U_i = e_i(A)$. Clearly, $(e_1, \ldots, e_k)$ is a sequence of simultaneous C–twins, where each component is an idempotent polynomial of $\mathbf{A}$. Furthermore, the idempotence of each e_i implies that

$$U = C \cap (U_1 \times \cdots \times U_k).$$

Denote by B_i and T_i the image of B and T under the i–th projection. Since $\mathbf{C}|_B/\eta_i|_B$ is isomorphic to $\mathbf{A}|_{B_i}$, it follows that $\mathbf{A}|_{B_i}$ is Mal'cev and E–minimal.

Lemma 4.9. *We have $U_i \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ for all i. The body and tail of U_i are B_i and T_i, respectively.*

Proof. Since $e \in \mathrm{Sep}(\alpha', \beta')$, we get that $e_i \in \mathrm{Sep}(\alpha, \beta)$ for at least one i. This implies that $e_i \in \mathrm{Sep}(\alpha, \beta)$ for all i, since the e_i are simultaneous C–twins, $C \subseteq \gamma^{(k)}$ and $\gamma \leq (\alpha : \beta)$. From this it follows that each $U_i = e_i(A)$ contains an $\langle \alpha, \beta \rangle$–minimal set. Assume that, say, U_1 properly contains the $\langle \alpha, \beta \rangle$–minimal set V. Choose an idempotent polynomial f_1 of $\mathbf{A}$ such that $f_1(A) = V$. Since $\mathbf{C}$ is a subdirect power of $\mathbf{A}$, it is possible to choose a polynomial f of $\mathbf{C}$ which has f_1 as its first component. Now $ef(x)$ is a unary polynomial of $\mathbf{C}$ whose first component is $e_1 f_1(x) = f_1(x) \in \mathrm{Sep}(\alpha, \beta)$. It follows that all components of ef belong to $\mathrm{Sep}(\alpha, \beta)$, since they are simultaneous C–twins. Choose a good i and then pick $(\mathbf{a}, \mathbf{b}) \in \beta' - \alpha_i$. Since $(a_i, b_i) \in \beta - \alpha$ and $e_i f_i(\beta) \not\subseteq \alpha$, there exists a unary polynomial g_i of $\mathbf{A}$ such that $(e_i f_i g_i(a_i), e_i f_i g_i(b_i)) \in \beta - \alpha$. We can lift $g_i(x)$ to a unary polynomial $g(x)$ of $\mathbf{C}$ whose i–th component is g_i, since $\mathbf{C} \leq \mathbf{A}^k$

is subdirect. For this g we have

$$(efg(\mathbf{a}), efg(\mathbf{b})) \in \beta'|_U - \alpha_i \subseteq \rho'|_U - \alpha' = \rho'|_B - \alpha'.$$

It follows that $efg(C)$ contains an $\langle \alpha', \rho' \rangle$–minimal set. But $efg(C)$ is properly contained in the minimal set $e(C) = U$, since $e_1 f_1 g_1(A) \subseteq V \subset U_1$. This contradicts the minimality of $e(C) = U$. The conclusion is that each U_i is a member of $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$.

We now prove that $\alpha_i|_B < \beta_i|_B$ for each coordinate i. Select a coordinate j at random. Since $U_j \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, it follows from the definition of U_j that there exist $\mathbf{c}, \mathbf{d} \in U$ such that $(c_j, d_j) \in \beta|_{U_j} - \alpha$. This means that $(\mathbf{c}, \mathbf{d}) \in \beta_j|_U - \alpha_j$. In particular, it means that $\alpha_j|_U < \beta_j|_U$, and so U contains an $\langle \alpha_j, \beta_j \rangle$–minimal set. We claim that $U \in \mathrm{M}_{\mathbf{C}}(\alpha_j, \beta_j)$. To see this, choose an idempotent unary polynomial f such that

$$f(C) = ef(C) = V \subseteq U$$

and $V \in \mathrm{M}_{\mathbf{C}}(\alpha_j, \beta_j)$. Since $f = ef \in \mathrm{Sep}(\alpha_j, \beta_j)$, we must have $e_j f_j \in \mathrm{Sep}(\alpha, \beta)$. This implies that all coordinates of ef are in $\mathrm{Sep}(\alpha, \beta)$. Thus, each $e_i f_i(A)$ contains an $\langle \alpha, \beta \rangle$–minimal set and is at the same time contained in U_i. We conclude that $f_i(A) = e_i f_i(A) = U_i = e_i(A)$ for all i. Hence,

$$U = e(C) = C \cap (e_1(A) \times \cdots \times e_k(A)) = C \cap (f_1(A) \times \cdots \times f_k(A)) = f(C) = V.$$

This proves that $U \in \mathrm{M}_{\mathbf{C}}(\alpha_j, \beta_j)$. By Lemma 4.2 (1), the quotient $\langle \alpha_j, \beta_j \rangle$ is of type **2**. From Lemma 2.11 (7) we get that the $\langle \alpha_i, \beta_i \rangle$–body and tail of U are B and T, respectively; which implies that $\alpha_i|_B < \beta_i|_B$.

We now show that B_i and T_i are the body and tail of U_i, respectively. If c is in the body of U_i, then there is some element d also in the body with $(c, d) \in \beta - \alpha$. Since U_i is the projection of U onto its i–th component, there are elements $\mathbf{a}$ and $\mathbf{b} \in U$ with $a_i = c$ and $b_i = d$. Then $(\mathbf{a}, \mathbf{b}) \in \beta_i|_U - \alpha_i|_U$, and so both of these elements lie in B, the body of U. This shows that $a_i = c$ is in B_i.

For the converse, suppose that c is a member of B_i. Then there is some $\mathbf{a}$ in B with $a_i = c$. Being a member of B means that there is some $\mathbf{b}$ also in B with $(\mathbf{a}, \mathbf{b}) \in \beta_i - \alpha_i$. Then b_i belongs to U_i and $(a_i, b_i) \in \beta - \alpha$. This shows that $a_i = c$ is a member of the body of U_i.

We have shown that the body of U_i equals B_i. To prove that the tail of U_i is T_i, it will suffice to show that $\{B_i, T_i\}$ is a partition of U_i. The fact that $U_i = B_i \cup T_i$ follows from the way B_i and T_i were defined. Assume that $B_i \cap T_i \neq \emptyset$. Then we can find $\mathbf{b} \in B$ and $\mathbf{t} \in T$ such that $b_i = t_i$. This implies that $(\mathbf{b}, \mathbf{t}) \in B \times T$ and that

$$(\mathbf{b}, \mathbf{t}) \in \eta_i|_U \leq \gamma'|_U \leq (\delta : \theta)|_U,$$

where $\langle \delta, \theta \rangle$ is an arbitrarily chosen centralized quotient. But $U \in \mathrm{M}_{\mathbf{A}}(\delta, \theta)$, and therefore (by Lemma 2.11 (6)) B is a $(\delta : \theta)|_U$–class. Now the last displayed line implies that $\mathbf{b} \in B \Leftrightarrow \mathbf{t} \in B$. Thus, we cannot have $(\mathbf{b}, \mathbf{t}) \in B \times T$, after all. This completes the proof. □

One consequence of Lemma 4.9 is that $B = C \cap (B_1 \times \cdots \times B_k)$ and $T = C \cap (T_1 \times \cdots \times T_k)$. To see this, notice that $C \cap (B_1 \times \cdots \times B_k)$ and $C \cap (T_1 \times \cdots \times T_k)$ are disjoint, in the range of e, and that the first set contains B while the second contains T.

Now we prove the last part of Theorem 4.1.

Lemma 4.10. *Assume the hypotheses of Theorem 4.1.*

(6) *The elements of* $\mathcal{M}$ *are exactly the sets* $U = C \cap (e_1(A) \times \cdots \times e_k(A))$, *where* $(e_1, \dots, e_k)$ *is a sequence of simultaneous* C*–twins and each* e_i *is an idempotent polynomial of* $\mathbf{A}$ *with* $e_i(A) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. *The body and tail of* U *are of the form* $C \cap (B_1 \times \cdots \times B_k)$ *and* $C \cap (T_1 \times \cdots \times T_k)$, *respectively, where* B_i *and* T_i *are the* $\langle \alpha, \beta \rangle$*–body and tail of* $e_i(A)$.

Proof. The element $U \in \mathcal{M}$ which we fixed prior to Lemma 4.9 has the prescribed structure. Since U was chosen arbitrarily, all elements of $\mathcal{M}$ are of this form. Furthermore, as we remarked just before this lemma, the body and tail of U are as claimed. It remains to show is that if $(e_1, \dots, e_k)$ is a sequence of simultaneous C–twins and $e_i(A) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ for each i, then $C \cap (e_1(A) \times \cdots \times e_k(A)) \in \mathcal{M}$.

The function $e(x)$ is a unary polynomial of $\mathbf{C}$, since $(e_1, \dots, e_k)$ is a sequence of simultaneous C–twins. Furthermore, each e_i belongs to $\mathrm{Sep}(\alpha, \beta)$. This is enough to force $e \in \mathrm{Sep}(\alpha', \beta')$. To see this, choose $(\mathbf{a}, \mathbf{b}) \in \beta' - \alpha'$. Assume that, say, $(a_i, b_i) \in \beta - \alpha$. There is a unary polynomial g_i such that $(e_i g_i(a_i), e_i g_i(b_i)) \in \beta - \alpha$. Let g be a unary polynomial of $\mathbf{C}$ which has g_i as its i–th component. Then $(\mathbf{c}, \mathbf{d}) = (eg(\mathbf{a}), eg(\mathbf{b})) \in \beta' - \alpha'$. Since $(e(\mathbf{c}), e(\mathbf{d})) = (\mathbf{c}, \mathbf{d})$, we get $e \in \mathrm{Sep}(\alpha', \beta')$.

Let U be a member of $\mathcal{M}$ which is contained in $e(C)$. Let f be an idempotent unary polynomial of $\mathbf{C}$ for which $f(C) = U$. By the first part of this proof, $f_i(A) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ for all i. But $f_i(A) \subseteq e_i(A) = U_i \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ for all i, since $f(x) = ef(x)$. We must have $f_i(A) = e_i(A) = U_i$ for all i. Hence,

$$U = f(C) = C \cap (U_1 \times \cdots \times U_k) = e(C)$$

which proves that $e(C) \in \mathrm{M}_{\mathbf{C}}(\alpha', \rho')$. □

To conclude we summarize the results from this section for the case in which we are dealing with a finite simple abelian algebra. In this case, we obtain a precise description of all type **2** minimal sets in subpowers of $\mathbf{A}$.

Corollary 4.11. *Let* $\mathbf{A}$ *be a finite simple abelian algebra and let* $\mathbf{C}$ *be a finite subdirect power of* $\mathbf{A}$. *Let* $\mathcal{M}$ *be the collection of all subsets of* C *which are minimal with respect to at least one prime quotient of* $\mathbf{C}$ *of type* **2**. *Let* $\mathbf{K}$ *denote the finite field such that* $\mathbf{A}$ *induces a 1-dimensional* $\mathbf{K}$*-vector space structure on each of its minimal sets. The following hold:*

(1) $\mathcal{M}$ *is nonempty, and every member of* $\mathcal{M}$ *is minimal with respect to every prime quotient of* $\mathbf{C}$ *of type* **2**.
(2) *Each* U *in* $\mathcal{M}$ *has an empty tail with respect to every type* **2** *prime quotient, and* $\mathbf{C}|_U$ *is polynomially equivalent to a vector space over* $\mathbf{K}$.
(3) *If* $U \in \mathcal{M}$ *and* f *is a unary polynomial of* $\mathbf{C}$ *which is nonconstant on* U, *then* $f(U) \in \mathcal{M}$ *and* f *is a polynomial isomorphism of* U *onto* $f(U)$. *If* f *is an* n*-ary polynomial of* $\mathbf{C}$, *then* $f(U, \dots, U)$ *is a coordinatizable* E*–trace of* $\mathbf{C}$ *with respect to* U^l *for some* $l \leq n$.
(4) *The elements of* $\mathcal{M}$ *are exactly the sets* $U = C \cap (e_1(A) \times \cdots \times e_k(A))$, *where* $(e_1, \dots, e_k)$ *is a sequence of simultaneous* C*–twins and each* e_i *is an idempotent polynomial of* $\mathbf{A}$ *with* $e_i(A)$ *a minimal set of* $\mathbf{A}$.
(5) *If* ρ' *is the join of all of the atoms in* $\mathrm{Con}\,\mathbf{C}$, *then the interval* $I[0_C, \rho']$ *is tame of type* **2** *and the interval* $I[\rho', 1_C]$ *is strongly solvable.*

5. Minimal locally solvable varieties

A variety is called *minimal* (or *equationally complete*) if it is nontrivial, but its only proper subvariety is trivial. Every nontrivial variety contains a nontrivial simple algebra, so every minimal variety is generated by a simple algebra. A minimal locally finite variety is generated by a strictly simple algebra. We recommend [18] to the reader interested in a survey of strictly simple algebras and minimal locally finite varieties.

If a strictly simple generator of a minimal variety is nonabelian, then every member of the variety is nonabelian; in fact, nonsolvable. If the generator is abelian, every member of the variety is guaranteed to be locally solvable. Thus, minimal locally finite varieties either are locally solvable or contain no solvable algebras. In this section we describe all minimal, locally finite, locally solvable varieties. Here is our result.

Theorem 5.1. *Let $\mathcal{V}$ be a locally finite, locally solvable variety. Then $\mathcal{V}$ is minimal if and only if one of the following possibilities holds.*

(1) *$\mathcal{V}$ is term equivalent to a matrix power of the variety of sets with no operations, or to the variety of sets with one constant operation. In this case $\mathcal{V}$ is strongly abelian.*
(2) *$\mathcal{V}$ is affine (in particular, it is congruence permutable), and is generated by a finite, simple algebra that is polynomially equivalent to a module over a finite ring, and has a 1–element subalgebra.*

The structure of the varieties described in (2) is well–known (see Freese and McKenzie [3], Theorem 12.4), and it is proved there that such varieties are indeed minimal (all subdirectly irreducible algebras are isomorphic to the generator). In view of Theorem 3.4 (6), the varieties given in (1) are also minimal, since the variety of sets and the variety of pointed sets are obviously minimal. By the same theorem, the statement in (1) is equivalent to saying that $\mathcal{V}$ is generated by a finite simple algebra that is term equivalent to a matrix power of the 2–element set or of the 2–element pointed set.

As promised in the Introduction, we give three different proofs of case (2) in this paper (and one proof of case (1)). Still more proofs of Theorem 5.1 are known. For instance, Ágnes Szendrei discovered a different proof independently and at about the same time that we discovered ours. Her results appear in [19] and [16] for the type **1** and type **2** cases, respectively. Three years later, Szendrei and the first author discovered two more proofs of this theorem. (One proof and the outline of the second can be found in [9].) The reader will find one proof of the type **2** case in the next section, two in this one. The difference between the two arguments here is that one uses the theory of minimal sets in subdirect powers, the other one does not. This difference occurs only in the proof of the following key lemma (which also applies in the type **1** case, but we only have one proof of that).

Lemma 5.2. *Let $\mathbf{A}$ be a finite, simple, abelian algebra generating a minimal variety $\mathcal{V}$. Then for each nonconstant, idempotent polynomial e of $\mathbf{A}$ there exist a binary polynomial $s(x, y)$ of $\mathbf{A}$ and a trace $N \subseteq T = e(A)$ of $\mathbf{A}$ satisfying the following conditions.*

(*i*) $s(A, A) \subseteq T$.
(*ii*) $s(N, T) = T$.
(*iii*) $|s(t, T)| < |T|$ *for a suitable (that is, all)* $t \in T$.

Proof. First we explain statement *(iii)* of the lemma. Suppose that $|s(t,T)| < |T|$ for a suitable $t \in T$. Then the mapping $x \mapsto s(t,x)$ is not a bijection on T, so we have $s(t,t_1) = s(t,t_2)$ for some $t_1, t_2 \in T$. As $\mathbf{A}$ satisfies the term condition, we have $s(t',t_1) = s(t',t_2)$ for every $t' \in T$. As T is finite, this indeed implies $|s(t',T)| < |T|$.

Our first argument works only for the case when $\mathrm{typ}\{\mathbf{A}\} = \{\mathbf{2}\}$. We shall use the theory of minimal sets in subdirect powers. Consider a listing $\mathbf{t} = (t_1, \dots, t_k)$ of the elements of T, and let $\mathbf{C}$ be the subalgebra of A^k generated by the diagonal and the element $\mathbf{t}$. As $\mathbf{A}$ is simple and abelian, Corollary 4.11 applies for $\mathbf{A}$ and $\mathbf{C}$. From Corollary 4.11 (5) we know that if ρ' is the join of all of the atoms in $\mathrm{Con}\,\mathbf{C}$, then the interval $I[\rho', 1_C]$ is strongly solvable and the interval $I[0_C, \rho']$ is tame of type $\mathbf{2}$. It follows that $\mathbf{C}/\rho'$ is strongly solvable. But the locally strongly solvable algebras of $\mathcal{V}$ form a subvariety $\mathcal{W}$ by Corollary 7.6 of [6]. $\mathbf{A}$ is not in $\mathcal{W}$, since its type is $\mathbf{2}$, and so $\mathcal{W}$ must be trivial. Therefore $\mathbf{C}/\rho'$ is the trivial algebra, and we must have $\rho' = 1_{\mathbf{C}}$. We conclude that the algebra $\mathbf{C}$ is tame of type $\mathbf{2}$. In particular, any two elements of $\mathbf{C}$ are connected by a chain of minimal sets. The collection of these minimal sets is called $\mathcal{M}$ in Section 4, and their structure is described in Corollary 4.11 (4).

For $c \in A$, let $\hat{c}$ denote the element $(c, \dots, c)$ of C. Fix some element t from T. Since $|T| > 1$, $\mathbf{t}$ and $\hat{t}$ are two different elements. Connect $\mathbf{t}$ to $\hat{t}$ with a chain of members of $\mathcal{M}$. Let $\hat{e}$ denote the (idempotent) unary polynomial of $\mathbf{C}$ that acts as e in every component. Apply $\hat{e}$ to the elements of this chain. Since every element of the chain is a minimal set of the tame algebra $\mathbf{C}$, then on any given element of the chain, either e is constant or it maps that element onto another member of $\mathcal{M}$. We get another chain of elements of $\mathcal{M}$ running entirely in T^k which connects $\hat{e}(\mathbf{t}) = \mathbf{t}$ to $\hat{e}(\hat{t}) = \hat{t}$. In particular, there exists a $V \in \mathcal{M}$ such that $\mathbf{t} \in V \subseteq T^k$.

Since V is a minimal set, we obtain that there exists an idempotent unary polynomial f of $\mathbf{C}$ satisfying $f(C) = V$. Since $\mathbf{C}$ is generated by the diagonal and the element $\mathbf{t}$, we may express f as

$$f(x) = g^{\mathbf{C}}(x, \mathbf{t}, \hat{c}_1, \dots, \hat{c}_m)$$

for some term g and elements c_i from A. Let $s(x,y) = eg^{\mathbf{A}}(x, y, c_1, \dots, c_m)$. Clearly, s is a binary polynomial of $\mathbf{A}$. The construction of s ensures that for every $\mathbf{x} \in C$ we have

$$f_i(x_i) = s(x_i, t_i)\,,$$

where f_i is the i–th component function of f. As f is idempotent and $\mathbf{C}$ contains the diagonal, we have $s(s(x,t_i),t_i) = s(x,t_i)$ for each $x \in A$. From the abelian property of $\mathbf{A}$ we get that $s(s(x,t_i),z) = s(x,z)$ holds for all $z, t_i \in T$.

Corollary 4.11 (4) states that we have $\hat{e}(C) \supseteq V = C \cap (N_1 \times \cdots \times N_k)$ for some minimal sets $N_i \subseteq e(A) = T$ of $\mathbf{A}$. We show that s satisfies the conditions of the lemma with $N = N_1$. Condition (i) holds, since g is prefixed by e in the definition of s. From $f(C) = V$ and $\mathbf{t} \in V$ we see that $t_i \in N_i = s(A, t_i)$. By the equality above,

$$s(N_1, t_j) = s(s(A, t_1), t_j) = s(A, t_j) = N_j$$

for every $1 \leq i, j \leq k$. In particular, $s(N_1, T) = T$, implying (ii). To prove (iii), assume that $s(t,T) = T$ for some $t \in T$. Then

$$N_1 = s(N_1, t_1) \subseteq s(T, t_1) = s(s(t,T), t_1) = \{s(t, t_1)\},$$

which is our final contradiction.

This was the proof of the lemma for the type **2** case using the theory of minimal sets in subdirect powers. We included this argument to demonstrate the usefulness of this theory. Now we present our "elementary" proof. Note that in the above argument we used only that the locally strongly solvable subvariety of $\mathcal{V}$ is trivial. Here we shall use the minimality of $\mathcal{V}$ in a different way. We do not distinguish between type **1** and type **2** until the end of the argument.

First note that $T = e(A)$ contains a trace N of $\mathbf{A}$. Indeed, e is not constant, and therefore its range contains a minimal set, that is, a trace.

Let $N = p(A)$, where $p(x) = r^{\mathbf{A}}(x, d_1, \dots, d_\ell)$ is an idempotent polynomial and r is a term of $\mathbf{A}$. Then $\mathbf{A}$ does not satisfy the identity $r(x, z_1, \dots, z_\ell) = r(y, z_1, \dots, z_\ell)$, since we can choose $x, y \in N$ to be different, and $z_i = d_i$. Hence, the subvariety of $\mathcal{V}$ defined by this identity is trivial. Now, assume that $C \in \mathcal{V}$ is any finite algebra, having a congruence $\theta \neq 1_{\mathbf{C}}$, and elements $s_1, \dots, s_\ell$ such that $r^{\mathbf{C}}(x, s_1, \dots, s_\ell)\ \theta\ r^{\mathbf{C}}(y, s_1, \dots, s_\ell)$ for all $x, y \in C$. Taking a maximal congruence ψ of $\mathbf{C}$ containing θ, the simple algebra $\mathbf{S} = \mathbf{C}/\psi$ is abelian and satisfies

$$\forall x, y(r^{\mathbf{S}}(x, \bar{s}_1, \dots, \bar{s}_\ell) = r^{\mathbf{S}}(y, \bar{s}_1, \dots, \bar{s}_\ell)).$$

Using the term condition, we get that $\mathbf{S}$ is a nontrivial algebra satisfying the equation $r(x, z_1, \dots, z_\ell) = r(y, z_1, \dots, z_\ell)$. This is impossible, since this equation together with the equations of $\mathcal{V}$ defines the trivial variety. We conclude that there is no finite $C \in \mathcal{V}$ having a congruence $\theta \neq 1_{\mathbf{C}}$, and elements $s_1, \dots, s_\ell$ such that $r^{\mathbf{C}}(x, s_1, \dots, s_\ell)\ \theta\ r^{\mathbf{C}}(y, s_1, \dots, s_\ell)$ for all $x, y \in C$.

Again let $\mathbf{t} = (t_1, \dots, t_k)$ be a listing of the elements of T, and $\mathbf{C}$ the subalgebra of A^k generated by the diagonal and the element $\mathbf{t}$. Let $U = N^k \cap C$, and denote by θ the smallest congruence of $\mathbf{C}$ collapsing U. Since $p(x) = r^{\mathbf{A}}(x, d_1, \dots, d_\ell)$ and $p(A) = N$, then we have $r^{\mathbf{C}}(x, \hat{d}_1, \dots, \hat{d}_\ell)\ \theta\ r^{\mathbf{C}}(y, \hat{d}_1, \dots, \hat{d}_\ell)$ for all $x, y \in C$. By the remarks in the previous paragraph, the minimality of $\mathcal{V}$ implies that $\theta = 1_{\mathbf{C}}$. Thus, the images of U under the unary polynomials of $\mathbf{C}$ connect the elements of C.

Notice that we had a similar statement in the previous proof. We now have it for type **1** as well. The next few steps of the proof are the same as above, but we now know less about the polynomial images of U (in particular, we do not know if they can be obtained as the range of an idempotent polynomial), so we have to do more calculations.

Connect the element $\mathbf{t}$ to $\hat{t} = (t, \dots, t)$, where t is some fixed element of T, with a chain of polynomial images of U. These are two different elements, since $|T| > 1$. Let $\hat{e}$ denote the (idempotent) unary polynomial of $\mathbf{C}$ that acts as e in every component. Apply $\hat{e}$ to the elements of this chain. We get another chain of polynomial images of U contained entirely in T^k. In particular, there exists a unary polynomial f of $\mathbf{C}$ such that $V = f(U)$ has at least two elements and satisfies $\mathbf{t} \in V \subseteq T^k$.

Since $\mathbf{C}$ is generated by the diagonal and the element $\mathbf{t}$, we may express f as

$$f(x) = g^{\mathbf{C}}(x, \mathbf{t}, \hat{a}_1, \dots, \hat{a}_m)$$

for some term g and elements a_i from A. Let $s(x, y) = eg^{\mathbf{A}}(x, y, a_1, \dots, a_m)$. Clearly, s is a binary polynomial of $\mathbf{A}$. The construction of s ensures that for every $\mathbf{x} \in C$ we have

$$f_i(x_i) = s(x_i, t_i)\,,$$

where f_i is the i–th component function of f.

We have an element $\mathbf{u} \in U$ such that $f(\mathbf{u}) = \mathbf{t}$, that is, $s(u_i, t_i) = t_i$ for every $1 \leq i \leq k$. Since $u_i \in N$, this implies that $t \in s(N, t)$ for every $t \in T$; hence $s(N, T) \supseteq T$. On the other hand, g is prefixed by e in the definition of s, so we have $s(A, A) \subseteq T$. Thus s satisfies (i) and (ii).

Now we have to split the proof into two cases according to the type of $\mathbf{A}$. First suppose that this type is **1**. As f is not constant on U, there exist elements $n_1, n_2 \in N$ and $x \in T$ such that $s(n_1, x) \neq s(n_2, x)$. But $\mathbf{A}$ is strongly abelian, so this implies that $s(n_1, x) \neq s(n_2, y)$ for every $y \in T$. That is, $s(n_1, T)$ is contained in $T - s(n_2, T)$, and therefore we have condition (iii) with $t = n_2$.

In the type **2** case we transform s in three steps to get a new binary polynomial that still satisfies conditions (i) and (ii), but satisfies (iii) as well. As f is not constant on U, there exist elements $n_1, n_2 \in N$ and $0 \in T$ such that $s(n_1, 0) \neq s(n_2, 0)$. Hence, $M = s(N, 0)$ is a trace of $\mathbf{A}$, which contains 0 (since $t \in s(N, t)$ for every $t \in T$). Let q be a polynomial inverse of $s(x, 0)$ mapping M to N and satisfying $q(A) = q(M) = N$. Set

$$s_1(x, y) = s(q(x), y)\,.$$

Then $s_1(x, 0) = x$ for all $x \in M$, so $s_1(M, 0) = s_1(A, 0) = M$. We also have $t \in s_1(M, t)$ for every $t \in T$. Thus, s_1 satisfies conditions (i) and (ii) with respect to M instead of N. Thus, if $s_1(0, y)$ is not a permutation of T, then we are done because (iii) will be satisfied with $t = 0$. Otherwise, consider a power $h(y)$ of this permutation, which is its inverse on the set T. Set

$$s_2(x, y) = s_1(x, h(y))\,.$$

By the definition of h we have $s_2(0, y) = y$ for all $y \in T$. As h is a permutation of T, it maps T onto T, so $s_2(M, T) = s_1(M, h(T)) = s_1(M, T) = T$. From $0 \in M$ we get that $s_1(0, 0) = 0$, so the element 0 is a fixed point of $s_1(0, y)$; hence $h(0) = 0$. Therefore $s_2(x, 0) = x$ holds for all $x \in M$, and we have $s_2(A, 0) = s_2(M, 0) = M$.

Let $+$ denote the (polynomial) addition on M with zero element 0. We show that for each $x, y \in M$ we have $s_2(x, y) = x + y$. (This follows easily from the fact that $\mathbf{A}$ is quasi–affine, but the following argument is simpler and more elementary.) We apply the term condition. From

$$s_2(0 + 0, y) = y = s_2(0 + y, 0)$$

we obtain, by changing the first zero to x, that

$$s_2(x + 0, y) = s_2(x + y, 0) = x + y\,,$$

since $x + y \in M$.

Finally, let $e_0(x) = s_2(x, 0)$; this is an idempotent polynomial of $\mathbf{A}$ with range M. Set

$$s_3(x, y) = s_2(e_0(x) - e_0(y), y)\,.$$

We show that s_3 satisfies all three conditions. Obviously, $s_3(A, A) \subseteq T$. If $t \in T$, then $t = s_2(m, t')$ for some $m \in M$ and $t' \in T$. Let $m' = e_0(t') + m$; then $s_3(m', t') = s_2(e_0(t') + m - e_0(t'), t') = s_2(m, t') = t$, so we have $s_3(M, T) = T$. Finally if $x, y \in M$, then we have $s_3(x, y) = s_2(x - y, y) = (x - y) + y = x$, showing that $s_3(0, M) = \{0\}$. Therefore $s_3(0, x)$ is not a permutation of T and so $s_3(0, T) \neq T$, as T is finite. Thus, all proofs of Lemma 5.2 are complete. □

Lemma 5.3. *Let* $\mathbf{A}$ *be a finite, simple, abelian algebra generating a minimal variety* $\mathcal{V}$*. Then* $\mathbf{A}$ *is coordinatizable by traces.*

Proof. Let T be minimal among all E–traces of $\mathbf{A}$ that are not coordinatizable by traces, and let $T = e(A)$ for an idempotent polynomial e of $\mathbf{A}$. Consider the trace N and binary polynomial s provided by Lemma 5.2 for this T. Iterate s in its second variable so that it becomes idempotent. If this happens in m steps, then let

$$g(x_1, \dots, x_m, y) = s(x_1, s(x_2, \dots s(x_m, y) \dots)),$$

and $h(x, y) = g(x, \dots, x, y)$. Pick $t \in T$ arbitrarily. Then $f(x) = h(t, x)$ is an idempotent polynomial of $\mathbf{A}$. Let $R = f(A)$. As $s(A, A) \subseteq T$, we have $R \subseteq T$. As $s(t, T)$ is a proper subset of T, by the properties of s, the definitions of g and h show that R is a proper subset of T. On the other hand, $s(N, T) = T$ implies that $g(N, \dots, N, T) = T$.

We show that $g(N, \dots, N, R) = T$. Indeed, from $h(x, h(x, y)) = h(x, y)$ we get that

$$g(x, \dots, x, g(x, \dots, x, y)) = g(x, \dots, x, y),$$

so by applying the term condition we obtain that

$$g(x_1, \dots, x_m, g(x, \dots, x, y)) = g(x_1, \dots, x_m, y).$$

Thus $g(N, \dots, N, T) = g(N, \dots, N, h(t, T))$ as stated.

By the minimality of T we know that R is coordinatizable by traces. This means that $R = p(M, \dots, M)$ for some polynomial p and trace M of $\mathbf{A}$. As M and N are polynomially isomorphic, we may assume that $M = N$ (by changing p appropriately). Hence $T = g(N, \dots, N, p(N, \dots, N))$, so by Lemmas 3.8 and 3.9, the set T is coordinatizable by traces. This contradiction proves the lemma. □

Finally we show that Theorem 5.1 follows from this lemma.

Proof of Theorem 5.1. Let $\mathcal{V}$ be a locally finite, locally solvable, minimal variety. Then $\mathcal{V}$ is generated by a finite simple solvable (and hence abelian) algebra $\mathbf{A}$. If we put together Lemma 5.3 and Theorem 3.7 (2), we find that $\mathbf{A}|_A$ is term equivalent to $(\mathbf{U}|_U)^{[k]}$, where $\mathbf{U}$ is either a finite simple vector space or a finite simple algebra whose basic operations are all unary and permutations of U, and k is some natural number. Thus, we can assume that $\mathbf{A}$ is polynomially equivalent to $\mathbf{U}^{[k]}$. This means that the universe of A will be assumed to be U^k, and it further entails that the clone of $\mathbf{A}$ is contained in the clone of $(\mathbf{U}|_U)^{[k]}$.

In the case where $\mathbf{U}$ is a vector space we have that $\mathbf{A}$ is an abelian algebra which has a Mal'cev polynomial. This says that $\mathbf{A}$ is polynomially equivalent to an affine algebra. But an algebra polynomially equivalent to an affine algebra is affine itself as we now explain. Let $p(x, y, z)$ be a polynomial of $\mathbf{A}$ that interprets as $x - y + z$. If $p(x, y, z) = t^{\mathbf{A}}(x, y, z, a_1, \dots, a_k)$ for some term t, then in fact

$$p(x, y, z) = t^{\mathbf{A}}(x, t^{\mathbf{A}}(y, y, y, y, \dots, y), z, y, \dots, y).$$

That is, the term $t(x, t(y, y, y, y, \dots, y), z, y, \dots, y)$ interprets as $x - y + z$. One can see this most easily by first representing $t(x, y, z, \bar{u})$ as a module polynomial for which $t^{\mathbf{A}}(x, y, z, \bar{a}) = x - y + z$ and then showing that the operation $t^{\mathbf{A}}(x, t^{\mathbf{A}}(y, y, y, \bar{u}), z, \bar{u})$ is independent of $\bar{u}$. Now that we see that $\mathbf{A}$ is affine, we can rely on Theorem 12.4 of [3] to obtain part (2) of our theorem.

In the case where $\mathbf{U}$ is unary it follows from the definition of the matrix power of an algebra that all term operations of $\mathbf{U}^{[k]}$ (and hence of $\mathbf{A}$) depend on at most k variables. This implies that any polynomial of $\mathbf{A}$ which depends on exactly k variables must in fact be a term operation of $\mathbf{A}$. In particular, since the clone

of $\mathbf{U}^{[k]}$ can be generated by k–ary operations which depend on all of their variables, it follows that the clone of $\mathbf{A}$ contains the clone of $\mathbf{U}^{[k]}$. (Here it is essential that the basic operations of $\mathbf{U}$ are permutations.)

If the unary term operations of $\mathbf{U}$ act transitively on U, then the unary term operations of $\mathbf{U}^{[k]}$ will act transitively on U^k. In this case, the clone of $(\mathbf{U}|_U)^{[k]}$ covers the clone of $\mathbf{U}^{[k]}$ in the lattice of clones on U^k. The clone of $\mathbf{A}$ must equal one or the other of these clones, since it contains one clone and is contained in the other. Thus, when the terms of $\mathbf{U}$ act transitively, then $\mathbf{A}$ is term equivalent to either $\mathbf{U}^{[k]}$ or $(\mathbf{U}|_U)^{[k]}$.

The algebras $\mathbf{U}$ and $\mathbf{U}|_U$ do not generate minimal varieties when the unary term operations of $\mathbf{U}$ act transitively on U (the subvariety defined by the equations $t(x) \approx x$ for all nonconstant unary terms t is nontrivial); hence their matrix powers cannot either. Thus, in this case, $\mathbf{A}$ can't generate a minimal variety, since term equivalence preserves this property.

We are reduced to considering the case where $\mathbf{U}$ is a 2–element algebra with no basic operations and the clone of $\mathbf{A}$ contains the clone of $\mathbf{U}^{[k]}$ but is contained in the clone of $(\mathbf{U}|_U)^{[k]}$. However, there are only four clones on the set U^k which contain the clone of $\mathbf{U}^{[k]}$ and are contained in the clone of $(\mathbf{U}|_U)^{[k]}$. If we let $U = \{0, 1\}$, then the four clones are the clones of

- $\langle \{0, 1\}; \emptyset \rangle^{[k]}$,
- $\langle \{0, 1\}; 0 \rangle^{[k]}$,
- $\langle \{0, 1\}; 1 \rangle^{[k]}$, and
- $\langle \{0, 1\}; 0, 1 \rangle^{[k]}$.

(It takes a small calculation to see that there are no other clones in this interval.) $\mathbf{A}$ is term equivalent to one of these four algebras. The second and third are term equivalent to each other. The fourth algebra on the list does not generate a minimal variety (since the equation $\bar{0} \approx \bar{1}$ defines a nontrivial proper subvariety). Hence, $\mathbf{A}$ must be term equivalent to either $\langle \{0, 1\}; \emptyset \rangle^{[k]}$ or $\langle \{0, 1\}; 0 \rangle^{[k]}$.

To summarize, we have shown that the algebra $\mathbf{A}$ either must generate an affine variety or must be term equivalent to a matrix power of a 2–element set or to a matrix power of a 2–element set with a single constant operation. □

To conclude this section, we give a more detailed description of the minimal locally finite varieties of type **2**. We have shown that a minimal locally finite variety of type **2** is affine and has a 1–element subalgebra. This is already a good description of minimal varieties of type **2**, but it is not as good a description as the one we have given for minimal varieties of type **1**. In particular, Theorem 5.1 does not tell us what the clone of a minimal type **2** variety is.

Let $\mathbf{A}$ be a strictly simple algebra which generates a minimal variety of type **2**. Let S denote the set of trivial subalgebras of $\mathbf{A}$, and choose some $0 \in S$. If we expand $\mathbf{A}$ by adding in all polynomials which preserve 0 as new basic operations, we obtain an affine algebra with exactly one trivial subalgebra. Such an algebra is term equivalent to a finite simple module, $\mathbf{B}$, with the same universe as $\mathbf{A}$. The endomorphism ring $\mathrm{End}(\mathbf{B})$ is a finite field which we denote by $\mathbf{F}$. If V is the universe of $\mathbf{B}$, then V is a finite–dimensional $\mathbf{F}$–space and $\mathbf{B}$ is isomorphic to the $\mathbf{R}$–module structure on V where $\mathbf{R} = \mathrm{End}_{\mathbf{F}}(V)$. The algebras $\mathbf{A}$ and $\mathbf{B}$ are polynomially equivalent, so the following theorem serves to describe the clone of $\mathbf{A}$. The proof of this theorem can be derived from Propositions 2.6 and 2.10 from [17].

Theorem 5.4. *Let V be a finite–dimensional vector space over the field $\mathbf{F}$ and let $\mathbf{B}$ equal V considered as an $\mathbf{R}$–module, where $\mathbf{R} = \mathrm{End}_{\mathbf{F}}(V)$. Let $\mathbf{A}$ be any reduct of $\mathbf{B}$ which is polynomially equivalent to $\mathbf{B}$. Let S be the set of trivial subalgebras of $\mathbf{A}$. The following are true.*

1. *S is a subspace of V.*
2. *The clone of $\mathbf{A}$ consists precisely of those linear operations on V which preserve the members of S.*
3. *There is a left ideal J of $\mathbf{R}$ such that the clone of $\mathbf{A}$ consists precisely of those linear operations $m_1(x_1) + \cdots + m_r(x_r)$ on V which satisfy*

$$m_1 + \cdots + m_r \ \equiv \ 1 \ (\mathrm{mod} J).$$

(Here 1 denotes the identity element of $\mathbf{R}$.)

By a *reduct* of an algebra $\mathbf{C}$ we mean any algebra with universe C whose clone of term operations is a subset of the clone of term operations of $\mathbf{C}$. In the following corollary an *affine module* is an idempotent reduct of a module.

Corollary 5.5. *A minimal, locally finite affine variety is categorically equivalent to a variety of vector spaces or a variety of affine modules.*

Proof. A unary term $\sigma(x)$ for the variety $\mathcal{V}$ is said to be *invertible* in $\mathcal{V}$ if there exist some $n > 0$, an n–ary term $p(\bar{x})$ and n unary terms $q_1, \ldots, q_n$ such that $\mathcal{V}$ satisfies $p(\sigma(q_1(x)), \ldots, \sigma(q_n(x))) = x$. If σ is an idempotent term of $\mathcal{V}$, then for $\mathbf{A} \in \mathcal{V}$ we write $\mathbf{A}(\sigma)$ for the algebra with universe $\sigma(A)$ and whose basic operations are the operations of the form $\sigma \circ f|_{\sigma(A)}$, where f is a term of $\mathbf{A}$. We write $\mathcal{V}(\sigma)$ for the variety of algebras $\{\mathbf{A}(\sigma) | \mathbf{A} \in \mathcal{V}\}$. It is shown in [12] that if σ is an idempotent term which is invertible in $\mathcal{V}$, then $\mathcal{V}$ is categorically equivalent to $\mathcal{V}(\sigma)$.

If $\mathcal{V}$ is a minimal, locally finite affine variety, then using Theorem 5.4 it is fairly easy to show that any nonconstant idempotent term is invertible. Just follow these steps:

- (*i*) Let $\mathbf{A}$ be a strictly simple generator of $\mathcal{V}$ and choose $q_1, \ldots, q_m \in \mathrm{Clo}_1(\mathbf{A})$ such that $\{\sigma q_1, \ldots, \sigma q_m\}$ separates the points of A.
- (*ii*) Show that the left ideal of $\mathbf{R}$ generated by $\{\sigma q_1, \ldots, \sigma q_m\}$ is $\mathbf{R}$. In this step use the fact, which we established in the proof of Theorem 5.4, that left ideals of $\mathbf{R}$ are just the annihilators of subspaces of V.
- (*iii*) If $1 = \sum m_i \sigma q_i$, then $p(\bar{x}) = \sum m_i(x_i) \in \mathrm{Clo}_m(\mathbf{A})$ by Theorem 5.4 (3), and so p and $q_1, \ldots, q_m$ are terms which witness that σ is invertible.

Now if $\mathbf{A}$, the strictly simple generator of $\mathcal{V}$, has more than one trivial subalgebra, then the description of the clone of $\mathbf{A}$ given in Theorem 5.4 implies that $\mathbf{A}$ has a nonconstant idempotent term whose range is the space of trivial subalgebras. If σ is such a term, then $\mathcal{V}(\sigma)$ is an idempotent affine variety. That is, it is term equivalent to a variety of affine modules. Since term equivalence is a categorical equivalence, we get that $\mathcal{V}$ is categorically equivalent to a variety of affine modules in this case. In the other case $\mathbf{A}$ has exactly one trivial subalgebra. We choose σ to be any idempotent, invertible term whose range has vector space dimension 1. The term operations of $\mathbf{A}(\sigma)$ contain the vector space operations and are all linear with respect to these operations. Hence, $\mathbf{A}(\sigma)$ is term equivalent to a 1–dimensional vector space. But $\mathbf{A}(\sigma)$ generates $\mathcal{V}(\sigma)$, so the latter is term equivalent to a variety of vector spaces. This finishes the argument. □

Since the matrix power construction, viewed as a functor $\mathcal{V} \mapsto \mathcal{V}^{[k]}$, is a categorical equivalence, the results of this section show that any minimal, locally finite, locally solvable variety is categorically equivalent to one of the following varieties:

- the variety of sets,
- the variety of pointed sets,
- a variety of vector spaces, or
- a variety of affine modules over a finite simple ring.

No two varieties on the list are categorically equivalent to each other; they can be categorically distinguished by comparing the endomorphism monoids of $\mathbf{A}^2$, where $\mathbf{A}$ is the unique simple algebra in each variety.

We would like to point out that from the results of this section it is not hard to see that every locally finite minimal abelian variety is ω-categorical. A class of algebras is *ω-categorical* if up to isomorphism there is a single countably infinite algebra in the class. What is perhaps more interesting is that our results can be used to provide another proof of the classification of ω-categorical varieties [4, 5, 8, 14, 15], since it is not difficult to show that such a variety must be locally finite, abelian and minimal (see Theorem 4.1 of [8]).

6. TSSS varieties

We will call a locally finite variety with trivial locally strongly solvable subvariety a *TSSS variety*. Examples of TSSS varieties include all locally finite varieties which satisfy a nontrivial special Mal'cev condition, as well as all minimal locally finite varieties which are not of type **1**. We are going to analyze the commutator properties of algebras in TSSS varieties. We give a short argument which establishes that a TSSS variety generated by an abelian algebra is congruence permutable. This is a quick proof of the fact that a minimal variety of type **2** is affine. We further show that a TSSS variety generated by a left nilpotent algebra is congruence permutable.

Lemma 6.1. *Let $\mathcal{V}$ be a locally finite variety. The following conditions are equivalent.*

(*i*) *$\mathcal{V}$ is a TSSS variety.*
(*ii*) *$\mathcal{V}$ contains no finite simple algebra of type* **1**.
(*iii*) *Whenever $\mathbf{A} \in \mathcal{V}$ is finite, $\alpha \prec \beta$ in $\mathbf{Con}(\mathbf{A})$ and $\operatorname{typ}(\alpha, \beta) = \mathbf{1}$, then $\neg C(1, \beta; \alpha)$.*

Proof. We shall prove that $\neg(i) \Longrightarrow \neg(ii) \Longrightarrow \neg(iii) \Longrightarrow \neg(i)$. If $\mathcal{V}$ is not a TSSS variety, then it has a nontrivial locally strongly solvable subvariety which contains a finite simple algebra of type **1**. Hence, $\neg(i) \Longrightarrow \neg(ii)$. Next, if $\mathcal{V}$ contains a finite simple algebra $\mathbf{S}$ of type **1**, then by choosing $\mathbf{A} = \mathbf{S}$ and setting $\alpha = 0$ and $\beta = 1$ we get that $C(1, \beta; \alpha)$ since $\mathbf{S}$ is abelian. Hence, $\neg(ii) \Longrightarrow \neg(iii)$. To finish, we need to show that if $\mathcal{V}$ contains a finite algebra $\mathbf{A}$ with congruences $\alpha \prec \beta$ in $\mathbf{Con}(\mathbf{A})$ such that $\operatorname{typ}(\alpha, \beta) = \mathbf{1}$ and $C(1, \beta; \alpha)$, then $\mathcal{V}$ contains a nontrivial strongly solvable algebra. Without loss of generality we may assume that $\alpha = 0$.

Let $\overline{\beta}$ be the congruence $\beta \times \beta$ restricted to the subalgebra $\mathbf{A}(\beta)$ of $\mathbf{A} \times \mathbf{A}$ (as in Definition 2.2). Clearly, $\overline{\beta}$ is strongly abelian, so we have $\overline{\beta} \overset{ss}{\sim} 0$. It is easy to check that $\overline{\beta} \vee \Delta_{1,\beta} = 1$. Hence

$$1 = \overline{\beta} \vee \Delta_{1,\beta} \overset{ss}{\sim} 0 \vee \Delta_{1,\beta} = \Delta_{1,\beta}.$$

Therefore, $\mathbf{B} = \mathbf{A}(\beta)/\Delta_{1,\beta}$ is a strongly solvable member of $\mathcal{V}$. To finish our proof that $\mathcal{V}$ is not a TSSS variety, we will show that $\mathbf{B}$ is not a 1–element algebra. (This will show that $\mathcal{V}$ contains a nontrivial strongly solvable member.) To see this, note that our hypothesis $C(1, \beta; 0)$ is equivalent to $[1, \beta] = 0$, which in turn is equivalent to the condition that the diagonal of $\mathbf{A}(\beta)$ is a union of $\Delta_{1,\beta}$–classes. But not every element of $\mathbf{A}(\beta)$ is on the diagonal, since $\beta > 0$. It follows that $\Delta_{1,\beta}$ has at least one class contained in the diagonal of $\mathbf{A}(\beta)$ and at least one class disjoint from the diagonal of $\mathbf{A}(\beta)$. Hence, $\mathbf{B} = \mathbf{A}(\beta)/\Delta_{1,\beta}$ has at least 2 elements. □

Theorem 6.2. *If $\mathcal{V}$ is a TSSS variety generated by an abelian algebra, then $\mathcal{V}$ is affine.*

Proof. Since $\mathcal{V}$ is generated by an abelian algebra, then we know from [6] that $\mathcal{V}$ is locally solvable, or equivalently, that $\mathrm{typ}\{\mathcal{V}\} \subseteq \{\mathbf{1}, \mathbf{2}\}$. Corollary 2.7 tells us that in fact every finite member of $\mathcal{V}$ is left nilpotent. Now, if $\mathbf{1} \in \mathrm{typ}\{\mathcal{V}\}$, then $\mathcal{V}$ contains a finite subdirectly irreducible algebra $\mathbf{A}$ with monolith μ, where $\mathrm{typ}(0, \mu) = \mathbf{1}$. As $\mathbf{A}$ is left nilpotent, $[1, \mu] = 0$; that is, $C(1, \mu; 0)$. But now the equivalence $(i) \iff (iii)$ of Lemma 6.1 proves that $\mathcal{V}$ is not TSSS. Hence $\mathbf{1} \notin \mathrm{typ}\{\mathcal{V}\}$. The conclusion is that $\mathrm{typ}\{\mathcal{V}\} = \{\mathbf{2}\}$, and therefore that $\mathcal{V}$ is congruence permutable by Theorem 7.11 (3) of [6]. Any congruence permutable variety generated by an abelian algebra is affine, and so the theorem is proved. □

Corollary 6.3. *Every minimal variety of type* $\mathbf{2}$ *is affine.*

The following lemma generalizes the result, found in [7], that every homomorphic image of a finite abelian algebra is left nilpotent. (To see that it generalizes the result in [7], take $\alpha = 1$ and $\beta = 0$.)

Lemma 6.4. *If* $\mathbf{A}$ *is a finite algebra with congruences α, β, then*

$$[\alpha, \alpha] \leq \beta \Longrightarrow C(\alpha \vee \beta, \theta; \delta)$$

whenever $\beta \leq \delta \prec \theta \leq \alpha \vee \beta$.

Proof. If the statement of the lemma is false for $\mathbf{A}$, then it is false for $\mathbf{A}/[\alpha, \alpha]$, so we need only to prove the lemma in the case where $[\alpha, \alpha] = 0$. Assume throughout the proof that $[\alpha, \alpha] = 0$ and $\beta \leq \delta \prec \theta \leq \alpha \vee \beta$. We will argue that $C(\alpha \vee \beta, \theta; \delta)$.

Since $\beta \leq \delta \leq \alpha \vee \beta$, we get $\alpha \vee \delta = \alpha \vee \beta$. Hence, we need to show that $C(\alpha \vee \delta, \theta; \delta)$. But

$$C(\alpha \vee \delta, \theta; \delta) \iff C(\alpha, \theta; \delta) \;\&\; C(\delta, \theta; \delta).$$

Since $C(\delta, \theta; \delta)$ holds for any two congruences δ and θ, we can establish the lemma by showing that $C(\alpha, \theta; \delta)$. We will use the fact that $\langle \delta, \theta \rangle$ is α–regular, which follows from Theorem 2.6 (1). Theorem 2.6 (4) applies, since $[\alpha, \alpha] = 0 \leq \theta$ and $\langle \delta, \theta \rangle$ is α–regular. This guarantees that the conditions $C(\alpha; \theta; \delta)$, $C(\theta; \alpha; \delta)$, $[\theta, \alpha] \leq \delta$ and $[\alpha, \theta] \leq \delta$ are equivalent, so it suffices to establish any one of these conditions.

Case 1. $\alpha \wedge \theta \leq \delta$.

In this case, $[\alpha, \theta] \leq \alpha \wedge \theta \leq \delta$, so $C(\alpha, \theta; \delta)$ and we are done.

Case 2. $\alpha \wedge \theta \not\leq \delta$.

Let $\lambda = \alpha \wedge \delta$ and choose ν such that $\lambda \prec \nu \leq \alpha \wedge \theta$. The prime quotients $\langle \lambda, \nu \rangle$ and $\langle \delta, \theta \rangle$ are perspective prime quotients which are both α–regular (since $[\alpha, \alpha] = 0$). Now,

$$[\nu, \alpha] \leq [\alpha, \alpha] = 0 \leq \lambda,$$

so $C(\nu, \alpha; \lambda)$ by Theorem 2.6 (4). But $\lambda = \alpha \wedge \delta$, so $C(\nu, \alpha; \lambda)$ implies $C(\nu, \alpha; \delta)$. Together with $C(\delta, \alpha; \delta)$ we get $C(\delta \vee \nu, \alpha; \delta)$. But $\delta \vee \nu = \theta$, so we have $C(\theta, \alpha; \delta)$. By Theorem 2.6 (4), we have $C(\alpha, \theta; \delta)$. This finishes the proof of Case 2, and therefore it finishes the proof of the lemma. □

Lemma 6.5. *Assume that* $\mathbf{A}$ *is a finite algebra and that* $\mathbf{Con}(\mathbf{A})$ *has congruences* α, β *such that* $[\alpha, \alpha] \leq \beta$ *and* $\alpha \vee \beta = 1$. *Then for the conditions listed below,* $(i) \Longrightarrow (ii) \Longrightarrow (iii)$.

(*i*) $V(\mathbf{A})$ *is a TSSS variety.*
(*ii*) $\mathrm{typ}\{\beta, 1\} = \{\mathbf{2}\}$.
(*iii*) $C(1, 1; \beta)$ *holds.*

Proof. The implication $(ii) \Longrightarrow (iii)$ clearly follows from Corollary 2.13. So assume that (i) holds. From the previous lemma we know that $C(1, \theta; \delta)$ whenever $\beta \leq \delta \prec \theta \leq 1$. This tells us two things. First, the interval $I[\beta, 1]$ is solvable, so $\mathrm{typ}\{\beta, 1\} \subseteq \{\mathbf{1}, \mathbf{2}\}$. Second, referring to Lemma 6.1 $(i) \Longleftrightarrow (iii)$, we find that $\mathbf{1} \notin \mathrm{typ}\{\beta, 1\}$ since we are in a TSSS variety. Hence, $\mathrm{typ}\{\beta, 1\} = \{\mathbf{2}\}$ and (ii) holds. □

Lemma 6.6. *Assume that* $\mathbf{A}$ *belongs to a TSSS variety and* $\mathbf{A}$ *has a congruence* α *such that* $[1, \alpha] = 0$. *Then* $\mathbf{B} = \mathbf{A}(\alpha)/\Delta_{1,\alpha}$ *generates an affine variety. If* $\alpha > 0$, *then* $\mathbf{B}$ *is nontrivial.*

Proof. Since $C(1, \alpha; 0)$ in $\mathbf{Con}(\mathbf{A})$, we get $C(1, \overline{\alpha}; \eta_i)$, $i = 1, 2$, in $\mathbf{Con}(\mathbf{A}(\alpha))$, and therefore $C(1, \overline{\alpha}; 0)$ as well. Thus, $[1, \overline{\alpha}] = 0$, and so $[\overline{\alpha}, \overline{\alpha}] = 0 \leq \Delta_{1,\alpha}$. We also have $\overline{\alpha} \vee \Delta_{1,\alpha} = 1$. Lemma 6.5 proves that $C(1, 1; \Delta_{1,\alpha})$ holds; so, by Theorem 6.2, $\mathbf{B}$ generates an affine variety.

If $\alpha > 0$, then the universe of $\mathbf{A}(\alpha)$ properly contains the diagonal, but the diagonal is a union of $\Delta_{1,\alpha}$–classes. Hence, there are at least two distinct $\Delta_{1,\alpha}$–classes. It follows that $\mathbf{B}$ contains at least two elements. □

Lemma 6.7. *Assume that* $\mathbf{A}$ *is an algebra with a congruence* α *such that* $[1, \alpha] = 0$. *If* $d(x, y, z)$ *is a term which interprets as a Mal'cev operation on* $\mathbf{A}/\alpha$ *and on* $\mathbf{A}(\alpha)/\Delta_{1,\alpha}$, *then a term* $M(x, y, z)$ *which interprets as a Mal'cev operation on* $\mathbf{A}$ *may be constructed by composition from* $d(x, y, z)$.

Proof. Write Δ for $\Delta_{1,\alpha}$. The statement that $d(x, y, z)$ interprets as a Mal'cev operation on each of $\mathbf{A}/\alpha$ and $\mathbf{A}(\alpha)/\Delta$ is equivalent to the statement that for all $u, v \in A$ and $(a, b), (c, e), (f, g) \in \alpha$ we have that

$$d^{\mathbf{A}}(u, u, v) \; \alpha \; v \; \alpha \; d^{\mathbf{A}}(v, u, u)$$

and that $\begin{pmatrix} a \\ b \end{pmatrix} \Delta \begin{pmatrix} c \\ e \end{pmatrix}$ implies

$$d^{\mathbf{A}(\alpha)}\left(\begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} c \\ e \end{pmatrix}\begin{pmatrix} f \\ g \end{pmatrix}\right) \Delta \begin{pmatrix} f \\ g \end{pmatrix} \Delta \; d^{\mathbf{A}(\alpha)}\left(\begin{pmatrix} f \\ g \end{pmatrix}\begin{pmatrix} c \\ e \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}\right).$$

Claim 1. For any $a \in A$ the polynomials $d^{\mathbf{A}}(x, a, a), d^{\mathbf{A}}(a, a, x)$ and $d^{\mathbf{A}}(x, x, x)$ are one–to–one functions. Furthermore, if $(a, b) \in \alpha$, then $d^{\mathbf{A}}(x, a, a) = d^{\mathbf{A}}(x, b, b)$ and $d^{\mathbf{A}}(a, a, x) = d^{\mathbf{A}}(b, b, x)$.

Proof of Claim 1. Assume that for $u, v \in A$ we have that $d^{\mathbf{A}}(u,a,a) = w = d^{\mathbf{A}}(v,a,a)$. Since $d^{\mathbf{A}}(x,a,a)\ \alpha\ x$, then

$$u\ \alpha\ d^{\mathbf{A}}(u,a,a) = d^{\mathbf{A}}(v,a,a)\ \alpha\ v;$$

hence $(u,v) \in \alpha$. But now, $(u,v),(a,a) \in \alpha$ and $\begin{pmatrix} a \\ a \end{pmatrix}\ \Delta\ \begin{pmatrix} a \\ a \end{pmatrix}$. Hence, from above we see that

$$\begin{pmatrix} w \\ w \end{pmatrix} = d^{\mathbf{A}(\alpha)}\left(\begin{pmatrix} u \\ v \end{pmatrix}\begin{pmatrix} a \\ a \end{pmatrix}\begin{pmatrix} a \\ a \end{pmatrix}\right)\ \Delta\ \begin{pmatrix} u \\ v \end{pmatrix}.$$

Since the diagonal of $\mathbf{A}(\alpha)$ is a union of Δ–classes, we conclude that $u = v$ and hence that $d^{\mathbf{A}}(x,a,a)$ is one–to–one. A similar proof works for $d^{\mathbf{A}}(a,a,x)$.

Now, assume that $(a,b) \in \alpha$ and that $r \in A$. Since $\begin{pmatrix} a \\ b \end{pmatrix}\ \Delta\ \begin{pmatrix} a \\ b \end{pmatrix}$, then

$$\begin{pmatrix} r \\ r \end{pmatrix}\ \Delta\ d^{\mathbf{A}(\alpha)}\left(\begin{pmatrix} r \\ r \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}\right) = \begin{pmatrix} d^{\mathbf{A}}(r,a,a) \\ d^{\mathbf{A}}(r,b,b) \end{pmatrix}.$$

Again using the fact that the diagonal of $\mathbf{A}(\alpha)$ is a union of Δ–classes we see that $d^{\mathbf{A}}(r,a,a) = d^{\mathbf{A}}(r,b,b)$. A similar proof shows that $d^{\mathbf{A}}(a,a,x) = d^{\mathbf{A}}(b,b,x)$ for all $x \in A$.

Finally we must show that $d^{\mathbf{A}}(x,x,x)$ is one–to–one. Assume that $d^{\mathbf{A}}(u,u,u) = w = d^{\mathbf{A}}(v,v,v)$ for some $u, v \in A$. Since d is Mal'cev on $\mathbf{A}/\alpha$, we get that $d^{\mathbf{A}}(x,x,x)\ \alpha\ x$, so we must have $(u,w),(w,v) \in \alpha$. From what we have already proved, $d^{\mathbf{A}}(x,u,u) = d^{\mathbf{A}}(x,v,v)$, so $d^{\mathbf{A}}(u,v,v) = d^{\mathbf{A}}(u,u,u) = w$. Since $d^{\mathbf{A}}(x,v,v)$ is one–to–one and $d^{\mathbf{A}}(u,v,v) = w = d^{\mathbf{A}}(v,v,v)$, we get $u = v$. Claim 1 is proved. □

Claim 2. For η_i equal to the i–th projection kernel of $\mathbf{A}(\alpha)$ we have $\eta_i \wedge \Delta = 0_{\mathbf{A}}$.

Proof of Claim 2. We prove the claim for η_1 only. Assume that $\begin{pmatrix} a \\ b \end{pmatrix}\ \eta_1\ \wedge\ \Delta\ \begin{pmatrix} a \\ c \end{pmatrix}$. Necessarily we have $(a,b),(a,c) \in \alpha$. Using Claim 1, we get the first equality in

$$\begin{pmatrix} d^{\mathbf{A}}(c,c,c) \\ d^{\mathbf{A}}(b,b,b) \end{pmatrix} = \begin{pmatrix} d^{\mathbf{A}}(a,a,c) \\ d^{\mathbf{A}}(b,c,c) \end{pmatrix} = d^{\mathbf{A}(\alpha)}\left(\begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} a \\ c \end{pmatrix}\begin{pmatrix} c \\ c \end{pmatrix}\right)\ \Delta\ \begin{pmatrix} c \\ c \end{pmatrix}.$$

Hence $d^{\mathbf{A}}(b,b,b) = d^{\mathbf{A}}(c,c,c)$. By Claim 1 we have that $b = c$. This completes the argument for Claim 2. □

We define a first approximation to a Mal'cev term on $\mathbf{A}$:

$$p(x,y,z) = d(d(z,z,x), d(d(x,x,z),z,y),z).$$

Claim 3. The algebras $\mathbf{A}/\alpha$ and $\mathbf{A}(\alpha)/\Delta$ satisfy the equation $d(x,y,z) = p(x,y,z)$. Furthermore, $\mathbf{A}$ satisfies the equation $p(x,x,z) = z$.

Proof of Claim 3. The fact that $\mathbf{A}/\alpha$ and $\mathbf{A}(\alpha)/\Delta$ satisfy the equation $d(x,y,z) = p(x,y,z)$ follows from the definition of p and the fact that d interprets as a Mal'cev operation on these algebras.

We must show that $\mathbf{A}$ satisfies the equation $p(x,x,z) = z$, which may be written as $d(d(z,z,x), d(d(x,x,z),z,x),z) = z$. To show that this holds, choose $a, b \in A$ arbitrarily. We will show that $d^{\mathbf{A}}(d^{\mathbf{A}}(b,b,a), d^{\mathbf{A}}(d^{\mathbf{A}}(a,a,b),b,a),b) = b$. Set $u =$

$d^{\mathbf{A}}(d^{\mathbf{A}}(a,a,b),b,a)$. Since $d^{\mathbf{A}}(a,a,b)\ \alpha\ b$, we get that $u\ \alpha\ d^{\mathbf{A}}(b,b,a)\ \alpha\ a$. Hence the pairs $\begin{pmatrix} d^{\mathbf{A}}(b,b,a) \\ u \end{pmatrix}$, $\begin{pmatrix} u \\ u \end{pmatrix}$ and $\begin{pmatrix} b \\ b \end{pmatrix}$ belong to $\mathbf{A}(\alpha)$, and the latter two are Δ–related. This means that

$$\begin{pmatrix} d^{\mathbf{A}}(d^{\mathbf{A}}(b,b,a),u,b) \\ d^{\mathbf{A}}(u,u,b) \end{pmatrix} = d^{\mathbf{A}(\alpha)}\left(\begin{pmatrix} d^{\mathbf{A}}(b,b,a) \\ u \end{pmatrix}\begin{pmatrix} u \\ u \end{pmatrix}\begin{pmatrix} b \\ b \end{pmatrix}\right)\ \Delta\ \begin{pmatrix} d^{\mathbf{A}}(b,b,a) \\ u \end{pmatrix}.$$

We can modify the left side of this displayed line by noticing that $d^{\mathbf{A}}(d^{\mathbf{A}}(b,b,a),u,b) = p^{\mathbf{A}}(a,a,b)$ and that (since $u\ \alpha\ a$) $d^{\mathbf{A}}(u,u,b) = d^{\mathbf{A}}(a,a,b)$. Hence the left side equals $\begin{pmatrix} p^{\mathbf{A}}(a,a,b) \\ d^{\mathbf{A}}(a,a,b) \end{pmatrix}$. We can modify the right side replacing u with $d^{\mathbf{A}}(d^{\mathbf{A}}(a,a,b),b,a)$. Starting with this and continuing yields

$$\begin{pmatrix} d^{\mathbf{A}}(b,b,a) \\ d^{\mathbf{A}}(d^{\mathbf{A}}(a,a,b),b,a) \end{pmatrix} = d^{\mathbf{A}(\alpha)}\left(\begin{pmatrix} b \\ d^{\mathbf{A}}(a,a,b) \end{pmatrix}\begin{pmatrix} b \\ b \end{pmatrix}\begin{pmatrix} a \\ a \end{pmatrix}\right)\ \Delta\ \begin{pmatrix} b \\ d^{\mathbf{A}}(a,a,b) \end{pmatrix}.$$

Putting the left and right modifications together, we get that

$$\begin{pmatrix} p^{\mathbf{A}}(a,a,b) \\ d^{\mathbf{A}}(a,a,b) \end{pmatrix}\ \eta_2 \wedge \Delta\ \begin{pmatrix} b \\ d^{\mathbf{A}}(a,a,b) \end{pmatrix}.$$

From Claim 2 we deduce that $p^{\mathbf{A}}(a,a,b) = b$, as desired. This completes the proof of Claim 3. □

Our Mal'cev operation M must be constructed from p in a different way than p was constructed from d. The definition of M is

$$M(x,y,z) = p(p(x,p(x,z,z),x),p(y,p(y,z,z),y),z).$$

Claim 4. The algebras $\mathbf{A}/\alpha$ and $\mathbf{A}(\alpha)/\Delta$ satisfy $p(x,y,z) = M(x,y,z)$. Furthermore, $M^{\mathbf{A}}(x,y,z)$ is a Mal'cev operation.

Proof of Claim 4. The first part of Claim 4 is handled just like the first part of Claim 3. From the definition of M and the fact that $\mathbf{A} \models p(x,x,z) = z$ we get that $\mathbf{A} \models M(x,x,z) = z$. We must prove that for any $a, b \in A$ we have

$$\begin{aligned} a &= M^{\mathbf{A}}(a,b,b) \\ &= p^{\mathbf{A}}(p^{\mathbf{A}}(a,p^{\mathbf{A}}(a,b,b),a),p^{\mathbf{A}}(b,p^{\mathbf{A}}(b,b,b),b),b) \\ &= p^{\mathbf{A}}(p^{\mathbf{A}}(a,p^{\mathbf{A}}(a,b,b),a),b,b). \end{aligned}$$

In the upcoming calculations, when moving from the first line to the second, we will use the fact that $p^{\mathbf{A}}(a,p^{\mathbf{A}}(a,b,b),p^{\mathbf{A}}(a,b,b)) = p^{\mathbf{A}}(a,a,a) = a$, which follows from $p^{\mathbf{A}}(a,b,b)\ \alpha\ a$ and Claim 1.

$$\begin{aligned} &p^{\mathbf{A}(\alpha)}\left(\begin{pmatrix} p^{\mathbf{A}}(a,p^{\mathbf{A}}(a,b,b),a) \\ a \end{pmatrix}\begin{pmatrix} b \\ b \end{pmatrix}\begin{pmatrix} b \\ b \end{pmatrix}\right)\Delta\begin{pmatrix} p^{\mathbf{A}}(a,p^{\mathbf{A}}(a,b,b),a) \\ a \end{pmatrix} \\ &= p^{\mathbf{A}(\alpha)}\left(\begin{pmatrix} a \\ a \end{pmatrix}\begin{pmatrix} p^{\mathbf{A}}(a,b,b) \\ p^{\mathbf{A}}(a,b,b) \end{pmatrix}\begin{pmatrix} a \\ p^{\mathbf{A}}(a,b,b) \end{pmatrix}\right)\Delta\begin{pmatrix} a \\ p^{\mathbf{A}}(a,b,b) \end{pmatrix}. \end{aligned}$$

Replacing the first expression in the above sequence with an equal value yields

$$\begin{pmatrix} M^{\mathbf{A}}(a,b,b) \\ p^{\mathbf{A}}(a,b,b) \end{pmatrix} \eta_2 \wedge \Delta \begin{pmatrix} a \\ p^{\mathbf{A}}(a,b,b) \end{pmatrix}.$$

From Claim 2 we deduce that $M^{\mathbf{A}}(a,b,b) = a$. This finishes the proof of Claim 4 and therefore of the theorem. □

There is a simpler proof of the previous lemma if one assumes that $\mathbf{A}$ is finite. After proving Claim 1 one knows that for all $a \in A$ the polynomials $d^{\mathbf{A}}(x,a,a)$ and $d^{\mathbf{A}}(a,a,x)$ are one–to–one. When $\mathbf{A}$ is finite this implies that these polynomials are permutations. From this one can construct a Mal'cev term from d by iteration. Unlike the argument given above, in this argument the complexity of the term M depends on $|A|$.

Theorem 6.8. *If $\mathcal{V}$ is a TSSS variety generated by a left nilpotent algebra, then $\mathcal{V}$ is congruence permutable.*

Proof. We may assume that $\mathcal{V}$ is generated by a finite, left nilpotent algebra. For if $\mathcal{V}$ is a TSSS variety generated by a left nilpotent algebra, then $\mathbf{F}_{\mathcal{V}}(2)$ is a finite, left nilpotent algebra. If the theorem holds for finitely generated varieties, then $\mathcal{V}' = \mathsf{V}(\mathbf{F}_{\mathcal{V}}(2))$ is congruence permutable. But $\mathcal{V}' = \mathsf{V}(\mathbf{F}_{\mathcal{V}}(2))$ is congruence permutable iff $\mathcal{V}$ is congruence permutable. (The reason for this is that any Mal'cev term for $\mathcal{V}'$ is also a Mal'cev term for $\mathcal{V}$, since the defining equations for a Mal'cev term involve only two variables.) Thus, we only need to prove the theorem in the case when $\mathcal{V}$ is generated by a finite, left nilpotent algebra.

Let $\mathcal{A}$ denote the class of finite, left nilpotent algebras that generate TSSS varieties. We will use induction on the nilpotence class to prove that for any $\mathbf{A} \in \mathcal{A}$ the variety $\mathsf{V}(\mathbf{A})$ is congruence permutable. As we explained in the last paragraph, this will finish the proof.

If $\mathbf{A} \in \mathcal{A}$ is abelian, then Theorem 6.2 proves that $\mathsf{V}(\mathbf{A})$ is affine and therefore congruence permutable. The base case for our inductive proof has been established. For the inductive step of our argument, choose $\mathbf{A} \in \mathcal{A}$ of nilpotence class $k > 1$ and assume that the theorem is true for all $\mathbf{A}' \in \mathcal{A}$ of smaller nilpotence class. Since $\mathbf{A}$ is of nilpotence class k, we have $(1]^{k+1} = 0 < (1]^k$. Let $\alpha = (1]^k$; note that $\mathbf{A}/\alpha$ has nilpotence class $k-1$. Let $\Delta = \Delta_{1,\alpha} \in \mathrm{Con}(\mathbf{A}(\alpha))$. We have $[1,\alpha] = 0$, so by Lemma 6.6 we have that $\mathbf{A}(\alpha)/\Delta$ is affine. Let $\beta = \overline{\alpha} \wedge \Delta$ in $\mathbf{Con}(\mathbf{A}(\alpha))$. Notice that $\mathbf{A}(\alpha)/\overline{\alpha} \cong \mathbf{A}/\alpha$ is of nilpotence class $k-1$, and $\mathbf{A}(\alpha)/\Delta$ is abelian since it is affine. $\mathbf{B} = \mathbf{A}(\alpha)/\beta$ is of nilpotence class $\leq k-1$, since it is a subdirect product of algebras of nilpotence class $\leq k-1$. Since $\mathbf{B} \in \mathsf{V}(\mathbf{A})$, we get that $\mathsf{V}(\mathbf{B})$ is TSSS. This means that $\mathbf{B} \in \mathcal{A}$ and, from our inductive hypothesis, $\mathsf{V}(\mathbf{B})$ is congruence permutable. Let $d(x,y,z)$ be a term which interprets as a Mal'cev operation on $\mathbf{B}$. Then $d(x,y,z)$ interprets as a Mal'cev operation, both on $\mathbf{A}(\alpha)/\overline{\alpha} \cong \mathbf{A}/\alpha$ and on $\mathbf{A}(\alpha)/\Delta$. Hence, by Lemma 6.7, there is a term $M(x,y,z)$ constructible from $d(x,y,z)$ which interprets as a Mal'cev operation on $\mathbf{A}$. This proves that $\mathsf{V}(\mathbf{A})$ is congruence permutable, and the argument for the inductive step is complete. □

Corollary 6.9. *If $\mathcal{V}$ is a TSSS variety, then $\mathcal{V}$ has a congruence permutable subvariety containing all left nilpotent members of $\mathcal{V}$.*

Proof. We need to prove that if $\mathcal{V}$ is a TSSS variety, then there is a term which interprets as a Mal'cev operation on every left nilpotent algebra in $\mathcal{V}$. For then the

equations which state that this term is a Mal'cev operation define a congruence permutable subvariety of $\mathcal{V}$ containing all the left nilpotent members of $\mathcal{V}$.

Let $\{t_1(x,y,z),\dots,t_n(x,y,z)\}$ be a set of representatives of the $\mathcal{V}$–inequivalent ternary terms. If, for each i, there is a left nilpotent $\mathbf{A}_i \in \mathcal{V}$ such that t_i does not interpret as a Mal'cev operation on $\mathbf{A}_i$, then no ternary term interprets as a Mal'cev operation on the left nilpotent algebra $\prod_{i\leq n}\mathbf{A}_i$. We proved this to be impossible in Theorem 6.8. The conclusion is that some t_i interprets as a Mal'cev operation on every left nilpotent member of $\mathcal{V}$. □

Example. (We cannot replace left nilpotence with solvability) To see that the nilpotence hypothesis in Theorem 6.8 cannot be weakened to solvability, we exhibit a TSSS variety which is generated by a finite solvable algebra but is not congruence permutable.

Let $\mathcal{V}$ be the variety with one binary operation, denoted by juxtaposition, and one nullary operation, 1, which is defined by the equations $\mathcal{V} \models 1x = x1 = x$. If $\mathbf{A} \in \mathcal{V}$ and $a \in A - \{1\}$, then $\langle a, 1\rangle$ is a 1–snag of $\mathbf{A}$. Hence there does not exist a nontrivial, finite, strongly solvable algebra in $\mathcal{V}$. It follows that every locally finite subvariety of $\mathcal{V}$ is a TSSS variety. So let $\mathbf{A}$ be the member of $\mathcal{V}$ presented by

$$\langle a, b \mid a^2 = b^2 = ab = ba = 1\rangle.$$

$A = \{1, a, b\}$, and Con $\mathbf{A}$ is a 3–element chain with $\alpha = \mathrm{Cg}(a,b)$ the unique nontrivial, proper congruence. It is easy to see that $\mathrm{typ}(0,\alpha) = \mathbf{1}$ and $\mathrm{typ}(\alpha,1) = \mathbf{2}$, so $\mathbf{A}$ is solvable and $\mathsf{V}(\mathbf{A})$ is a TSSS variety, but $\mathsf{V}(\mathbf{A})$ is not congruence permutable.

We pointed out in Section 5 that an abelian algebra with a Mal'cev polynomial has a Mal'cev term. This can be taken as the basis step in a proof by induction, modeled on the proof of Theorem 6.8, of the following result (which becomes false if the word "nilpotent" is replaced by "solvable").

Theorem 6.10. *Any nilpotent algebra with a Mal'cev polynomial has a Mal'cev term.*

In this section we have focused on left nilpotent algebras in TSSS varieties. The results extend to other types of nilpotent algebras in TSSS varieties, since [7] proves that the hypothesis of left nilpotence is weaker than any other notion of nilpotence. For example, if $\mathbf{A}$ is a finite algebra satisfying $[1,1)^{k+1} = 0$ ($\mathbf{A}$ is k–step right nilpotent), then $\mathbf{A}$ is left nilpotent although possibly of higher nilpotence class. Similarly, if a mixed expression like $[1,[[1,[1,1]],1]] = 0$ holds, then $\mathbf{A}$ is left nilpotent. We know very little about which non–nilpotent algebras generate TSSS varieties, except that some of the arguments in this section may be localized.

We conclude this section with a peculiar application of Theorem 6.8.

Corollary 6.11. *Let $\mathcal{V}$ be an idempotent variety generated by nilpotent algebras. If $\mathbf{F}_{\mathcal{V}}(2)$ has odd cardinality, then $\mathcal{V}$ is congruence permutable.*

Proof. As we pointed out in the proof of Theorem 6.8, to show that $\mathcal{V}$ is congruence permutable it suffices to prove that the subvariety $\mathcal{V}' = \mathsf{V}(\mathbf{F}_{\mathcal{V}}(2))$ is congruence permutable. We shall prove this with the aid of Theorem 6.8. If $\mathbf{F}_{\mathcal{V}}(2)$ has odd cardinality, then $\mathcal{V}'$ is generated by the finite, left nilpotent algebra $\mathbf{F}_{\mathcal{V}}(2)$. We need only to prove that the locally strongly solvable subvariety of $\mathcal{V}'$ is trivial to complete the argument.

Let α be the automorphism of $\mathbf{F}_{\mathcal{V}}(2)$ determined by switching the generators. This automorphism has order two, and, since $|F_{\mathcal{V}}(2)|$ is odd, this implies that there is an element $w \in F_{\mathcal{V}}(2)$ such that $\alpha(w) = w$. If $w(x, y)$ is any binary term representing w, then $w(x, y) = w(y, x)$ is an equation of $\mathcal{V}'$.

If $\mathcal{V}'$ has a nontrivial locally strongly solvable subvariety, then it has a strongly abelian, minimal subvariety, $\mathcal{M}$. The strictly simple generator of $\mathcal{M}$ is term equivalent to a matrix power of a 2–element set or a 2–element pointed set, as we have proved. But since we are working with idempotent algebras, $\mathcal{M}$ must in fact be equivalent to the variety of sets. The term $w(x, y)$ must interpret as a projection in $\mathcal{M}$; either $w(x, y) = x$ or $w(x, y) = y$ is an equation of $\mathcal{M}$. But now we have a contradiction: $\mathcal{M}$ satisfies $w(x, y) = w(y, x)$ and either $w(x, y) = x$ or $w(x, y) = y$, but it does not satisfy $x = y$. This is clearly impossible. The conclusion is that $\mathcal{V}'$ is TSSS and so is congruence permutable. It follows that $\mathcal{V}$ is congruence permutable as well. □

We called this corollary 'peculiar' because the odd cardinality hypothesis results in such a strong conclusion. If, for example, we start with a finite nilpotent group $\mathbf{G}$ and take the reduct $\langle G; x^r y^{1-r} \rangle$ for some r, then we get a nilpotent algebra which generates an idempotent variety. The cardinality $|F_{\mathcal{V}}(2)|$ can turn out to be either odd or even. Often, but only when $|F_{\mathcal{V}}(2)|$ is even, this type of variety is not congruence permutable.

References

[1] J. Berman and S. Seif. An approach to tame congruence theory via subtraces. *Algebra Universalis*, 30:479–520, 1993. MR **94f:**08003

[2] S. Burris and H.P. Sankappanavar. *A Course in Universal Algebra*. Springer-Verlag, 1981. MR **83k:**08001

[3] R. Freese and R. McKenzie. *Commutator Theory for Congruence Modular Varieties*, volume 125 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1987. MR **89c:**08006

[4] S. Givant. Universal Horn classes categorical or free in power. *Ann. Math. Logic*, 15:1–53, 1978. MR **80c:**03032

[5] S. Givant. A representation theorem for universal Horn classes categorical in power. *Ann. Math. Logic*, 17:91–116, 1979. MR **81b:**03038

[6] D. Hobby and R. McKenzie. *The Structure of Finite Algebras*, volume 76 of *Contemporary Mathematics*. American Mathematical Society, 1988. MR **89m:**08001

[7] K. Kearnes. An order-theoretic property of the commutator. *International Journal of Algebra and Computation*, 3:491–534, 1993. MR **95c:**08002

[8] K. Kearnes. Categorical quasivarieties via Morita equivalence. preprint, 1994.

[9] K. Kearnes and Á. Szendrei. A characterization of minimal locally finite varieties. Trans. Amer. Math. Soc. 349:1749–1768, 1977. CMP 97:09

[10] E. Kiss. An easy way to minimal algebras. Internat. J. Algebra Comput. 7:55–75, 1977. CMP 97:06

[11] E. Kiss and P. Pröhle. Problems and results in tame congruence theory. *Algebra Universalis*, 29:151–171, 1992. MR **93g:**08004

[12] R. McKenzie. Algebraic version of the general Morita theorem for algebraic varieties. preprint.

[13] R. McKenzie. Finite forbidden lattices. In *Universal Algebra and Lattice Theory*, volume 1004 of *Springer Lecture Notes*. Springer-Verlag, 1983, pp. 176-205. MR **85b:**06006

[14] R. McKenzie. Categorical quasivarieties revisited. *Algebra Universalis*, 19:273–303, 1984. MR **87g:**08022

[15] E. Palyutin. The description of categorical quasivarieties. *Algebra and Logic*, 14:86–111, 1975. MR **53:**2672

[16] Á. Szendrei. Maximal non-affine reducts of simple affine algebras. *Algebra Universalis*. 34:144–174, 1995. MR **96i:**08001

[17] Á. Szendrei. *Clones in Universal Algebra*, volume 99 of *Séminaire de Mathématiques Superieures*. Les Presses de l'Université de Montréal, 1986. MR **87m:**08005

[18] Á. Szendrei. A survey on strictly simple algebras and minimal varieties. In A. Romanowska and J. D. H. Smith, editors, *Universal Algebra and Quasigroup Theory*. Heldermann Verlag, Berlin, 1992, pp. 209–239. MR **93h:**08001

[19] Á. Szendrei. Strongly abelian minimal varieties. *Acta Sci. Math. (Szeged)*, 59:25–42, 1994. MR **95g:**08002

[20] W. Taylor. The fine spectrum of a variety. *Algebra Universalis*, 5:262–303, 1975. MR **52:**10547

Department of Mathematics, University of Louisville, Louisville, Kentucky 40292
E-mail address: kakear01@homer.louisville.edu

Department of Algebra and Number Theory, Eötvös Lóránd University, 1088 Budapest, Múzeum krt. 6–8, Hungary
E-mail address: ewkiss@cs.elte.hu

Department of Mathematics and Statistics, McMaster University, Hamilton, Ontario, Canada, L8S 4K1
E-mail address: valeriot@mcmaster.ca