CONTEMPORARY MATHEMATICS

76

The Structure of Finite Algebras

David Hobby
Ralph McKenzie

American Mathematical Society
Providence, Rhode Island

2000 *Mathematics Subject Classification.* Primary 08A05.

Library of Congress Cataloging-in-Publication Data

Hobby, David Charles.
The structure of finite algebras.
(Contemporary mathematics, v. 76)
Bibliography: p.
Includes indexes.
1. Algebra, Universal. I. McKenzie, Ralph. II. Title. III. Series: Comtemporary mathematics (American Mathematical Society, v. 76)
QA251.H65 1988 512 88-16712
ISBN 0-8218-5073-3

---

10 9 8 7 6 5 4 3 04 03 02 01 00

Dedicated to

PROFESSOR JAMES DONALD MONK

An inspiring teacher of

congruence lore

Contents

INTRODUCTION

By a *finite algebra* we mean a finite set of elements together with a (possibly infinite) set of operations acting on this set of elements. This concept includes finite groups and rings and many other algebraic systems of interest in mathematics. Excluded are finite systems with infinitary operations, and those having "partial operations" (operations defined for some, but not all, n-tuples of elements). By a *locally finite variety* we mean a class of algebras of one type, closed under the formation of homomorphic images, subalgebras, and direct products, whose finitely generated algebras are finite. The class of groups satisfying $x^3 = 1$ is an example of a locally finite variety.

The main discovery presented in this book is that the lattice of congruences of a finite algebra determines very deeply the structure of that algebra. Our theory reveals a sharp division of locally finite varieties of algebras into six interesting new families, each of which is characterized by the behavior of congruences in the algebras. We use the theory to derive many new results that will be of interest not only to universal algebraists, but to other algebraists as well.

The utility of congruence lattices for revealing the structure of general algebras has been recognized since Garrett Birkhoff's pioneering work in the 1930's and 1940's. Our theory, nevertheless, is of very recent origin; and its germ can be found in the paper [27] of P.P. Pálfy and P. Pudlák. In 1981, McKenzie obtained two crucial results for the theory (rudimentary versions of Theorem 2.8 and Theorem 2.11) and applied them in [22]. Further impetus was given by results of Hobby in [18] (an early version of Theorem 5.5) and of Pálfy in [26] (Theorem 4.7). The theory then rapidly evolved through the joint efforts of the authors. Most of the results presented here were discovered during the first ten months of 1983.

Basic tame congruence theory is presented in Chapters 1 through 5. We have strived for a straightforward and complete development of this material, since we believe that the theory offers great promise for a wide variety of investigations. In Chapters 6 and 7, we move beyond the consideration of individual algebras, into a study of locally finite varieties. Chapters 8 through 14 focus on various aspects of locally finite varieties. A list of open problems finishes the work.

We now give a non-technical overview of the chief results contained in this book, often summarizing the results in a weaker form than is proved in the text, in order to avoid technicalities.

The first noteworthy product of the theory is the result that every finite algebra with three or more congruences, having a simple and complemented congruence lattice, is a subreduct of a module over a finite simple ring with unit. If the congruence lattice of such an algebra is not isomorphic to the congruence lattice of a finite vector space, then the algebra is a subreduct of a matrix power of an algebra whose operations are trivial. These results are contained in Theorems 2.11, 5.7, 5.8, 13.3 and 13.5; and they are also valid locally, for interval sublattices of a congruence lattice. They imply, indirectly, two theorems of [22]: A finite, simple, complemented lattice of more than two elements cannot be isomorphic to the lattice of subvarieties of any locally finite variety; and under certain further mild conditions, cannot be isomorphic to the congruence lattice of a finite algebra with one basic operation.

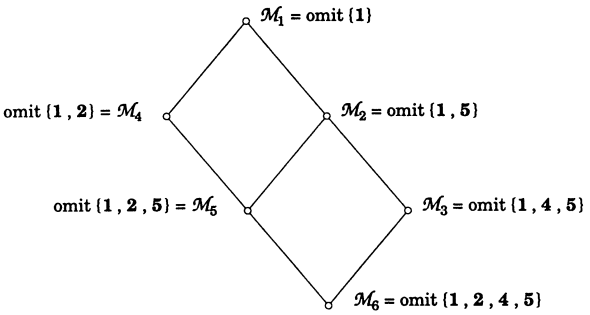
In the underlying theory, "tight" intervals in a congruence lattice, including two-element intervals or prime quotients, are divided into five types, or categories. Each type has a particular kind of algebra associated with it. The correspondences are as follows: **1** – a finite set with a group of permutations, **2** – a vector space over a finite field, **3** – the two element Boolean algebra, **4** – the two element lattice, **5** – the two element semilattice. To some extent, the properties of these algebras carry over to the types that correspond to them.

We label each prime quotient with its type, thereby making the congruence lattice of a finite algebra into a labeled graph. It soon appears that intervals in which only a restricted set of types appear are special; for instance they must be modular or semi-distributive lattices, depending on the types (Corollary 5.20, Corollary 6.8). Furthermore, the type of a prime quotient is strongly influenced in various ways by the shape of the congruence lattice in its local neighborhood (Lemmas 5.19, 6.2–6.6, 6.9–6.10).

There is a close connection between the set of Mal'cev conditions satisfied by a locally finite variety, and its type set (the set of all types of prime quotients of the finite algebras in the variety). The main tool for the development of this connection comes out of the study of solvability in Chapter 7. Every locally finite algebra $\mathbf{A}$ admits two natural congruences, the solvability congruences $\overset{s}{\sim}$ and $\overset{ss}{\sim}$, on its congruence lattice. These are complete lattice congruences such that the quotient lattices are algebraic and $(\mathbf{Con}\ \mathbf{A})/\overset{s}{\sim}$ is a meet semi-distributive lattice. Every congruence class of $\overset{s}{\sim}$, modulo the smaller congruence $\overset{ss}{\sim}$, is a modular lattice. If $\mathbf{A}$ is finite and if $\alpha \leq \beta$ in $\mathbf{Con}\ \mathbf{A}$, then $\alpha \overset{s}{\sim} \beta$ iff β is solvable over α. (Solvability is defined using a generalization of the commutator for modular varieties.) With the same conditions, $\alpha \overset{ss}{\sim} \beta$ iff all the prime quotients in the interval $I[\alpha, \beta]$ are of type **1**. Then if $\mathcal{V}$ is any locally finite variety we find (Theorem 7.12) that these statements are equivalent: $\mathbf{1} \notin \mathrm{typ}\{\mathcal{V}\}$; $\alpha \overset{ss}{\sim} \beta$ iff $\alpha = \beta$ in algebras of $\mathcal{V}$; whenever $\alpha \overset{s}{\sim} \beta$ in an algebra of $\mathcal{V}$, then α and β permute; $\mathcal{V}$ has a ternary term that satisfies Mal'cev's equations when restricted to an equivalence class of any solvable congruence.

The equivalent conditions of Theorem 7.12 define what turns out to be, in a precise sense, the largest proper Mal'cev class of locally finite varieties. The theorem itself is the principal tool used in Chapter 9 to investigate the connection between type sets and Mal'cev classes.

To simplify our discussion, it is convenient to define "Mal'cev class" in a slightly unusual way. By a *Mal'cev class* we shall mean any class of locally finite varieties consisting of all the varieties satisfying an ordinary Mal'cev condition defined by a set of linear equations which implies that the operations appearing in the equations are idempotent. (See Definition 9.1 for further explication. Nearly all of the Mal'cev conditions in the literature have this property.) A Mal'cev class is *proper* if it does not include every locally finite variety. In Chapter 9, we examine six Mal'cev classes, ordered by inclusion as in this picture. The notation "omit (S)", where S is a set of types, denotes the class of all locally finite varieties that omit all the types in S.



The six classes are defined by the omission of types, by variants of a congruence equation (see Theorem 9.6 (3)), and by various other equivalent conditions. (See Theorems 9.6, 9.8, 9.14, 9.10, 9.11, and 9.15 for the respective classes.)

$\mathcal{M}_1$ is the class of locally finite varieties satisfying the conditions of Theorem 7.12 and the equivalent conditions of Theorem 9.6. It is the largest proper Mal'cev class. The condition 9.6 (3) makes it clear that $\mathcal{M}_1$ is a Mal'cev class; and it is interesting to find that the largest proper Mal'cev class can be defined by relatively simple equations involving joins, meets, and compositions of congruences.

$\mathcal{M}_4$ is the class of varieties having no nontrivial Abelian congruences (or prime quotients of type **1** or **2**). It is also the class of varieties whose congruence lattices are meet semi-distributive; and it is the largest Mal'cev class not containing the variety of all vector spaces over any finite field. $\mathcal{M}_2$ is the largest Mal'cev class not containing the variety of semilattices; and we have $\mathcal{M}_5 = \mathcal{M}_2 \cap \mathcal{M}_4$.

$\mathcal{M}_2$ is defined by a very simple congruence equation (see 9.8 (3)), and it is quite large. Every locally finite variety whose congruence lattices obey a nontrivial equation in joins and meets belongs to $\mathcal{M}_2$.

$\mathcal{M}_3$ is the class of locally finite varieties $\mathcal{V}$ such that $\mathcal{V}$ has n-permuting congruences for some n. It is the largest Mal'cev class not containing the variety of distributive lattices. A surprising result is that for every $\mathcal{V}$ belonging to $\mathcal{M}_3$, there is a nontrivial equation in joins and meets that holds in the congruence lattice of each algebra in $\mathcal{V}$ (Theorem 9.19).

With the aid of tame congruence theory, we are able to extend all the results proved in [10] for congruence-modular varieties to every variety in $\mathcal{M}_2$. Every residually small variety in $\mathcal{M}_2$ is congruence-modular (Theorem 10.4). If $\mathcal{V}$ belongs to $\mathcal{M}_2$, then every two finite simple algebras in $\mathcal{V}$ that obey the same equations are isomorphic; and if $\mathbf{A} \in \boldsymbol{V}(\mathbf{B}) \subseteq \mathcal{V}$ and $\mathbf{B}$ is finite, then every block of a minimal congruence in $\mathbf{A}$ has cardinality no greater than the cardinality of $\mathbf{B}$ (Theorem 14.6).

In Chapter 11, we extend the results proved in [5] for congruence-modular varieties to every variety in $\mathcal{M}_1$. Every variety in $\mathcal{M}_1$ that fails to be congruence-modular is hereditarily undecidable.

In Chapter 12, we prove that if $\mathcal{V}$ is a variety in $\mathcal{M}_2$ which fails to have permuting congruences, or contains a finite non-nilpotent algebra, then for some constant $c > 0$ the free algebra $\mathbf{F}_{\mathcal{V}}(n)$ has at least $2^{2^{cn}}$ elements for all sufficiently large n.

In Chapters 13 and 14, we obtain a lot of new information about finite simple algebras. The five types of simple algebras possess distinctively different personalities. Simple algebras of the first two types are Abelian; a locally finite variety can contain only finitely many such algebras. Simple algebras of the fourth and fifth types possess connected partial orderings with respect to which all operations are monotone. A simple algebra of the third or fourth type "splits" any locally finite variety that contains it (Exercise 14.9 (1)).

Finally, we can mention Theorem 8.7. For every finite algebra $\mathbf{A}$ that generates a congruence-modular variety, there exists a finite algebra $\mathbf{B}$ such that the two algebras have isomorphic congruence lattices and the congruences of $\mathbf{B}$ permute; in fact, $\mathbf{B}$ is a loop with operators.

0. BASIC CONCEPTS AND NOTATION

This chapter can be quickly passed over by anyone familiar with modern universal algebra. The less familiar concepts and notations will be defined again in the text at their first occurrence. Occasionally, one may need to consult the index at the back of the book to find the place where a term has first been defined. For more complete treatments of the material of this chapter, one can consult the books by Grätzer, [14] and [15], for everything pertaining to algebras or lattices, and the book by Burris and Sankapannavar [4] for varieties.

0.1 ALGEBRAS. An algebra consists of a nonvoid set and some finitary operations over that set. For example, a group is a set of elements and a binary operation on those elements (or sometimes, a binary operation and a unary operation are used). We shall deal with two kinds of algebras, the indexed and the non-indexed. An *indexed algebra*, written usually as $\mathbf{A} = \langle A, f_i(i \in I)\rangle$, consists of a nonvoid set A of elements (the *base set* or *universe*) and a function $\langle f_i : i \in I\rangle$ whose values, f_i, are operations on $\mathbf{A}$. A *non-indexed algebra* is just a pair $\mathbf{A} = \langle A, F\rangle$, consisting of a nonvoid set A and a set F of operations on A. Both kinds of algebras are called, simply "algebras". The operations given, either the $f_i(i \in I)$, or the members of F, are called the *basic operations* of the algebra. Indexed algebras are preferable to non-indexed in many instances. For example, in speaking of a homomorphism between two rings, one may need to refer to the "addition operations" of both rings. (In our general framework, rings can be construed as algebras $\langle A, f_+, f_-, f_\cdot\rangle$, taking as index set for the operations $I = \{+, -, \cdot\}$.) On the other hand, non-indexed algebras arise frequently in the theory we shall develop, in situations where it is both inconvenient and unnecessary to make a list of the operations.

The n th Cartesian power of a set A, where n is a non-negative integer, is denoted A^n. Its elements are written as $\bar{x} = \langle x_0, \ldots, x_{n-1}\rangle$. By an n-ary operation on A, we mean any function $f : A^n \to A$. The only restriction we impose on an algebra is that its basic operations be *finitary*. This means that every basic operation f of an algebra whose universe is A must be an n-ary operation on A for some non-negative integer n. It is common practice to use the word "unary" instead of "1-ary", and to use "binary" to replace "2-ary".

By *composition of operations* we mean the construction of an n-ary operation, h, from k given n-ary operations $f_0, \ldots, f_{k-1}$ and a k-ary operation g, through the defining formula $h(\bar{x}) = g(f_0(\bar{x}), \ldots, f_{k-1}(\bar{x}))$. (All of these operations must be defined on the same set; while the non-negative integers k and n are arbitrary.) The *projection operations* on a set A are the trivial operations p_i^n satisfying $p_i^n(x_0, \ldots, x_{n-1}) = x_i$. A *clone* on a set A is a set of operations on A that is closed under all compositions and contains the projections p_i^n (for all n and i satisfying $0 \leq i < n$).

There are two important sets of derived operations in any algebra $\mathbf{A}$. One is the *clone of polynomial operations of* $\mathbf{A}$ denoted Pol $\mathbf{A}$. It is the close on A generated by the basic operations of A together with all of the constant 0-ary operations on A (and the projection operations, of course). The set of n-ary operations in this clone is denoted by $\mathrm{Pol}_n\mathbf{A}$. The other is the *clone of* (so-called) *term operations* of $\mathbf{A}$, denoted Clo $\mathbf{A}$. It is the clone on A generated by the basic operations of $\mathbf{A}$. To illustrate these definitions, let $\mathbf{A} = \langle \{0,1\}, + \rangle$ be the 2-element group, with $1+1=0$. Here $\mathrm{Clo}_2\mathbf{A}$ consists of the four operations

$$f(x,y) = x,\ y,\ x+y, \quad \text{and} \quad 0\ \ (= x+x)\ .$$

$\mathrm{Pol}_2\,\mathbf{A}$ has eight operations, the term operations just listed, plus

$$f(x,y) = x+1,\ y+1,\ x+y+1 \quad \text{and} \quad 1\ .$$

If f is an $m+n$-ary term operation of $\mathbf{A}$ and $\alpha = \langle \alpha_0, \ldots, \alpha_{m-1} \rangle \in A^m$, then the formula

$$g(\bar{x}) = f(\bar{\alpha}, \bar{x}) \quad (= f(\alpha_0, \ldots, \alpha_{m-1}, x_0, \ldots, x_{n-1}))$$

defines an n-ary polynomial operation of $\mathbf{A}$. Conversely, every n-ary polynomial operation of $\mathbf{A}$ arises in this way, through substitution of constants for some of the variables in some term operation of $\mathbf{A}$. By a *polynomial clone* on A, we mean a clone on A containing all the constant operations. Thus Pol $\mathbf{A}$ is the polynomial clone generated by Clo $\mathbf{A}$.

Let $\mathbf{A}$ be any algebra, U be a nonvoid subset of the universe of $\mathbf{A}$, and f be a polynomial operation of $\mathbf{A}$ such that U is closed under f. Then the restriction of f to U, or $f|_U$, is obviously an operation on U. By $(\mathrm{Pol}\,\mathbf{A})|_U$ we denote the set of all those $f|_U$ where $f \in \mathrm{Pol}\,\mathbf{A}$ and U is closed under f. The non-indexed algebra $\langle U, (\mathrm{Pol}\,\mathbf{A})|_U \rangle$ will be called the *algebra induced by* $\mathbf{A}$ *on* U and we shall denote it by $\mathbf{A}|_U$. These induced algebras play a cardinal role in this book. Notice that

$$\mathrm{Clo}\,(\mathbf{A}|_U) = \mathrm{Pol}\,(\mathbf{A}|_U) = (\mathrm{Pol}\,\mathbf{A})|_U\ ;$$

i.e., every polynomial operation of this algebra is already a basic operation.

Indexed algebras $\mathbf{A} = \langle A, f_i (i \in I) \rangle$ and $\mathbf{B} = \langle B, g_i (i \in I) \rangle$ are called *similar* iff they have the same index set I, and f_i and g_i are of equal arity for all $i \in I$. For

indexed algebras, the basic notions of *subalgebra* of an algebra, of *homomorphism* or *isomorphism* between two similar algebras, and of (*Cartesian*) *product* of a system of similar algebras are so well known that we shall not bother to define them carefully. We write $\mathbf{A} \subseteq \mathbf{B}$ for "$\mathbf{A}$ is a subalgebra of $\mathbf{B}$", and $f : \mathbf{A} \to \mathbf{B}$ for "f is a homomorphism of $\mathbf{A}$ into $\mathbf{B}$". The expression $\prod\{\mathbf{A}_t : t \in T\}$ denotes the algebra which is the Cartesian product of a system $\langle \mathbf{A}_t : t \in T \rangle$. To denote that $\mathbf{A}$ is isomorphic to $\mathbf{B}$ we write $\mathbf{A} \cong \mathbf{B}$. A *subuniverse* of $\mathbf{A}$ is a subset closed under all the operations of $\mathbf{A}$. We will sometimes confuse subalgebras with nonvoid subuniverses, when no ambiguity is likely to result.

For non-indexed algebras $\mathbf{A} = \langle A, F \rangle$ and $\mathbf{B} = \langle B, G \rangle$, the nomenclature and notation of homomorphism and isomorphism will be used with the following meanings. Let $f : A \to B$. We call f a homomorphism (or isomorphism, respectively) iff the basic operations can be indexed, $F = \{f_i : i \in I\}$ and $G = \{g_i : i \in I\}$, in such a way that $\langle A, f_i(i \in I) \rangle$ and $\langle B, g_i(i \in I) \rangle$ are similar and f is a homomorphism (an isomorphism) between these indexed algebras.

When X is a subset of an algebra $\mathbf{A}$ (i.e., a subset of the universe of $\mathbf{A}$), then the smallest set containing X and closed under the basic operations (i.e., the *subuniverse of* $\mathbf{A}$ *generated by* X) is obtained by applying $\mathrm{Clo}\,\mathbf{A}$ to X. It is the set

$$\overline{X} = \{f(x_0, \ldots, x_{n-1}) : f \in \mathrm{Clo}_n\mathbf{A} \quad \text{and} \quad \{x_0, \ldots, x_{n-1}\} \subseteq X \quad \text{and } n \text{ is arbitrary}\} .$$

If $\mathbf{B} = \prod\{\mathbf{A}_t : t \in T\}$ with $\mathbf{A}_t = \langle A_t, f_{it}(i \in I) \rangle$, and $\mathbf{B} = \langle B, g_i(i \in I) \rangle$, then the operation g_i of $\mathbf{B}$ is the operation on B which "acts coordinate-wise" and "acts like f_{it} in the t-th coordinate," for all t. Of special interest is the case where $\mathbf{A}_t = \mathbf{A} = \langle A, f_i\,(i \in I) \rangle$ for all t, i.e., where $\mathbf{B} = \mathbf{A}^T$ is a Cartesian power of the algebra $\mathbf{A}$. The universe of $\mathbf{A}^T$ is of course the set A^T of all functions from T into the universe of $\mathbf{A}$. Suppose that the i th operation of $\mathbf{A}$ is n-ary and that $h_0, \ldots, h_{n-1} \in A^T$. Then the i th operation of $\mathbf{A}^T$, when applied to $h_0, \ldots, h_{n-1}$, gives the result

$$g_i(h_0, \ldots, h_{n-1}) = h \in A^T$$

with h defined by

$$h(t) = f_i(h_0(t), \ldots, h_{n-1}(t)) .$$

If, in the above, $T = A^n$ then $\mathrm{Clo}_n\mathbf{A}$ is a subset of A^T; and in fact it can easily be shown that $\mathrm{Clo}_n\mathbf{A}$ is identical with the subuniverse of $\mathbf{A}^{A^n}$ generated by the n projections. Similarly, $\mathrm{Pol}_n\mathbf{A}$ is identical with the subuniverse of $\mathbf{A}^{A^n}$ generated by the projections and all the constant n-ary operations on $\mathbf{A}$.

We adopt a convention used in logic and set theory, and identify each natural number n with the set $\{0, \ldots, n-1\}$ of all smaller natural numbers. Then A^n denotes

a set of functions (n-tuples of elements of A), and $\mathbf{A}^n$ denotes the n th direct power of the algebra $\mathbf{A}$. We use the Greek letter ω to denote the set of all natural numbers.

By an n-ary relation on a set A, we mean a subset of A^n. For binary relations σ and ρ on A, the *converse* of σ is the relation

$$\sigma^{\cup} = \{\langle y, x\rangle : \langle x, y\rangle \in \sigma\} .$$

and the *relational product* of σ and ρ is

$$\sigma \circ \rho = \{\langle x, z\rangle : \exists y(\langle x, y\rangle \in \sigma \quad \text{and} \quad \langle y, z\rangle \in \rho)\} .$$

The relation $\{\langle x, x\rangle : x \in A\}$ is at once the identity function on A, denoted id_A, and the least equivalence relation on A (see below). When it plays the second role, we denote it by 0_A. (The largest equivalence relation on A is $1_A = A^2$.) A binary relation σ on A is called *reflexive over* A iff $\sigma \supseteq \mathrm{id}_A$; *symmetric* iff $\sigma = \sigma^{\cup}$; *transitive* iff $\sigma \supseteq \sigma \circ \sigma$. The *transitive closure* of a binary relation σ is the smallest transitive relation including σ; it is identical with the set $\cup\{\sigma^n : n \geq 1\}$, where $\sigma^1 = \sigma$ and, inductively, $\sigma^{k+1} = \sigma^k \circ \sigma$.

By an n-ary *admissible relation* of an indexed algebra $\mathbf{A}$ we mean a subuniverse of $\mathbf{A}^n$. Thus an n-ary relation ρ is admissible for $\mathbf{A}$ iff $\rho \subseteq A^n$ and ρ is closed (or admissible) under all the operations of $\mathbf{A}$ acting co-ordinatewise. (For "operation" read either "basic operation" or "term operation"; it will not change the concept defined.) Phrased in this way, the concept of admissible relation makes sense for both kinds of algebra, indexed and non-indexed. Note that an admissible binary relation of $\mathbf{A}$ is reflexive over A iff it is admissible for the polynomial operations, as well as for the term operations, of $\mathbf{A}$.

Two types of admissible relations play a large role in this book. A *tolerance* of $\mathbf{A}$ is an admissible binary relation that is symmetric and reflexive over the universe of $\mathbf{A}$. A *congruence* of $\mathbf{A}$ is a transitive tolerance of $\mathbf{A}$, i.e., an admissible equivalence relation.

Notation for equivalence relations: Π_A denotes the set of all equivalence relations (reflexive, symmetric, transitive binary relations) on A. If $\sigma \in \Pi_A$ and $x, y \in A$, then $x \equiv y \pmod{\sigma}$ means that $\langle x, y\rangle \in \sigma$. We put $x/\sigma = \{z : \langle x, z\rangle \in \sigma\}$. Given an equivalence relation σ, the set $A/\sigma = \{x/\sigma : x \in A\}$ is a *partition* of A; that is, $A = \cup\{x/\sigma : x \in A\}$ and for all x and y we have $x/\sigma \cap y/\sigma = \emptyset$ or $x/\sigma = y/\sigma$. The elements of A/σ are called *equivalence classes* (sometimes, *blocks*) of σ.

Quotient algebras: If an n-ary operation f on A preserves an equivalence relation $\sigma \in \Pi_A$, i.e., if σ is a congruence of the algebra $\langle A, f\rangle$, then an operation f_σ is defined on A_σ by the formula

$$f_\sigma(x_0/\sigma, \ldots, x_{n-1}/\sigma) = f(x_0, \ldots, x_{n-1})/\sigma .$$

Thus if $\mathbf{A} = \langle A, f_i\,(i \in I)\rangle$ (or $\mathbf{A} = \langle A, F\rangle$) is an algebra and σ is a congruence of $\mathbf{A}$, then we have an algebra $\mathbf{A}/\sigma = \langle A/\sigma, f_{i\sigma}\,(i \in I)\rangle$ (or $\mathbf{A}/\sigma = \langle A/\sigma, \{f_\sigma : f \in F\}\rangle$). The mapping π_σ that takes x to x/σ is a homomorphism of $\mathbf{A}$ onto $\mathbf{A}/\sigma$ in either case. $\mathbf{A}/\sigma$ is called the *quotient* of $\mathbf{A}$ by the congruence σ. Whenever we have a homomorphism $\pi : \mathbf{A} \to \mathbf{B}$, then $\ker\pi = \{\langle x, y\rangle \in A^2 : \pi x = \pi y\}$ is a congruence of $\mathbf{A}$. This congruence is called the kernel of π, and we have $\mathbf{B} \cong \mathbf{A}/\ker\pi$ if π is onto B. The congruences of $\mathbf{A}$ are the same as the kernels of the homomorphisms from $\mathbf{A}$.

Two algebras, $\mathbf{A} = \langle A, \dots\rangle$ and $\mathbf{B} = \langle B, \dots\rangle$, are called *polynomially equivalent* iff they have the same universe and precisely the same polynomial operations, i.e., $A = B$ and $\mathrm{Pol}\,\mathbf{A} = \mathrm{Pol}\,\mathbf{B}$. It is easy to show that the algebras $\mathbf{A}, \langle A, \mathrm{Clo}\,\mathbf{A}\rangle$, $\langle A, \mathrm{Pol}\,\mathbf{A}\rangle$, and $\langle A, \mathrm{Pol}_1\mathbf{A}\rangle$, have the property that any $\theta \in \Pi_A$ is a congruence of one of these algebras iff it is a congruence of all of them. (This is true for every $\mathbf{A}$.) Each of the first three of these algebras is polynomially equivalent to $\mathbf{A}$.

0.2 LATTICES. A *po-set* (*partially ordered set*) is a nonvoid set A together with a binary relation ρ on A satisfying $\rho \circ \rho \subseteq \rho$, $\rho \cap \rho^{\cup} = \mathrm{id}_A$. The binary relation (partial ordering) of a po-set is usually denoted as $\leq$. We use the notation $x < y$ ($x \leq y$ and $x \neq y$), and $x \prec y$ (y *covers* x, which means that $x < y$ and for no z does $x < z < y$ hold). Finite po-sets can be pictured in *Hasse diagrams*, with the elements depicted as points on a plane, larger elements corresponding to higher points, and the covering relation represented by ascending straight line segments. Here are some Hasse diagrams.

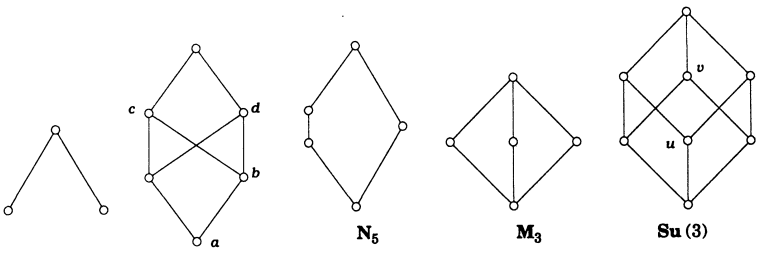


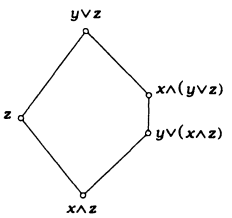
Figure 0

The rule for decoding Hasse diagrams is that $x \leq y$ iff one can get from point x to point y by following ascending line segments between points. Turns of direction are allowed only at the points. Thus in the last diagram of the figure, $u \not\leq v$. The elements u and v in the diagram are *incomparable*, that is, neither $u \leq v$ nor $v \leq u$ holds. In the second diagram of Figure 0, $a \prec b \prec c$ and thus $a < c$.

A *lattice* is an algebra $\langle A, \vee, \wedge \rangle$ with two binary operations such that for some partial ordering $\leq$ of A, the formulas $(x \vee y \leq z) \leftrightarrow (x \leq z \text{ and } y \leq z)$ and $(z \leq x \wedge y) \leftrightarrow (z \leq x \text{ and } z \leq y)$ are valid for all elements x, y, and z. Each of the operations of a lattice, $\vee$ (called *join*) and $\wedge$ (called *meet*), determines $\leq$ uniquely, and thus each operation determines the other. A po-set $\langle A, \leq \rangle$ is correlated with a lattice in this fashion if and only if every pair of elements of A have a least upper bound and a greatest lower bound in A (with respect to $\leq$).

The final three diagrams in Figure 0 are Hasse diagrams of lattices, the first two are not. $\mathbf{Su}(3)$ is our name for the lattice of subsets of a three-element set.

Lattices are algebras, and so we can speak of their subalgebras, homomorphisms and congruences. The *modular law* is the equation $x \wedge ((x \wedge y) \vee z) = (x \wedge y) \vee (x \wedge z)$. A lattice which satisfies this as an identity, i.e., for all choices of elements x, y, and z, is called *modular*. A lattice $\mathbf{L}$ is modular iff in $\mathbf{L}$, $y \leq x$ implies $x \wedge (y \vee z) = y \vee (x \wedge z)$. The lattice $\mathbf{N}_5$ is nonmodular (Figure 0), and every lattice having a sublattice isomorphic to $\mathbf{N}_5$ is nonmodular. Conversely, if $\mathbf{L}$ is nonmodular then it has a sublattice isomorphic to $\mathbf{N}_5$. For suppose $y < x$ and $x \wedge (y \vee z) \neq y \vee (x \wedge z)$. It is then easily verified that this is a sublattice of L isomorphic to $\mathbf{N}_5$:



The *distributive law* for lattices is the equation $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. Lattices satisfying this as an identity are called *distributive*. (Exercise: A modular lattice is distributive iff it has no sublattice isomorphic to the lattice $\mathbf{M}_3$ in Figure 0.)

Set inclusion is a lattice ordering of the set Π_A of all equivalence relations on a set A. In the lattice $\mathbf{\Pi}_A = \langle \Pi_A, \vee, \wedge \rangle$, called the *full partition lattice* over A, the join of two equivalence relations is the transitive closure of their set union, and the meet of two equivalence relations is simply their intersection.

Congruence lattices: For any algebra $\mathbf{A}$, $\mathrm{Con}\,\mathbf{A}$ denotes the set of all congruence relations of $\mathbf{A}$. It is closed under the join and meet in $\mathbf{\Pi}_A$, and so we have a lattice $\mathbf{Con\,A} = \langle \mathrm{Con}\,A, \vee, \wedge \rangle$, called the *congruence lattice* of $\mathbf{A}$. This lattice is *complete*, in fact, it is a *complete sublattice* of $\mathbf{\Pi}_A$. That is to say, for any set X of congruences on $\mathbf{A}$, the join or least upper bound of X, and the meet or greatest lower bound of

X, exist in $\mathbf{Con}\,\mathbf{A}$, and these joins and meets are the same as in $\mathbf{\Pi}_A$. The join and meet of X are written as $\bigvee X$ and $\bigwedge X$.

We write $\Theta(T)$ for the congruence generated by a set $T \subseteq A^2$. If $T = \{\langle a, b\rangle\}$, we write instead $\Theta(a, b)$. $\Theta(T)$ is the transitive closure of the relation

$$\mathrm{id}_A \cup \{\langle f(a), f(b)\rangle : f \in \mathrm{Pol}_1\,\mathbf{A} \text{ and } \langle a, b\rangle \in T \text{ or } \langle b, a\rangle \in T\}.$$

The *finitely generated congruences* of $\mathbf{A}$ are those of the form $\Theta(T)$ where T is a finite subset of A^2. By a *compact* element of a complete lattice $\mathbf{L}$ is meant an element c for which $c \leq \bigvee X$ always implies the existence of a finite set $X' \subseteq X$ with $c \leq \bigvee X'$. It is easy to see that the compact elements of $\mathbf{Con}\,\mathbf{A}$ are precisely the finitely generated congruences.

A lattice $\mathbf{L}$ is called *algebraic* if and only if $\mathbf{L}$ is complete and every element of $\mathbf{L}$ is the join of a set of compact elements of $\mathbf{L}$. The nomenclature is justified by a classical theorem of G. Grätzer and E.T. Schmidt: A lattice $\mathbf{L}$ is algebraic iff for some algebra $\mathbf{A}$, $\mathbf{L} \cong \mathbf{Con}\,\mathbf{A}$. Every finite lattice is algebraic. The Grätzer-Schmidt proof produces in nearly every case an infinite algebra; and it is not known if every finite lattice is isomorphic to $\mathbf{Con}\,\mathbf{A}$ for some finite algebra $\mathbf{A}$.

Simple and subdirectly irreducible algebras: An algebra $\mathbf{A}$ is called *simple* iff $\mathbf{Con}\,\mathbf{A}$ is a two-element lattice. This holds iff $\mathbf{A}$ has at least two elements and every homomorphism $f : \mathbf{A} \to \mathbf{B}$ is one-to-one or constant. (Exercise: The lattice $\mathbf{M}_3$ of Figure 0 is a simple algebra.) An algebra $\mathbf{A}$ is called *subdirectly irreducible* iff $\mathbf{Con}\,\mathbf{A}$ has an element $\beta \neq 0_A$ such that every congruence δ satisfies $\delta \geq \beta \leftrightarrow \delta \neq 0_A$. Thus $\mathbf{A}$ is subdirectly irreducible iff it has elements $a \neq b$ such that every homomorphism $f : \mathbf{A} \to \mathbf{B}$ is either one-to-one or has $f(a) = f(b)$. The least non-zero congruence β of a subdirectly irreducible algebra $\mathbf{A}$ is called the *monolith* of $\mathbf{A}$.

We say that $\mathbf{A}$ is a *subdirect product* of a system of algebras $\langle \mathbf{B}_i : i \in I\rangle$, symbolically $\mathbf{A} \overset{\mathrm{sd}}{\leq} \prod\{\mathbf{B}_i : i \in I\}$, if $\mathbf{A}$ is a subalgebra of the product and the coordinate homomorphism $p_i : \mathbf{A} \to \mathbf{B}_i$ is onto $\mathbf{B}_i$ for each and every i. It is not hard to see that an algebra $\mathbf{A}$ is subdirectly irreducible iff for every one-to-one homomorphism $\varphi : \mathbf{A} \to \prod\{\mathbf{B}_i : i \in I\}$ of $\mathbf{A}$ into a product, there exists i for which $p_i\varphi : \mathbf{A} \to \mathbf{B}_i$ is injective—in other words, iff $\mathbf{A}$ is not isomorphic in a non-trivial way to a subdirect product.

For any two elements $a \leq b$ in a lattice $\mathbf{L}$, we have the interval

$$I[a, b] = \{x \in L : a \leq x \leq b\},$$

which is a sublattice of $\mathbf{L}$. If $\varphi : \mathbf{A} \twoheadrightarrow \mathbf{B}$ is onto $\mathbf{B}$, and $\theta = \ker\varphi$, then we have an isomorphism φ^{-1} of $\mathbf{Con}\,\mathbf{B}$ with the interval sublattice $I[\theta, 1_A]$ in $\mathbf{Con}\,\mathbf{A}$, defined by $\varphi^{-1}(\alpha) = \{\langle x, y\rangle \in A^2 : \langle\varphi(x), \varphi(y)\rangle \in \alpha\}$. Thus, in fact, for any congruence δ of $\mathbf{A}$, $\mathbf{Con}\,(\mathbf{A}/\delta) \cong I[\delta, 1_A]$. This is a generalization of one of the isomorphism theorems

of group theory. Using this fact, one may prove G. Birkhoff's *subdirect representation theorem*, which states that for any algebra $\mathbf{A}$, there is a set $\{\theta_i : i \in I\} \subseteq \mathbf{Con}\,\mathbf{A}$ (with I empty if $\mathbf{A}$ has only one element) such that $\mathbf{A}/\theta_i$ is subdirectly irreducible for each i, and $x \mapsto \langle x/\theta_i : i \in I\rangle$ is an isomorphism of $\mathbf{A}$ with a subdirect product of $\langle \mathbf{A}/\theta_i : i \in I\rangle$. (Let $I = A^2 - \mathrm{id}_A$ and for each $i = \langle a, b\rangle \in I$, let θ_i be a maximal member of the set $\{\delta \in \mathrm{Con}\,\mathbf{A} : \langle a, b\rangle \notin \delta\}$.)

0.3 VARIETIES. To come to terms with the wild diversity of form and character exhibited by algebras, it is desirable to group them into classes according to some scheme. One way to do this has proved so fruitful that it has no serious competitor. That is to group algebras into classes defined by equations. The basic classes in this scheme are called varieties. It is probably no accident that the first really broad classes of algebras to be studied systematically were varieties such as the class of groups, the class of rings, and the class of Lie algebras.

To give a completely adequate and precise introduction to the elementary theory of varieties would require more space than we are willing to commit here. We shall discuss varieties briefly and depend on the reader to supplement our remarks by a reading of Chaper II, §9-§11 in [4], if this subject has not been met before.

By a *language* we shall mean an ordered triple $L = \langle I, F, \sigma\rangle$ consisting of a set I, a one-to-one function $F = \langle f_i : i \in I\rangle$ (whose values, f_i, will be called *operation symbols*), and a function $\sigma = \langle \sigma_i : i \in I\rangle$ whose values are non-negative integers. A *model* of L, or *L-algebra*, is any algebra $\mathbf{A} = \langle A, f_i^{\mathbf{A}}(i \in I)\rangle$ in which $f_i^{\mathbf{A}}$ is a σ_i-ary operation on $\mathbf{A}$ for each i. For any nonvoid set X, there is an L-algebra $\mathbf{F}_L(X)$, generated by X, having the property that every mapping φ of X into any L-algebra $\mathbf{A}$ has a unique extension $\hat{\varphi}$ which is a homomorphism of $\mathbf{F}_L(X)$ into $\mathbf{A}$. $\mathbf{F}_L(X)$ is called the *free L-algebra, freely generated by X*. It is determined up to isomorphism by X; in fact, if $\mathbf{F}_L(X)$ and $\mathbf{F}'_L(X)$ both satisfy the conditions laid down above, then these algebras are isomorphic by an isomorphism which leaves fixed each element of X.

A *term* in the language L, or *L-term*, is simply a member of $\mathbf{F}_L(X)$ for some finite set X. Terms belonging to $\mathbf{F}_L(x_1, \ldots, x_k)$ (where $x_1, \ldots, x_k$ are assumed distinct) will be written as $t(x_1, \ldots, x_k)$. Let $t = t(x_1, \ldots, x_k)$ be such a term. Given elements $a_1, \ldots, a_k$ in an L-algebra $\mathbf{A}$, we define $t^{\mathbf{A}}(a_1, \ldots, a_k)$ to be the element $\varphi(t)$ where φ is the homomorphism of $\mathbf{F}_L(x_1, \ldots, x_k)$ into $\mathbf{A}$ with $\varphi(x_1) = a_1, \ldots, \varphi(x_k) = a_k$. This defines a k-ary operation $t^{\mathbf{A}}$ on the universe of $\mathbf{A}$, corresponding to the term $t(x_1, \ldots, x_k)$. (A fixed ordered list of the free generators $x_1, \ldots, x_k$ is required, in order to determine $t^{\mathbf{A}}$ precisely.) An operation in the algebra $\mathbf{A}$ that can be defined in this way, from some L-term, is called a term operation of $\mathbf{A}$. It is not hard to see that the set of all term operations of $\mathbf{A}$ is identical with the clone $\mathrm{Clo}\,\mathbf{A}$ which we defined earlier.

A formal equation in the language L, or *L-equation*, is an ordered pair of terms, both of which are members of the same free algebra. Formal equations are written in the form $s(x_1, \ldots, x_k) \approx t(x_1, \ldots, x_k)$. Such an equation is said to be an *identity* of an L-algebra $\mathbf{A}$ iff $s^{\mathbf{A}} = t^{\mathbf{A}}$. (Equivalent expressions: "$\mathbf{A}$ obeys $s \approx t$" ($x_1, \ldots, x_k$ are understood), "$\mathbf{A}$ satisfies $s \approx t$ identically", "$s \approx t$ holds in $\mathbf{A}$", "$\mathbf{A} \models s \approx t$".) When speaking of equations, the free generators $x_1, \ldots, x_k$ are called *variables.*

If Σ is any set of L-equations (in various finite sets of variables), the class of all algebras in which every member of Σ is an identity will be denoted by $\mathrm{Mod}(\Sigma)$ (the *class of models of* Σ). Classes of the form $\mathrm{Mod}(\Sigma)$ are called *varieties.* Every variety comes with a language attached; its members are similar algebras—all of them models for that language.

It is quite clear that the class of all groups, construed as models of a language with one binary operation symbol, $\cdot$, and one unary operation symbol, $^{-1}$, is a variety. The class of all lattices is a variety. We choose a language L with two binary operation symbols, $\vee$ and $\wedge$, and write some equations using terms in $\mathbf{F}_L(x, y, z)$:

$$x \vee x \approx x, \qquad x \vee y \approx y \vee x$$
$$(x \vee y) \vee z \approx x \vee (y \vee z)$$

[the equations obtained by replacing $\vee$ by $\wedge$ in the above]

$$x \vee (x \wedge y) \approx x, \qquad x \wedge (x \vee y) \approx x\ .$$

It is not hard to see that these equations define the class of lattices; i.e., an algebra $\langle A, \vee, \wedge \rangle$ is a lattice if and only if it obeys the above equations. For any ring $\mathbf{R}$ with unit, the class of left unitary $\mathbf{R}$-modules can be construed as a variety in a rather obvious fashion. The language should have a binary and a unary operation symbol, $+$ and $-$, and one unary symbol f_λ for scalar multiplication, for each $\lambda \in R$.

For any class $\mathcal{K}$ of similar algebras (models of one language), $\boldsymbol{H}\mathcal{K}$, $\boldsymbol{S}\mathcal{K}$, and $\boldsymbol{P}\mathcal{K}$ denote the class of all algebras that are, respectively, homomorphic images of algebras in $\mathcal{K}$, isomorphic to a subalgebra of an algebra in $\mathcal{K}$, or isomorphic to a product of algebras in $\mathcal{K}$. According to the HSP-theorem of G. Birkhoff, a class $\mathcal{K}$ of similar algebras is a variety iff $\mathcal{K} = \boldsymbol{HSP}\mathcal{K}$; and the smallest variety containing a class $\mathcal{K}$ of similar algebras is $\boldsymbol{V}(\mathcal{K}) = \boldsymbol{HSP}\mathcal{K}$.

Free algebras in varieties: Let L be a language and let $\mathcal{K}$ be a nontrivial class of L-algebras (one which contains an algebra with at least two elements). For any non-void set X there exists an algebra, $\mathbf{F}_{\mathcal{K}}(X)$, generated by X, such that $\mathbf{F}_{\mathcal{K}}(X) \in \boldsymbol{SP}\mathcal{K}$ and every mapping of X into an algebra of $\mathcal{K}$ (or of $\boldsymbol{SP}\mathcal{K}$) extends to a homomorphism of $\mathbf{F}_{\mathcal{K}}(X)$ into that algebra. Where φ is the homomorphism of $\mathbf{F}_L(X)$ onto $\mathbf{F}_{\mathcal{K}}(X)$ extending the identity map on X, the kernel of φ is

$$\theta_{\mathcal{K}} = \bigcap \{\ker f \mid f : \mathbf{F}_L(X) \to \mathbf{A} \quad \text{for some} \quad \mathbf{A} \in \mathcal{K}\}\ ,$$

and $\mathbf{F}_{\mathcal{K}}(X) \cong \mathbf{F}_L(X)/\theta_{\mathcal{K}}$. One proof of Birkhoff's theorem proceeds by noting that if $\mathbf{A}$ obeys all of the equations that hold in $\mathcal{K}$, then for large X there is a homomorphism f of $\mathbf{F}_L(X)$ onto $\mathbf{A}$ and $\ker f \supseteq \theta_{\mathcal{K}}$; thus $\mathbf{A} \in \boldsymbol{H}(F_{\mathcal{K}}(X)) \subseteq \boldsymbol{HSP}\mathcal{K}$.

Now let $\mathcal{V}$ be a nontrivial variety of L-algebras. For each nonvoid set X, $\mathbf{F}_{\mathcal{V}}(X)$ belongs to $\mathcal{V}$; it is called the *free algebra in* $\mathcal{V}$, *freely generated by* X. Elements of the finitely generated free algebras in $\mathcal{V}$ are called $\mathcal{V}$-terms. Every $\mathcal{V}$-term $t(x_1, \ldots, x_n)$ gives rise to a term operation $t^{\mathbf{A}}$ in each algebra $\mathbf{A}$ of $\mathcal{V}$. The kernel of the homomorphism $\mathbf{F}_L(x_1, \ldots, x_n) \to \mathbf{F}_{\mathcal{V}}(x_1, \ldots, x_n)$ is equal to the set of equations in the variables $x_1, \ldots, x_n$ that hold as identities in $\mathcal{V}$. If $\mathbf{C}$ is an algebra such that $\mathcal{V} = \boldsymbol{V}(\mathbf{C})$, then the map $t(x_1, \ldots, x_n) \to t^{\mathbf{C}}$ is an isomorphism between $\mathbf{F}_{\mathcal{V}}(x_1, \ldots, x_n)$ and the subalgebra of $\mathbf{C}^{C^n}$ whose universe is $\mathrm{Clo}_n\mathbf{C}$.

We close this chapter by proving three simple but important theorems about varieties. An algebra $\mathbf{A}$ is said to be *locally finite* iff every subalgebra of $\mathbf{A}$ generated by finitely many elements is finite. We call a variety $\mathcal{V}$ *locally finite* iff every algebra in $\mathcal{V}$ is locally finite, or equivalently, every finitely generated algebra in $\mathcal{V}$ is finite. We say that $\mathcal{V}$ is *finitely generated* iff it has the form $\boldsymbol{V}(\mathbf{A}_1, \ldots, \mathbf{A}_n)$ $(= \boldsymbol{V}(\mathbf{A}_1 \times \cdots \times \mathbf{A}_n))$ where n is some positive integer and each of $\mathbf{A}_1, \ldots, \mathbf{A}_n$ is a finite algebra. The free algebra $\mathbf{F}_{\mathcal{V}}(x_1, \ldots, x_k)$ in $\mathcal{V}$, freely generated by k distinct elements, will be denoted simply by $\mathbf{F}_{\mathcal{V}}(k)$.

THEOREM 0.1. *Let $\mathcal{V}$ be any variety.*

(1) *$\mathcal{V}$ is locally finite iff $\mathbf{F}_{\mathcal{V}}(k)$ is finite for all $1 \leq k < \omega$.*

(2) *If $\mathcal{V}$ is finitely generated than it is locally finite. In fact, if $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$ for a finite algebra $\mathbf{A}$ then, for each $k < \omega$, $\mathbf{F}_{\mathcal{V}}(k) \in \boldsymbol{S}(\mathbf{A}^n)$ for some $n < \omega$.*

PROOF. To prove (1) we simply note that $\mathbf{F}_{\mathcal{V}}(k)$ is finitely generated (if k is finite) and every finitely generated algebra in $\mathcal{V}$ is in $\boldsymbol{H}(\mathbf{F}_{\mathcal{V}}(k))$ for some $k < \omega$.

To prove (2), let $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$ where $|\mathbf{A}| = m$. Given any k, $1 \leq k < \omega$, we recall that $t(x_1, \ldots, x_k) \mapsto t^{\mathbf{A}}$ is an isomorphism of $\mathbf{F}_{\mathcal{V}}(k)$ onto the subalgebra of $\mathbf{A}^{A^k}$ with universe $\mathrm{Clo}_k\mathbf{A}$. Thus $\mathbf{F}_{\mathcal{V}}(k) \in \boldsymbol{S}(\mathbf{A}^n)$, where $n = m^k$. □

For any class $\mathcal{K}$, $\boldsymbol{P}_{fin}\mathcal{K}$ denotes the class of algebras isomorphic to a product $\mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ for some finite n, where $\{\mathbf{A}_1, \ldots, \mathbf{A}_n\} \subseteq \mathcal{K}$.

THEOREM 0.2. *If $\mathcal{V} = \boldsymbol{V}(\mathbf{A}_1, \ldots, \mathbf{A}_m)$ and $\mathbf{A}_1, \ldots, \mathbf{A}_m$ are finite, then every finite algebra in $\mathcal{V}$ belongs to the class $\boldsymbol{HSP}_{fin}(\mathbf{A}_1, \ldots, \mathbf{A}_m)$.*

PROOF. Let $\mathbf{A} = \mathbf{A}_1 \times \cdots \times \mathbf{A}_m$. Let $\mathbf{B}$ be any finite algebra in $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$, say $|\mathbf{B}| = k$. By Theorem 0.1 (2), $\mathbf{F}_{\mathcal{V}}(k) \in \boldsymbol{SP}_{fin}(\mathbf{A}) \subseteq \boldsymbol{SP}_{fin}(\mathbf{A}_1, \ldots, \mathbf{A}_m)$. Since $\mathbf{B} \in \boldsymbol{H}(\mathbf{F}_{\mathcal{V}}(k))$, the proof is finished. □

The third statement in the next theorem was proved by A. I. Mal'cev around 1954. Two equivalence relations, σ and τ, on a set A are said to be *permuting* iff $\sigma \circ \tau = \tau \circ \sigma$.

THEOREM 0.3.

(1) *If σ and τ are permuting equivalence relations on a set A then $\sigma \circ \tau = \sigma \vee \tau$ (the join in Π_A).*

(2) *If $\mathbf{A}$ is an algebra with permuting congruences (every two congruences permute) then $\mathbf{Con}\,\mathbf{A}$ is a modular lattice.*

(3) *A variety $\mathcal{V}$ has permuting congruences (every algebra in $\mathcal{V}$ has permuting congruences) iff there is a ternary term $t(x,y,z)$ in the language of $\mathcal{V}$ such that the equations $t(x,x,y) \approx y$, $t(x,y,y) \approx x$ are identities in $\mathcal{V}$ (Mal'cev's equations).*

PROOF. To prove (1) we simply note that

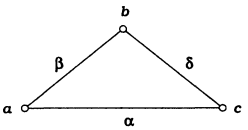
$$\sigma \vee \tau = \bigcup\{(\sigma \cup \tau)^n : 1 \leq n < \omega\} = \cup\{\sigma \circ \tau)^n : 1 \leq n < \omega\}.$$

Thus if $\sigma \circ \tau = \tau \circ \sigma$, we have

$$(\sigma \circ \tau)^2 = \sigma \circ \tau \circ \sigma \circ \tau = \sigma \circ \sigma \circ \tau \circ \tau = \sigma \circ \tau,$$

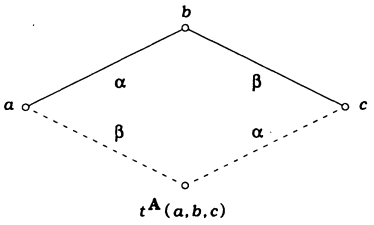
and so $(\sigma \circ \tau)^n = \sigma \circ \tau$ for all n.

To prove (2), suppose that the congruences of $\mathbf{A}$ permute, and let $\alpha, \beta, \delta \in \mathrm{Con}\,\mathbf{A}$ with $\beta \leq \alpha$. It must be shown that $\alpha \wedge (\beta \vee \delta) = \beta \vee (\alpha \wedge \delta)$, or equivalently, that $\alpha \wedge (\beta \vee \delta) \leq \beta \vee (\alpha \wedge \delta)$. Let $\langle a, c\rangle \in \alpha \wedge (\beta \vee \delta)$. Since $\langle a, c\rangle \in \beta \vee \delta$, by (1) there is $b \in A$ with $\langle a, b\rangle \in \beta$, $\langle b, c\rangle \in \delta$.



Since $\beta \leq \alpha = \alpha \circ \alpha$, we have $\langle b, c\rangle \in \alpha$. Thus $\langle b, c\rangle \in \alpha \wedge \delta$; consequently $\langle a, c\rangle \in \beta \circ (\alpha \wedge \delta) = \beta \vee (\alpha \wedge \delta)$ as desired.

The proof of (3) is a slightly more substantial enterprise. Suppose first that there is a term $t(x,y,z)$ for which Mal'cev's equations hold in $\mathcal{V}$. Let $A \in \mathcal{V}$, α, $\beta \in \mathrm{Con}\,\mathbf{A}$, $\langle a, b\rangle \in \alpha$, $\langle b, c\rangle \in \beta$. Now α and β are congruences and thus are preserved by all term operations of $\mathbf{A}$. Therefore $t^{\mathbf{A}}(a,b,b) \equiv t^{\mathbf{A}}(a,b,c) \pmod{\beta}$ and $t^{\mathbf{A}}(a,b,c) \equiv t^{\mathbf{A}}(b,b,c) \pmod{\alpha}$. Now $t^{\mathbf{A}}(a,b,b) = a$ and $t^{\mathbf{A}}(b,b,c) = c$ since $\mathbf{A}$ satisfies Mal'cev's equations. So we have the following picture, showing that $\alpha \circ \beta \subseteq \beta \circ \alpha$.



We can take converses, and conclude that $\beta \circ \alpha = \beta^{\cup} \circ \alpha^{\cup} = (\alpha \circ \beta)^{\cup} \subseteq (\beta \circ \alpha)^{\cup} = \alpha \circ \beta$; thus $\alpha \circ \beta = \beta \circ \alpha$.

Now suppose that $\mathcal{V}$ does have permuting congruences. On $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z)$ define the congruences $\alpha = \Theta(x, y)$, $\beta = \Theta(y, z)$. We have $\langle x, y \rangle \in \alpha$, $\langle y, z \rangle \in \beta$. Therefore for some $s = s^{\mathbf{F}}(x, y, z)$ in F we have $\langle x, s \rangle \in \beta$ and $\langle s, z \rangle \in \alpha$. Let π_α be the endomorphism of $\mathbf{F}$ satisfying $\pi_\alpha(x) = \pi_\alpha(y) = x$, $\pi_\alpha(z) = y$; and let π_β be the endomorphism satisfying $\pi_\beta(x) = x$, $\pi_\beta(y) = \pi_\beta(z) = y$. Since $\langle x, y \rangle \in \ker \pi_\alpha$, we have $\alpha \subseteq \ker \pi_\alpha$, similarly $\beta \subseteq \ker \pi_\beta$. (Exercise: Show that $\ker \pi_\alpha = \alpha$ and $\ker \pi_\beta = \beta$.) Therefore $\langle x, s \rangle \in \ker \pi_\beta$, $s = s^{\mathbf{F}}(x, y, z)$, implying

$$x = \pi_\beta(x) = \pi_\beta(s) = s^{\mathbf{F}}(\pi_\beta x, \pi_\beta y, \pi_\beta z) = s^{\mathbf{F}}(x, y, y) \ .$$

Similarly, we have $y = s^{\mathbf{F}}(x, x, y)$. There is a term $t(x, y, z) \in F_L(x, y, z)$ with $\varphi(t(x, y, z)) = s$ where $\varphi : \mathbf{F}_L(x, y, z) \twoheadrightarrow \mathbf{F}_{\mathcal{V}}(x, y, z)$ with $\varphi(x) = x$, $\varphi(y) = y$, $\varphi(z) = z$. It follows that $t^{\mathbf{F}}(x, y, z) = s$ and then, arguing as above, $t^{\mathbf{F}}(x, y, y) = x$ and $t^{\mathbf{F}}(x, x, y) = y$. Thus $\varphi(t(x, y, y)) = \varphi(x)$, implying that $t(x, y, y) \approx x$ is an identity of $\mathcal{V}$. Similarly, $t(x, x, y) \approx y$ is an identity of $\mathcal{V}$. This ends the proof. □

1. TIGHT LATTICES

In this chapter we give the slightly technical definition of the class of "tight" lattices (Definition 1.6). Each lattice of this class, when isomorphic to an interval in the congruence lattice of a finite algebra, produces an algebraic phenomenon we call "tameness".

DEFINITION 1.1. Let $\mathbf{L} = \langle L, \vee, \wedge \rangle$ be any lattice.

(1) By a **meet endomorphism** of $\mathbf{L}$ we mean a function $\mu : L \to L$ satisfying $\mu(x \wedge y) = \mu(x) \wedge \mu(y)$ for all elements x and y in $\mathbf{L}$.

(2) By a **join endomorphism** of $\mathbf{L}$ we mean a meet endomorphism of the dual lattice $\mathbf{L}^\partial = \langle L, \wedge, \vee \rangle$.

(3) A function $\mu : L \to L$ is **increasing** iff $\mu(x) \geq x$ for all x in L; and μ is **strictly increasing** iff $\mu(x) > x$ for all x in L except the largest element (if $\mathbf{L}$ has a largest element). The concepts of **decreasing** and of **strictly decreasing** function from $\mathbf{L}$ to $\mathbf{L}$ are defined in an analogous fashion.

(4) By a **polarity** of $\mathbf{L}$ we mean a pair $\langle \sigma, \mu \rangle$ such that σ is a decreasing join endomorphism of $\mathbf{L}$, and μ is an increasing meet endomorphism of $\mathbf{L}$, and $\sigma\mu(x) \leq x \leq \mu\sigma(x)$ for all x in L.

(5) By a **tolerance** of $\mathbf{L}$, we mean a reflexive and symmetric subalgebra of $\mathbf{L}^2$, i.e., a binary relation $\rho \subseteq L^2$ such that for all $x, y, u, v \in L$ we have : (i) $\langle x, x \rangle \in \rho$; (ii) $\langle x, y \rangle \in \rho$ iff $\langle y, x \rangle \in \rho$; (iii) if $\langle x, y \rangle$, $\langle u, v \rangle \in \rho$ then $\langle x \vee u, y \vee v \rangle \in \rho$ and $\langle x \wedge u, y \wedge v \rangle \in \rho$.

There is an extensive literature on tolerances of lattices. Our use of the concept will be restricted to finite lattices, for which the basic facts we need can be easily proved. In finite lattices, there are one-one correspondences: tolerances $\leftrightarrow$ polarities $\leftrightarrow$ increasing meet endomorphisms $\leftrightarrow$ decreasing join endomorphisms.

LEMMA 1.2. *Let* $\mathbf{L}$ *be a finite lattice.*

(1) *A pair* $\langle f, g \rangle$ *of mappings from* L *into* L *is a polarity iff* f *is decreasing or* g *is increasing, and for all* $x, y \in L$ *we have* $f(x) \leq y$ *iff* $x \leq g(y)$.

(2) *The relation* $\{\langle \sigma, \mu \rangle : \langle \sigma, \mu \rangle$ *is a polarity* $\}$ *is a one-to-one mapping of the set of all decreasing join endomorphism of* L *onto the set of all increasing meet endomorphisms of* $\mathbf{L}$.

(3) *If ρ is any tolerance of* $\mathbf{L}$, *then the formulas* $\sigma(x) = \bigwedge\{y : \langle x, y\rangle \in \rho\}$ *and* $\mu(x) = \bigvee\{y : \langle x, y\rangle \in \rho\}$ *define a polarity* $\langle \sigma, \mu\rangle$ *such that* $\rho = \{\langle x, y\rangle : \sigma(x \vee y) \leq x \wedge y\}$.

(4) *If* $\langle \sigma, \mu\rangle$ *is any polarity of* $\mathbf{L}$, *then there is a unique tolerance* ρ *such that* σ, μ, *and* ρ *are related as in* (3).

PROOF. We begin with (1). Suppose that $\langle f, g\rangle$ is a polarity. Then f and g are order preserving and $fg(x) \leq x \leq gf(x)$ for all x. Thus if $f(x) \leq y$, then $gf(x) \leq g(y)$, i.e., $x \leq gf(x) \leq g(y)$. That $x \leq g(y)$ implies $f(x) \leq y$, is analogously proved. Now suppose only that f is decreasing or g is increasing, and that $f(x) \leq y$ iff $x \leq g(y)$ holds for all x and y. From $f(x) \leq f(x)$, it follows that $x \leq gf(x)$; and $fg(x) \leq x$ follows from $g(x) \leq g(x)$. We have $f(x) \leq x$ for all x iff $x \leq g(x)$ for all x. Thus, in fact, f is decreasing and g is increasing. Both functions are order preserving; for example, if $x \leq y$ then $x \leq gf(y)$, implying $f(x) \leq f(y)$. Finally, let us show that f is a join endomorphism. (The proof that g is a meet endomorphism is entirely analogous to the argument we now give.) We choose any x and y in L, and notice that $g(f(x) \vee f(y)) \geq gf(x) \vee gf(y)$ (since g is order-preserving), and $gf(x) \vee gf(y) \geq x \vee y$. Thus $g(f(x) \vee f(y)) \geq x \vee y$, implying that $f(x \vee y) \leq f(x) \vee f(y)$. On the other hand, $f(x \vee y) \geq f(x) \vee f(y)$ since f is order-preserving. So we have $f(x \vee y) = f(x) \vee f(y)$.

Statement (2) breaks down into two assertions: that polarity is a one-to-one correspondence, and that every increasing meet endomorphism is one half of a polarity (and dually, every decreasing join endomorphism is one half of a polarity). If $\langle \sigma, \mu\rangle$ is to be a polarity, then each of σ and μ determine the other; by (1), for example, $\sigma(x)$ can be nothing but the least element y satisfying $\mu(y) \geq x$. Now suppose that μ is any increasing meet endomorphism. Define $\sigma(x) = \bigwedge\{y : \mu(y) \geq x\}$. Since the meet is a meet of finitely many elements, and μ is a meet endomorphism, we have $x \leq \mu\sigma(x)$ for all x. So if $\sigma(x) \leq y$ then $x \leq \mu\sigma(x) \leq \mu(y)$. If $x \leq \mu(y)$, then $\sigma(x) \leq y$ by the definition. It now follows from (1) that $\langle \sigma, \mu\rangle$ is a polarity. If we are given any decreasing join endomorphism σ, then we define $\mu(x) = \bigvee\{y : \sigma(y) \leq x\}$ and, proceeding as above, prove that $\langle \sigma, \mu\rangle$ is a polarity.

Let ρ be any tolerance of $\mathbf{L}$, and define σ and μ as in statement (3). Since ρ is reflexive, σ is decreasing and μ is increasing. Obviously, for all x we have $\langle x, \sigma(x)\rangle, \langle x, \mu(x)\rangle \in \rho$; and $\sigma(x)$ is the least element y with $\langle x, y\rangle \in \rho$, while $\mu(x)$ is the largest such element. Now if $\sigma(x) \leq y$, then from $\langle x, \sigma(x)\rangle \in \rho$ and $\langle y, y\rangle \in \rho$ we obtain $\langle x \vee y, \sigma(x) \vee y\rangle = \langle x \vee y, y\rangle \in \rho$. Thus $\langle y, x \vee y\rangle \in \rho$, and $\mu(y) \geq x \vee y \geq x$. Analogously, $\mu(y) \geq x$ implies $\sigma(x) \leq y$. By (1), it follows that $\langle \sigma, \mu\rangle$ is a polarity.

Let us show that $\langle \sigma, \mu\rangle$ determines ρ in the manner asserted. Let x and y be any elements such that $\sigma(x \vee y) \leq x \wedge y$. We have $\langle (x \vee y) \vee y, \sigma(x \vee y) \vee y\rangle \in \rho$, i.e., $\langle x \vee y, y\rangle \in \rho$; and similarly, $\langle x \vee y, x\rangle \in \rho$, implying that $\langle x, x \vee y\rangle \in \rho$. Thus $\langle x, y\rangle = \langle (x \vee y) \wedge x, y \wedge (x \vee y)\rangle$ is in ρ. Conversely, if $\langle x, y\rangle \in \rho$, then $\langle x \vee y, x\rangle$ and

$\langle x \vee y, y\rangle$ are in ρ, and taking meets, we find that $\langle x \vee y, x \wedge y\rangle \in \rho$. Thus, it follows from the definition that $\sigma(x \vee y) \leq x \wedge y$. This concludes the proof of (3).

Statement (4) has a straightforward proof. We leave it to the reader. □

Any congruence relation of a lattice is a tolerance. If ρ is a tolerance of $\mathbf{L}$, then the transitive closure of ρ is a congruence relation of $\mathbf{L}$. We call a tolerance ρ **connected** iff its transitive closure is all of L^2.

LEMMA 1.3. *Let ρ be a tolerance of a finite lattice $\mathbf{L}$, and let $\langle \sigma, \mu\rangle$ be the associated polarity. The following are equivalent.*

(1) *ρ is connected.*
(2) *There exists a sequence $0 = x_0 < x_1 < \cdots < x_n = 1$ of elements of $\mathbf{L}$ (for some $n \geq 0$) with $\langle x_i, x_{i+1}\rangle \in \rho$ for all $i < n$.*
(3) *σ is strictly decreasing.*
(4) *μ is strictly increasing.*

PROOF. Suppose that ρ is connected. This implies that there exists a sequence $0 = y_0, \ldots, y_n = 1$ with $\langle y_i, y_{i+1}\rangle \in \rho$ for $i < n$. Define $x_i = \bigvee\{y_j : j \leq i\}$ when $i \leq n$. Then for $i < n$, we have $\langle x_i, x_{i+1}\rangle = \langle x_i \vee y_i, x_i \vee y_{i+1}\rangle$, and so $\langle x_i, x_{i+1}\rangle \in \rho$; and obviously $x_i \leq x_{i+1}$, and $x_0 = 0$, $x_n = 1$. By removing any repeated terms from this sequence, we obtain a strictly increasing sequence. Thus (1) implies (2).

To prove that (2) implies (3), let the sequence $0 = x_0 < \cdots < x_n = 1$ be given as in (2), and let $x > 0$ in L. There is an $i < n$ such that $x_{i+1} \geq x$ and $x_i \not\geq x$. For this i, we have $\langle x, x \wedge x_i\rangle = \langle x \wedge x_{i+1}, x \wedge x_i\rangle \in \rho$, and consequently, $\sigma(x) \leq x \wedge x_i < x$. Thus σ is strictly decreasing.

Now suppose that σ is strictly decreasing. Let x be any element of L such that $x < 1$. Choose z to be a minimal member of $\{y \in L : y \not\leq x\}$. We have $z \neq 0$, consequently $\sigma(z) < z$, implying $\sigma(z) \leq x$. This last inclusion is equivalent to $z \leq \mu(x)$. Since $z \not\leq x$, it follows that $\mu(x) > x$. Thus μ is strictly increasing.

The proof that (4) implies (1) is a simple matter of considering the sequence $0 < \mu(0) < \mu\mu(0) < \cdots$. □

For two elements x and y of a lattice (or of a partially ordered set) recall that y **covers** x (in symbols $x \prec y$) iff $x < y$ and whenever $x \leq z \leq y$, either $z = x$ or $z = y$. If L has 0 (a smallest element) then an **atom** of L is simply any element u such that $0 \prec u$. A **dual atom of** L is an element u such that $u \prec 1$.

LEMMA 1.4. *Let $\mathbf{L}$ be a finite lattice.*

(1) *The subalgebra of $\mathbf{L}^2$ generated by $\{\langle x, x\rangle : x \in L\} \cup \{\langle x, y\rangle : x \prec y \text{ or } y \prec x\}$ is a connected tolerance, and it is the smallest connected tolerance of $\mathbf{L}$.*
(2) *A meet endomorphism μ (or join endomorphism σ) of $\mathbf{L}$ is strictly increasing (or strictly decreasing) iff $\mu(x) \geq y$ (or $\sigma(y) \leq x$) whenever $x \prec y$ in $\mathbf{L}$.*

PROOF. The relation defined in (1) is certainly a connected tolerance. Let ρ be any connected tolerance of L, and let $0 < x_1 < \cdots < x_n = 1$ be a sequence with $\langle x_i, x_{i+1}\rangle \in \rho$ for all i. Let $a \prec b$ be any covering in L. There exists an i such that $b \wedge x_i \leq a$ and $b \wedge x_{i+1} \not\leq a$. For this i, we have $\langle a, b\rangle = \langle a \vee (b \wedge x_i),\ a \vee (b \wedge x_{i+1})\rangle$, which implies that $\langle a, b\rangle \in \rho$. Thus ρ contains the tolerance generated by the covering relation. This proves (1); and (2) follows easily from (1), by Lemmas 1.2 and 1.3. □

DEFINITION 1.5. Let $\mathbf{L}$ be any lattice with 0 and 1. A homomorphism $f : \mathbf{L} \to \mathbf{L}'$ is called $0,1$–**separating** iff $f^{-1}\{f(0)\} = \{0\}$ (f separates 0) and $f^{-1}\{f(1)\} = \{1\}$ (f separates 1). To denote that f is a homomorphism with the property just defined, we write $f : \mathbf{L} \overset{0,1-\text{sep}}{\longrightarrow} \mathbf{L}'$. We say that $\mathbf{L}$ is $0,1$-**simple** iff $|L| > 1$ and every non-constant homomorphism $f : \mathbf{L} \to \mathbf{L}'$ ($\mathbf{L}'$ any lattice) is $0,1$–separating.

DEFINITION 1.6. A lattice $\mathbf{L}$ will be called **tight** iff $\mathbf{L}$ is finite, $|L| > 1$, and if ρ is any tolerance of $\mathbf{L}$ such that ρ contains $\langle 0, a\rangle$ for some $a > 0$ in $\mathbf{L}$, or ρ contains $\langle b, 1\rangle$ for some $b < 1$ in $\mathbf{L}$, then $\rho = L^2$.

The whole purpose of this chapter is to define tight lattices and to collect the facts about them that will be needed later on.

LEMMA 1.7. *A finite lattice $\mathbf{L}$ is tight iff $\mathbf{L}$ is $0,1$-simple and every strictly increasing meet endomorphism of $\mathbf{L}$ is constant (i.e., L^2 is the only connected tolerance of $\mathbf{L}$).*

PROOF. Assume that $\mathbf{L}$ is tight. It follows from Lemma 1.4 and Definition 1.6 that $\mathbf{L}$ has only the trivial connected tolerance. From Lemmas 1.2 and 1.3, every strictly increasing meet endomorphism μ of $\mathbf{L}$ satisfies $\mu(0) = 1$ (i.e., μ is constant). Let $f : \mathbf{L} \to \mathbf{L}'$ be a non-constant homomorphism, and let $\theta = \ker f = \{\langle x, y\rangle : f(x) = f(y)\}$. Thus θ is a tolerance of $\mathbf{L}$, in fact a congruence. Since $\theta \neq L^2$, it follows from the definition of tight lattice, that $\langle 0, x\rangle \notin \theta$ for any $x > 0$ in $\mathbf{L}$. This means that f is 0–separating. Similarly, we can prove that it is 1–separating. So we conclude that $\mathbf{L}$ is $0,1$-simple.

Now let us assume that $|L| > 1$ and $\mathbf{L}$ is not tight. Let ρ be a tolerance of $\mathbf{L}$ such that $\rho \neq L^2$, and say, $\langle b, 1\rangle \in \rho$ for some $b < 1$. If ρ is connected, then we have a non-trivial connected tolerance of $\mathbf{L}$. If ρ is not connected, and θ is the transitive closure of ρ, then θ is a congruence, $\theta \neq L^2$, and $\langle b, 1\rangle \in \theta$. The homomorphism $\mathbf{L} \twoheadrightarrow \mathbf{L}/\theta$ is not constant and not 1–separating. Thus $\mathbf{L}$ fails to be $0,1$-simple. □

LEMMA 1.8. *For any lattice $\mathbf{L}$ with 0 and 1, such that $|L| > 1$, the following are equivalent.*

(1) *$\mathbf{L}$ is $0,1$-simple.*

(2) *$\mathbf{L}$ has a largest congruence $\theta \neq L^2$, and this congruence satisfies $1/\theta = \{1\}$, $0/\theta = \{0\}$.*

PROOF. Suppose that L is 0,1-simple. Define $\theta = \bigvee\{\psi \in \operatorname{Con}\mathbf{L} : \psi \neq L^2\}$. We claim that $\theta \neq L^2$, in fact $1/\theta = \{1\}$ and $0/\theta = \{0\}$. To see it, suppose, for example, that $\langle x, 1\rangle \in \theta$. Now θ, the complete join in the lattice $\operatorname{Con}\mathbf{L}$ of all proper congruences of $\mathbf{L}$, is just the transitive closure of the relation $\rho = \bigcup\{\psi : \psi \neq L^2\}$. Therefore there exists a sequence $x = x_0, x_1, \ldots, x_n = 1$ such that for all $i < n$, $\langle x_i, x_{i+1}\rangle \in \psi_i$ for some congruence ψ_i of $\mathbf{L}$ with $\psi_i \neq L^2$. Since $\mathbf{L}$ is 0,1-simple, the map $\mathbf{L} \twoheadrightarrow \mathbf{L}/\psi_i$ is 1–separating, equivalently, $1/\psi_i = \{1\}$. Therefore $x_{n-1} = 1$, and then $x_{n-2} = 1$, and so on, leading to $x = 1$. We can conclude that $1/\theta = \{1\}$. Thus $\theta \neq L^2$, and it follows that θ is the largest congruence of L which is $\neq L^2$. That $0/\theta = \{0\}$ is proved as above. Thus (1) implies (2).

Suppose, now, that (2) holds. Let $f : \mathbf{L} \to \mathbf{L}'$ be any non-constant homomorphism. Then $\ker f \subseteq \theta$, implying that f is 0,1–separating. Thus (1) holds. □

Exercises 1.9

(1) Show that, among the lattices pictured below, $\mathbf{M}_n$ ($n \geq 3$) and $\mathbf{C}_2$ are tight, while the others are not.

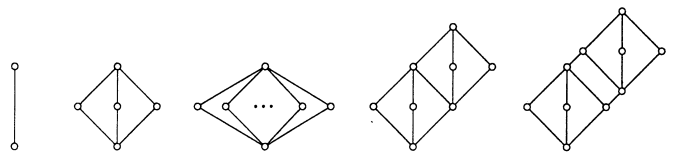


Figure 1

(2) Show that if $f : \mathbf{L} \overset{0,1-\text{sep}}{\longrightarrow} \mathbf{L}'$ is surjective and if $\mathbf{L}$ is 0,1-simple, then so is $\mathbf{L}'$. Use the lattices $\mathbf{M}'_{3,3}$ and $\mathbf{M}_{3,3}$ to show that $\mathbf{L}$ may fail to be 0,1-simple even if $\mathbf{L}'$ is, in this situation.

LEMMA 1.10.

(1) *Let $f : \mathbf{L} \overset{0,1-\text{sep}}{\longrightarrow} \mathbf{L}'$ be surjective, where $\mathbf{L}$ and $\mathbf{L}'$ are finite. Then $\mathbf{L}$ is tight iff $\mathbf{L}'$ is tight.*

(2) *A finite lattice $\mathbf{L}$ is tight iff there exists a simple tight lattice $\mathbf{L}'$ and a surjective 0,1–separating homomorphism of $\mathbf{L}$ onto $\mathbf{L}'$. When they exist, $\mathbf{L}'$ is determined up to isomorphism; and the kernel of f is the unique dual atom of $\operatorname{Con}\mathbf{L}$.*

PROOF. Suppose that $f : \mathbf{L} \overset{0,1-\text{sep}}{\longrightarrow} \mathbf{L}'$ is surjective and $\mathbf{L}$ is finite. Assume that $\mathbf{L}'$ is tight, and let ρ be a tolerance of $\mathbf{L}$ such that, say, $\langle 0, a\rangle \in \rho$ for some element $a > 0$ of $\mathbf{L}$. We define $\rho' = f(\rho) = \{\langle f(x), f(y)\rangle : \langle x, y\rangle \in \rho\}$, and verify that ρ' is

a tolerance of $\mathbf{L}'$ and $\langle 0', b' \rangle \in \rho'$, where $0' < b' = f(a)$ and $0'$ is the zero element of $\mathbf{L}'$. Therefore $\rho' = (L')^2$; and from this we conclude that for some $\langle u, v \rangle \in \rho$, $\langle f(u), f(v) \rangle = \langle 0', 1' \rangle$. Since f is $0,1$–separating, we must have $\langle u, v \rangle = \langle 0, 1 \rangle$. The tolerance ρ, containing $\langle 0, 1 \rangle$, can be nothing other than L^2. Thus $\mathbf{L}$ is tight if $\mathbf{L}'$ is tight. Now assume that $\mathbf{L}$ is tight. Let ρ' be a tolerance of $\mathbf{L}'$ containing, say, $\langle 0', c' \rangle$ for some $c' > 0'$. We define $\rho = f^{-1}(\rho') = \{\langle x, y \rangle \in L^2 : \langle f(x), f(y) \rangle \in \rho'\}$, and verify that ρ is a tolerance and $\langle 0, c \rangle \in \rho$ for some $c > 0$. Therefore $\rho = L^2$, and consequently $\rho' = (L')^2$. Thus $\mathbf{L}'$ is tight. This ends the proof of (1).

To prove (2), suppose first that $\mathbf{L}$ is tight. Let θ be the largest proper congruence of $\mathbf{L}$ (which exists by Lemma 1.8). The natural homomorphism $f : \mathbf{L} \twoheadrightarrow \mathbf{L}/\theta$ is $0,1$–separating (since $\mathbf{L}$ is $0,1$-simple), and $\mathbf{L}/\theta$ is a simple lattice, which is tight by statement (1). Now assume, conversely that $g : \mathbf{L} \twoheadrightarrow \mathbf{L}'$ is $0,1$–separating and $\mathbf{L}'$ is simple and tight. That $\mathbf{L}$ is tight follows from (1). The kernel of g can be nothing other than the unique dual atom of $\operatorname{Con}\mathbf{L}$. (Since $\mathbf{L}'$ is simple, $\ker g$ is a dual atom.) Thus $\mathbf{L}' \cong \mathbf{L}/\ker g$ is determined up to isomorphism by $\mathbf{L}$. □

The class of tight lattices is quite diverse, as can be seen from these examples.

Example 1.11. A finite simple (or $0,1$-simple) lattice, satisfying any one of the following conditions, is tight. (i): $\mathbf{L}$ is complemented (i.e., for all $x \in L$ there exists $x' \in L$ such that $x \vee x' = 1$ and $x \wedge x' = 0$). (ii): The atoms of $\mathbf{L}$ join to 1. (iii): The dual atoms of $\mathbf{L}$ meet to 0. In fact, condition (i) implies (ii) and (iii); and each of (ii) and (iii) implies that $\mathbf{L}$ cannot have a non-constant, strictly increasing, meet endomorphism (by Lemma 1.4 (2)). A finite $0,1$-simple lattice satisfying one of these conditions is tight (by Lemma 1.7).

Example 1.12. For each integer $n \geq 2$, the lattice $\mathbf{\Pi}_n$ of all equivalence relations on an n-element set is tight. These lattices are simple and complemented.

Example 1.13. For each prime p and integers $k, n \geq 1$, the lattice $\mathbf{S}(p^k, n)$ of all subspaces of an n-dimensional vector space over a finite field of p^k elements, is tight. This lattice is simple and complemented. It is isomorphic to the lattice of congruence relations of the vector space.

Any finite lattice that admits a $0,1$–separating homomorphism onto a lattice $\mathbf{\Pi}_n$ or $\mathbf{S}(p^k, n)$ is tight (by Lemma 1.10). According to Exercise 1.14 (1), such lattices are $0,1$-simple and complemented. Some tight lattices are pictured on the next page.

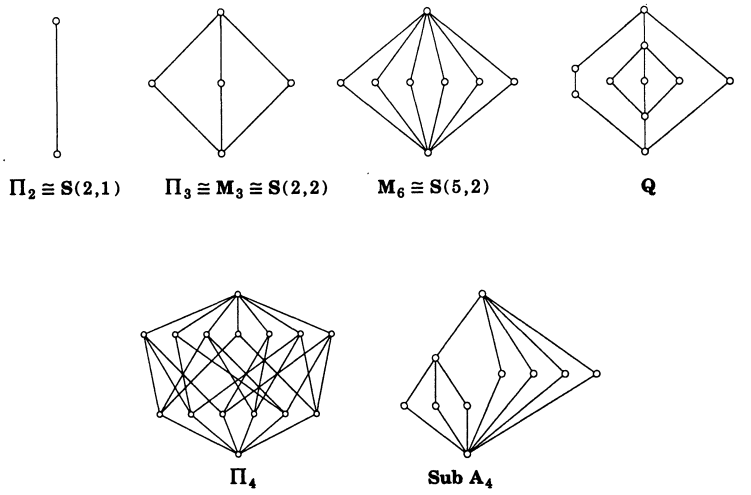


Figure 2

$\mathbf{Sub}\,\mathbf{A}_4$ is the lattice of subgroups of the twelve-element alternating group. The lattice $\mathbf{Q}$ admits an obvious $0,1$–separating homomorphism onto $\mathbf{M}_3$.

The first substantial result proved as an application of tame congruence theory was that $\mathbf{Sub}\,\mathbf{A}_4$ (and many other tight lattices, in particular $\mathbf{M}_n$ if $n \geq 3$) cannot be isomorphic to the congruence lattice of any finite algebra with just one basic operation, such as a semigroup. (This result will not be proved in this book. The proof can be found in [22].)

We shall prove in Chapter 5 (Theorem 5.7(4)) that, except in quite unusual situations, if an interval sublattice $\mathbf{L}$ of the congruence lattice of a finite algebra is tight, then $\mathbf{L}$ admits a $0,1$–separating homomorphism onto the lattice of subspaces of a finite vector space. In the next exercises, all lattices mentioned are assumed to be finite.

Exercises 1.14

(1) Let $f : \mathbf{L} \overset{0,1-\text{sep}}{\to} \mathbf{L}'$ be surjective. For each of conditions (i), (ii), (iii) of Example 1.11, show that $\mathbf{L}$ satisfies the condition iff $\mathbf{L}'$ satisfies it.

(2) The full partition lattice $\mathbf{\Pi}_n$ of Example 1.12 is simple and complemented, if $n \geq 2$.

(3) $\mathbf{Con}\,\mathbf{V}$ is simple and complemented whenever $\mathbf{V}$ is a finite vector space of more than one element. (It will be easier to work with the isomorphic lattices $\mathbf{S}(p^k, n)$ of Example 1.13.)

(4) Let $\mathbf{L}$ be modular. Show that the formula $\mu(x) = \bigvee\{y : x \prec y\}$ defines a meet endomorphism of $\mathbf{L}$. [By Lemma 1.4, the associated tolerance is the smallest connected tolerance of $\mathbf{L}$. This exercise is harder than most. The key is to prove that $x \leq \mu(y)$ iff $y \geq \bigwedge\{z : z \prec x\} = \sigma(x)$.]

(5) If $\mathbf{L}$ is modular then $\mathbf{L}$ is tight iff $\mathbf{L}$ is simple and complemented.

(6) $\mathbf{L}$ is tight iff the dual lattice, $\mathbf{L}^\partial$, is tight.

The next five exercises were contributed by Brian Davey and Emil Kiss. A sublattice of $\mathbf{L}^2$ containing the diagonal $\Delta = \{\langle x, x\rangle : x \in \mathbf{L}\}$ will be called a *diagonal sublattice.* $\mathbf{L}$ is called *order polynomially complete* iff every monotone mapping $L^n \to L$ (for any n) is a polynomial operation of $\mathbf{L}$. The diagonal sublattice generated by a pair $\langle a, b\rangle \in L^2$ is denoted $L(a, b)$.

(7) $\mathbf{L}$ is tight iff for every $a \neq 0$ and $b \neq 1$, $\langle 0, 1\rangle \in L(0, a) \cap L(b, 1)$.

(8) $\mathbf{L}$ is tight iff every diagonal sublattice of $\mathbf{L}^2$ is of the form K, $\leq \circ K$, $\geq \circ K$, or L^2, where K is a $0,1$–separating diagonal sublattice (i.e., $\langle a, 0\rangle$ or $\langle 0, a\rangle$ in K implies $a = 0$, and $\langle b, 1\rangle$ or $\langle 1, b\rangle$ in K implies $b = 1$).

(9) If $\mathbf{L}$ is simple then Δ is the only $0,1$–separating diagonal sublattice of $\mathbf{L}^2$.

(10) $\mathbf{L}$ is order polynomially complete iff Δ, $\leq$, $\geq$, L^2 are the only diagonal sublattices of $\mathbf{L}^2$.

(11) $\mathbf{L}$ is order polynomially complete iff $\mathbf{L}$ is tight and simple.

2. TAME QUOTIENTS

In this chapter we define the "tame quotients" of a finite algebra and their minimal sets (Definitions 2.5 and 2.6) and prove two principal theorems about them (Theorems 2.8 and 2.11).

We recall from Chapter 0 that the congruence lattice of an algebra $\mathbf{A}$, or $\mathbf{Con\ A}$, is a complete, 0, 1-sublattice of the full partition lattice $\mathbf{\Pi}_A$ of all equivalence relations on the base set of $\mathbf{A}$. That is to say, the join and meet of any subset of $\mathbf{Con\ A}$, computed in $\mathbf{\Pi}_A$, belong to $\mathbf{Con\ A}$, and $\mathbf{Con\ A}$ contains the least and largest elements, 0_A and 1_A, of $\mathbf{\Pi}_A$. The members of $\mathbf{Con\ A}$ are precisely the equivalence relations on A that are also subalgebras of $\mathbf{A} \times \mathbf{A}$. The congruences on $\mathbf{A}$, or members of $\mathbf{Con\ A}$, can also be defined as the equivalence relations α on A such that $f(\alpha) \subseteq \alpha$ for every unary polynomial f of $\mathbf{A}$. (By $f(\alpha) \subseteq \alpha$ we mean that whenever $\langle x, y \rangle \in \alpha$, then $\langle f(x), f(y) \rangle \in \alpha$.) Thus $\mathbf{Con\ A} = \mathbf{Con}\ \langle A, \mathrm{Pol}_1\mathbf{A} \rangle$; and in congruence theory it is often convenient to work directly with unary algebras (whose basic operations are 1-ary).

The basic (or given) operations of an algebra $\mathbf{A}$ determine the set $\mathrm{Pol}_1\mathbf{A}$, and this monoid determines the congruence lattice of $\mathbf{A}$. But often when examining an algebra, its set of unary polynomials and its congruence lattice are unknown. In this chapter, as we begin to present the basics of tame congruence theory, we will consider the congruence lattice and the unary polynomials of any algebra to be known entities. The principal thrust of our theory will be to reveal subtle ways in which the congruence lattice of a finite algebra $\mathbf{A}$, either considered as an abstract lattice or as a specific set of equivalence relations, influences all of the operations (not just the unary operations) which preserve these equivalence relations. In the beginning, however, we shall be looking only at the interaction between $\mathrm{Con}\,\mathbf{A}$ and $\mathrm{Pol}_1\mathbf{A}$.

DEFINITION 2.1. The set of all $e \in \mathrm{Pol}_1\mathbf{A}$ such that $e = e^2$ $(= e \circ e)$ will be denoted by $\mathrm{E}(\mathbf{A})$. (This is the set of **idempotents**, or **projections**, in $\mathrm{Pol}_1\mathbf{A}$.)

Our symbol for **restriction** is $|$. The several ways in which this symbol will be used are defined below.

DEFINITION 2.2. Suppose that A is a nonvoid set, $\emptyset \neq U \subseteq A$, $\theta \in \Pi_A$, f is a function with domain A, h is an n-ary operation on A, and $U_0 \cup \cdots \cup U_{n-1} \subseteq A$. We define

(1) $\theta|_U \stackrel{\text{def}}{=} \theta \cap (U \times U)$;

(2) $f|_U \stackrel{\text{def}}{=} \{\langle x, f(x)\rangle : x \in U\}$;

(3) $h|_{U_0 \times \cdots \times U_{n-1}} \stackrel{\text{def}}{=} \{\langle x_0, \ldots, x_{n-1}, h(x_0, \ldots, x_{n-1})\rangle : x_i \in U_i \text{ for } 0 \leq i < n\}$;

(4) $h|_U \stackrel{\text{def}}{=} h|_{U^n}$.

If $\mathbf{A} = \langle A, \cdots\rangle$ is any algebra with base set A, then we define:

(5) $(\operatorname{Pol}\mathbf{A})|_U$ is the set of all $h|_U$ such that $h \in \operatorname{Pol}_n\mathbf{A}$ for some n, and $h(U^n) \subseteq U$;

(6) $\mathbf{A}|_U \stackrel{\text{def}}{=} \langle U, (\operatorname{Pol}\mathbf{A})|_U\rangle$, called the **algebra induced on U by $\mathbf{A}$** (or an **induced algebra of $\mathbf{A}$**).

We can now state and prove an easy but very useful lemma discovered by P.P. Pálfy and P. Pudlák [27].

LEMMA 2.3. *Suppose that $\mathbf{A}$ is an algebra, $e \in \mathrm{E}(\mathbf{A})$, and $U = e(A)$. The mapping $|_U$ is a lattice homomorphism of $\operatorname{Con}\mathbf{A}$ onto $\operatorname{Con}\mathbf{A}|_U$.*

$$\operatorname{Con}\mathbf{A} \stackrel{\theta \mapsto \theta|_U}{\longrightarrow} \operatorname{Con}\mathbf{A}|_U .$$

PROOF. The restriction map of Π_A to Π_U trivially preserves meets. It is also obvious that $\theta|_U \in \operatorname{Con}\mathbf{A}|_U$ whenever $\theta \in \operatorname{Con}\mathbf{A}$. To see that $|_U$ preserves joins of pairs of elements of $\operatorname{Con}\mathbf{A}$, and that it maps $\operatorname{Con}\mathbf{A}$ onto $\operatorname{Con}\mathbf{A}|_U$, we define for each $\alpha \in \operatorname{Con}\mathbf{A}|_U$:

$$\hat{\alpha} = \{\langle x, y\rangle \in A^2 : \langle ef(x), ef(y)\rangle \in \alpha \text{ for all } f \in \operatorname{Pol}_1\mathbf{A}\} .$$

Now if $\alpha \in \operatorname{Con}\mathbf{A}|_U$ and $\langle x, y\rangle \in \hat{\alpha}$ and $g \in \operatorname{Pol}_1\mathbf{A}$, then for every $f \in \operatorname{Pol}_1\mathbf{A}$,

$$\langle ef(g(x)), ef(g(y))\rangle = \langle e(fg)(x), e(fg)(y)\rangle \in \alpha;$$

thus $\langle g(x), g(y)\rangle \in \hat{\alpha}$. Since $\hat{\alpha}$ is obviously an equivalence relation on A, it follows that $\hat{\alpha} \in \operatorname{Con}\mathbf{A}$.

The equation $\hat{\alpha}|_U = \alpha$ is easily demonstrated to be true. First, if $x, y \in U$ and $\langle x, y\rangle \in \hat{\alpha}$, then $\langle x, y\rangle = \langle ee(x), ee(y)\rangle \in \alpha$ by definition of $\hat{\alpha}$. Thus $\hat{\alpha}|_U \subseteq \alpha$. Second, if $\langle x, y\rangle \in \alpha$ and $f \in \operatorname{Pol}_1\mathbf{A}$, then $(ef)|_U$ is a polynomial of $\mathbf{A}|_U$, and this gives $\langle ef(x), ef(y)\rangle \in \alpha$. Consequently, $\alpha \subseteq \hat{\alpha}$. We have now shown that $|_U$ maps $\operatorname{Con}\mathbf{A}$ onto $\operatorname{Con}\mathbf{A}|_U$.

Just as easily, we see that for $\theta \in \operatorname{Con}\mathbf{A}$ and $\alpha \in \operatorname{Con}\mathbf{A}|_U$ we have $\theta|_U \leq \alpha$ iff $\theta \leq \hat{\alpha}$. Finally, we show that $|_U$ preserves joins. Let $\theta_1, \theta_2 \in \operatorname{Con}\mathbf{A}$ and put $\alpha = \theta_1|_U \vee \theta_2|_U$ and $\beta = \theta_1 \vee \theta_2$. We have to show that $\beta|_U = \alpha$. Clearly $\beta|_U \geq \alpha$. Conversely, since $\theta_i|_U \leq \alpha$ we have $\theta_i \leq \hat{\alpha}$ $(i = 1, 2)$. From this, it follows that $\beta \leq \hat{\alpha}$, and thus $\beta|_U \leq \alpha$. The proof is finished. □

A useful extension of the last lemma is the following one. In this lemma, $I[0_A, \theta]$ denotes the interval sublattice of $\mathbf{Con}\,\mathbf{A}$ consisting of all congruences α such that $\alpha \leq \theta$.

LEMMA 2.4. *Let* $\mathbf{A}$ *be an algebra,* $e \in \mathrm{E}(\mathbf{A})$, $U = e(A)$, $\theta \in \operatorname{Con}\mathbf{A}$, *and* $N \subseteq U$ *be such that* N *is a union of* $\theta|_U$*-equivalence classes. Then* $\mathbf{A}|_N = (\mathbf{A}|_U)|_N$ *and restriction is a lattice homomorphism of* $I[0_A, \theta]$ *into the interval* $I[0_N, \theta|_N]$ *in* $\mathbf{Con}\,\mathbf{A}|_N$. *If* $N^2 \subseteq \theta$, *this homomorphism is onto* $\mathbf{Con}\,\mathbf{A}|_N$.

$$I[0_A, \theta] \overset{\alpha \mapsto \alpha|_N}{\longrightarrow} I[0_N, \theta|_N] .$$

PROOF. Every operation of $(\mathbf{A}|_U)|_N$ is clearly an operation of $\mathbf{A}|_N$. On the other hand, let g be an operation of $\mathbf{A}|_N$. Then $g = f|_N$ for some polynomial operation f of $\mathbf{A}$ under which N is closed. U is closed under ef, and $(ef|_U)|_N = f|_N$. Thus g is an operation of $(\mathbf{A}|_U)|_N$. So the two non-indexed algebras are equal.

Now the mapping $\alpha \mapsto \alpha|_N$ is the composition of the lattice homomorphism $\alpha \mapsto \alpha|_U$ (Lemma 2.3) mapping $I[0_A, \theta] \subseteq \operatorname{Con}\mathbf{A}$ onto $I[0_U, \theta|_U] \subseteq \operatorname{Con}\mathbf{A}|_U$, with the restriction map from $I[0_U, \theta|_U]$ into Π_N. Thus we may as well assume that $U = A$ and $e = \mathrm{id}$. With these assumptions, it is clear that $|_N$ maps $\operatorname{Con}\mathbf{A}$ into $\operatorname{Con}\mathbf{A}|_N$, preserves meets, and preserves joins of congruences in the interval $I[0_A, \theta]$.

Now assume that $N^2 \subseteq \theta$, i.e., that N is a θ-equivalence class. Let $\alpha \in \operatorname{Con}\mathbf{A}|_N$, and put

$$\hat{\alpha} = \{\langle x, y\rangle \in \theta : \{f(x), f(y)\} \cap N \neq \emptyset \quad \text{implies} \quad \langle f(x), f(y)\rangle \in \alpha \ , \\ \text{for all} \quad f \in \mathrm{Pol}_1\mathbf{A}\} \ .$$

It is easily seen that $\hat{\alpha} \in \operatorname{Con}\mathbf{A}$, $\hat{\alpha} \leq \theta$, and $\hat{\alpha}|_N \leq \alpha$. To see that $\alpha \leq \hat{\alpha}|_N$, let $\langle x, y\rangle \in \alpha$, $f \in \mathrm{Pol}_1\mathbf{A}$, $f(x) \in N$ (or $f(y) \in N$). Then $f(N) \subseteq f(x)/\theta = N$ (since f preserves θ), so $f|_N \in \mathrm{Pol}_1\mathbf{A}|_N$, and it follows that $\langle f(x), f(y)\rangle = \langle f|_N(x), f|_N(y)\rangle \in \alpha$. Thus we see that $\langle x, y\rangle \in \hat{\alpha}$. □

Exercises 2.5

(1) Prove that the lattice homomorphisms of Lemmas 2.3 and 2.4 preserve all infinite joins and meets.

(2) Prove that if $e \in \mathrm{E}(\mathbf{A})$ and $\emptyset \neq N \subseteq U = e(A)$, then $\mathbf{A}|_N = (\mathbf{A}|_U)|_N$.

(3) Prove that for any algebra $\mathbf{A}$ and $\emptyset \neq B \subseteq A$, $\operatorname{Pol}(\mathbf{A}|_B) = (\operatorname{Pol}\mathbf{A})|_B$.

In the remainder of this chapter and throughout Chapters 3 and 4, all algebras considered will be assumed to be finite. The concept of a minimal set relative to a pair of congruences is fundamental for our work.

DEFINITION 2.5. Let $\mathbf{A}$ be a finite algebra and let $\alpha < \beta$ be two congruences of $\mathbf{A}$. We define $\mathrm{U}_{\mathbf{A}}(\alpha, \beta)$ to be the set of all sets of the form $f(A)$ where $f \in \mathrm{Pol}_1\mathbf{A}$ and $f(\beta) \not\subseteq \alpha$. We define $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ to be the set of all minimal members of $\mathrm{U}_{\mathbf{A}}(\alpha, \beta)$; i.e., $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ iff $\mathrm{U} \in \mathrm{U}_{\mathbf{A}}(\alpha, \beta)$ and there does not exist $V \in \mathrm{U}_{\mathbf{A}}(\alpha, \beta)$ with $V \subseteq U$, $V \neq U$. The members of $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ are called $\langle \alpha, \beta \rangle$-**minimal sets of A.**

Observe that in the framework of the definition, $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ is non-empty and for each $\langle \alpha, \beta \rangle$-minimal set U, we have $\alpha|_U \neq \beta|_U$.

By a **quotient** in a lattice $\mathbf{L}$, we shall mean simply a pair $\langle x, y \rangle$ of elements of $\mathbf{L}$ with $x < y$. A **prime quotient** is a quotient $\langle x, y \rangle$ where $x \prec y$. The interval lattice $I[x, y]$ associated with a quotient $\langle x, y \rangle$ is the sublattice of $\mathbf{L}$ consisting of all elements z such that $x \leq z \leq y$. By a **quotient (of congruences) in an algebra A** we mean any quotient $\langle \alpha, \beta \rangle$ in $\mathbf{Con}\,\mathbf{A}$.

The concept of a tame quotient is technical, but quite easy to define. Recall the notion of $0,1$-separating homomorphism, from Chapter 1 (Definition 1.5).

DEFINITION 2.6. Let $\mathbf{A}$ be a finite algebra and let $\langle \alpha, \beta \rangle$ be a quotient of congruences in $\mathbf{A}$. We call $\langle \alpha, \beta \rangle$ **tame** iff there exists $V \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $e \in \mathrm{E}(\mathbf{A})$ such that $e(A) = V$ and $I[\alpha, \beta] \xrightarrow{|_V} I[\alpha|_V, \beta|_V]$ is a $0,1$-separating lattice homomorphism.

In a short time we shall see that a quotient $\langle \alpha, \beta \rangle$ in a finite algebra is tame if the interval lattice $I[\alpha, \beta]$ is tight. (Thus, for instance, $\langle \alpha, \beta \rangle$ is tame whenever $\alpha \prec \beta$.) But first, we shall prove some facts which explain why the concept of tameness is natural and important. To do this, we need the concept of (internal) polynomial isomorphism.

DEFINITION 2.7. Let $\mathbf{A}$ be any algebra and let B and C be nonvoid subsets of $\mathbf{A}$. We say that B and C are **polynomially isomorphic in A**, and we write $B \overset{\mathbf{A}}{\simeq} C$ or simply $B \simeq C$ for this, iff there exists $f, g \in \mathrm{Pol}_1\mathbf{A}$ with

$$f(B) = C, \quad g(C) = B\,,$$
$$gf|_B = \mathrm{id}_B, \quad fg|_C = \mathrm{id}_C\,.$$

We write $f : B \simeq C$ iff $f \in \mathrm{Pol}_1\mathbf{A}$ and there exists $g \in \mathrm{Pol}_1\mathbf{A}$ such that the above equations hold.

It is important to observe that when $B \overset{\mathbf{A}}{\simeq} C$, the induced algebras $\mathbf{A}|_B$ and $\mathbf{A}|_C$ are isomorphic non-indexed algebras. If $f : B \simeq C$ then, where $\pi = f|_B$, we have $\pi(B) = C$ and $\pi((\mathrm{Pol}\,\mathbf{A})|_B) = (\mathrm{Pol}\,\mathbf{A})|_C$. [This last equation is understood to mean

that for any operation h on B (say h is n-ary), h is an operation of $\mathbf{A}|_B$ iff there exists a (unique) n-ary operation h' of $\mathbf{A}|_C$ such that $\pi h(x_0, \ldots, x_{n-1}) = h'(\pi x_0, \ldots, \pi x_{n-1})$ for all $x_0, \ldots, x_{n-1} \in B$.] Moreover, $\pi(\theta|_B) = \theta|_C$ for every congruence θ of $\mathbf{A}$.

The relation $\simeq$ is, of course, an equivalence relation on the set of non-void subsets of $\mathbf{A}$. We shall now see that when $\langle \alpha, \beta \rangle$ is tame, the set $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ defined in Definition 2.5 is an equivalence class under $\simeq$.

THEOREM 2.8. *Let $\langle \alpha, \beta \rangle$ be a tame quotient of a finite algebra $\mathbf{A}$. The following hold.*

(1) *For all $U, V \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, $U \simeq V$.*

(2) *For all $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ there is $e \in \mathrm{E}(\mathbf{A})$ with $e(A) = U$; moreover, the map $|_U : I[\alpha, \beta] \twoheadrightarrow I[\alpha|_U, \beta|_U]$ is 0,1–separating.*

(3) *For all $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $f \in \mathrm{Pol}_1\mathbf{A}$, if $f(\beta|_U) \not\subseteq \alpha$ then $f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $f : U \simeq f(U)$.*

(4) *If $\langle x, y \rangle \in \beta - \alpha$ and $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ then for some $f \in \mathrm{Pol}_1\mathbf{A}$, $f(A) = U$ and $\langle f(x), f(y) \rangle \in \beta|_U - \alpha|_U$.*

(5) *For each $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, β is the transitive closure of*

$$\alpha \cup \{\langle g(x), g(y) \rangle : \langle x, y \rangle \in \beta|_U \text{ and } g \in \mathrm{Pol}_1\mathbf{A}\}.$$

(6) *For all $f \in \mathrm{Pol}_1\mathbf{A}$, if $f(\beta) \not\subseteq \alpha$ then for some $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, $f : U \simeq f(U)$.*

PROOF. From the definition (i.e., 2.6) we can choose $V_0 \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $e_0 \in \mathrm{E}(\mathbf{A})$ such that $V_0 = e_0(A)$ and $|_{V_0}$ is 0,1–separating on the interval sublattice $I[\alpha, \beta]$. We first establish the truth of (4) and (5) just for this $\langle \alpha, \beta \rangle$-minimal set.

To prove (4) for V_0, we consider the congruence

$$\theta = \widehat{\alpha|_{V_0}} \cap \beta = \{\langle x, y \rangle \in \beta : \langle e_0 f(x), e_0 f(y) \rangle \in \alpha \text{ for all } f \in \mathrm{Pol}_1\mathbf{A}\}.$$

Now $\theta \in I[\alpha, \beta]$ and $\theta|_{V_0} = \alpha|_{V_0}$. This implies that $\theta = \alpha$, since $|_{V_0}$ is 0–separating on $I[\alpha, \beta]$. Thus for each pair $\langle x, y \rangle \in \beta - \alpha$ we have that $\langle x, y \rangle \in \beta - \theta$; and so, by the definition of θ, there must exist $g \in \mathrm{Pol}_1\mathbf{A}$ with $\langle e_0 g(x), e_0 g(y) \rangle \notin \alpha$. The function $f = e_0 g$ satisfies $f(A) \subseteq V_0$ and $\langle f(x), f(y) \rangle \in \beta|_{V_0} - \alpha|_{V_0}$. It follows that $f(A) = V_0$ by the $\langle \alpha, \beta \rangle$-minimality of V_0. We have proved that (4) holds for V_0.

To prove (5) for V_0, we notice that the transitive closure of the relation

$$\alpha \cup \{\langle g(x), g(y) \rangle : \langle x, y \rangle \in \beta|_{V_0},\ g \in \mathrm{Pol}_1\mathbf{A}\}$$

is the congruence $\alpha \vee \Theta(\beta|_{V_0})$ of $\mathbf{A}$. This congruence belongs to the interval lattice $I[\alpha, \beta]$, and obviously $(\alpha \vee \Theta(\beta|_{V_0}))|_{V_0} = \beta|_{V_0}$. Since $|_{V_0}$ is 1–separating on $I[\alpha, \beta]$, it follows that $\beta = \alpha \vee \Theta(\beta|_{V_0})$, as stated by (5).

Now let U be any $\langle\alpha,\beta\rangle$-minimal set. We shall prove that $U \simeq V_0$. This will prove (1), and in the process we shall prove (2), (4), and (5). We choose a $\mu \in \mathrm{Pol}_1\mathbf{A}$ with $\mu(A) = U$ and $\mu(\beta) \not\subseteq \alpha$. By (5) for V_0, there must exist $a, b \in V_0$ and $g \in \mathrm{Pol}_1\mathbf{A}$ such that $\langle a,b\rangle \in \beta$ and $\langle \mu g(a), \mu g(b)\rangle \notin \alpha$. (We use that $\mu^{-1}(\alpha)$ is an equivalence relation and that $\alpha \vee \Theta(\beta|_{V_0}) = \beta \not\subseteq \mu^{-1}(\alpha)$.) The function $\mu_1 = \mu g e_0$ satisfies $\mu_1(A) \subseteq U$ and $\mu_1(\beta) \not\subseteq \alpha$ (since $\langle \mu_1(a), \mu_1(b)\rangle \notin \alpha$). Thus $\mu_1(A) = U$ by the $\langle\alpha,\beta\rangle$-minimality of U. Since $\mu_1 = \mu_1 e_0$, we actually have that $\mu_1(V_0) = \mu_1(A) = U$. Next, to get a polynomial function mapping U onto V_0, we apply (4) for V_0 with $\langle x,y\rangle = \langle \mu_1(a), \mu_1(b)\rangle$. This produces a $\nu \in \mathrm{Pol}_1\mathbf{A}$ with $\nu(A) = V_0$ and $\langle \nu\mu_1(a), \nu\mu_1(b)\rangle \notin \alpha$. Thus $\nu\mu_1(A) = V_0 = \nu(A)$ by the $\langle\alpha,\beta\rangle$-minimality of V_0. Since $\mu_1(A) = U$, we actually have $\nu(U) = \nu(A) = V_0$ as well as $\mu_1(V_0) = \mu_1(A) = U$. The argument can now be completed easily. The function $\mu_1\nu|_U$ is a member of the finite group of all permutations on U, and so there exists an integer $k > 1$ such that $(\mu_1\nu)^k|_U = \mathrm{id}_U$. We write $e = (\mu_1\nu)^k$, $f = \nu$, $g = (\mu_1\nu)^{k-1}\mu_1$. It is now trivial to check that $e = e^2$, $e(A) = U$, $f(U) = V_0$, $g(V_0) = U$, $gf|_U = \mathrm{id}_U$, $fg|_{V_0} = \mathrm{id}_{V_0}$. Thus we have established that $U \simeq V_0$. In this situation, for all $\theta \in \mathrm{Con}\,\mathbf{A}$ we must have $\theta|_U = g(\theta|_{V_0})$ and $\theta|_{V_0} = f(\theta|_U)$. Statement (2) is an obvious corollary of these equalities. Statements (4) and (5) must be true for U, since in proving their validity for V_0, we used only that (2) holds for V_0.

The statements (3) and (6) still remain to be proved. Assume that $U \in \mathrm{M}_{\mathbf{A}}(\alpha,\beta)$, $f \in \mathrm{Pol}_1\mathbf{A}$, and $f(\beta|_U) \not\subseteq \alpha$. Choose $\langle a,b\rangle \in \beta|_U$ with $\langle f(a), f(b)\rangle \notin \alpha$ and apply (4) with $\langle x,y\rangle = \langle f(a), f(b)\rangle$. This gives a $g \in \mathrm{Pol}_1\mathbf{A}$ satisfying $g(A) = U$, $\langle gf(a), gf(b)\rangle \notin \alpha$. We choose $e \in \mathrm{E}(\mathbf{A})$ such that $e(A) = U$ (by (2)). Thus $gf(U) = gfe(A) = U$, by the $\langle\alpha,\beta\rangle$-minimality of U (since $\langle gfe(a), gfe(b)\rangle \notin \alpha$). From $gf(U) = U$ it follows that $|f(U)| = |U|$ and that f maps U one-to-one onto $f(U)$. The calculation that finished the proof of (1) (taking $\mu_1 = g$, $\nu = f$) will show that the inverse function of $f|_U$ is the restriction to $f(U)$ of some polynomial. Hence $f : U \simeq f(U)$, and this fact certainly implies that $f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha,\beta)$. This finishes the proof of (3).

To prove (6), let f be any unary polynomial of $\mathbf{A}$ such that $f(\beta) \not\subseteq \alpha$. By (5) there is a $g \in \mathrm{Pol}_1\mathbf{A}$ and $\langle x,y\rangle \in \beta|_{V_0}$ such that $\langle fg(x), fg(y)\rangle \notin \alpha$. Now this implies that $\langle g(x), g(y)\rangle \notin \alpha$, and so $g(\beta|_{V_0}) \not\subseteq \alpha$. By (3), we have that $g(V_0)$ is an $\langle\alpha,\beta\rangle$-minimal set U. Furthermore, $\langle g(x), g(y)\rangle \in \beta|_U$ implies that $f(\beta|_U) \not\subseteq \alpha$. Now (6) follows by an application of (3). □

Here is a brief history of the origins of tame congruence theory. In [27], Pálfy and Pudlák observed that if $\mathbf{Con}\,\mathbf{A}$ is a simple lattice and if e is an idempotent polynomial function of $\mathbf{A}$, then $\mathbf{Con}\,\mathbf{A}$ must be isomorphic to $\mathbf{Con}\,\mathbf{A}|_{e(A)}$ under the restriction map of Lemma 2.3, provided that $|e(A)| > 1$. They took e to be non-constant with a minimal range (here it was necessary to assume that $\mathbf{A}$ is finite) and proved, under

some further hypotheses on $\mathbf{Con}\,\mathbf{A}$, that $\mathbf{A}|_{e(A)}$ must be *permutational*: every one of its non-constant unary polynomials is a permutation of the set $e(A)$. From here, their reasoning led to a proof of the equivalence of these statements: (i) every finite lattice is isomorphic to the congruence lattice of some finite algebra; (ii) every finite lattice is isomorphic to an interval sublattice of the lattice of subgroups of some finite group. Whether these equivalent statements are actually true is still unknown.

Four years later, McKenzie found another way to exploit these ideas, and developed the first rudimentary version of tame congruence theory (which was reported in [22]). Involved was the discovery that under mild assumptions, all the "minimal sets" $e(A)$ are "polynomially isomorphic", and the collection of these sets behaves somewhat like a geometric structure on the base set of the algebra. Shortly later, during Spring 1982, Pálfy succeeded in writing down a complete list of all the finite permutational algebras (reported in [26]). All of these developments paved the way for an evolution of ideas that accelerated rapidly. Most of the theory presented in this book was discovered during 1983.

Exercises 2.9

(1) Let $\langle \alpha, \beta \rangle$ be a congruence quotient of a finite algebra. Show that if 2.8 (4) and 2.8 (5) are both valid for one $\langle \alpha, \beta \rangle$-minimal set U then $\langle \alpha, \beta \rangle$ is tame.

(2) Let $\langle \alpha, \beta \rangle$ be a tame quotient of a finite algebra $\mathbf{A}$. Show that this modified form of 2.8 (4) is valid.

(4′) For each $\langle x, y \rangle \in \beta - \alpha$ there exist $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $e \in \mathrm{E}(\mathbf{A})$ such that $e(A) = U$ and $\langle e(x), e(y) \rangle \in \beta|_U - \alpha|_U$.

Show that (4′) cannot be strengthened to read "For each $\langle x, y \rangle \in \beta - \alpha$ and $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ there exists $e \in \mathrm{E}(\mathbf{A})$ such that ..." by constructing a three-element unary algebra with tame quotient $\langle 0_A, 1_A \rangle$ for which the strengthened form of (4′) is false.

(3) Assertion (3) of Theorem 2.8 can be strengthened. Show that if $\langle \alpha, \beta \rangle$ is tame, $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, $f \in \mathrm{Pol}_1\mathbf{A}$ then $f(\beta|_U) \not\subseteq \alpha$ *iff* $f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. Show that if $f|_U$ is one-to-one it need not follow that $f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. (There is a three-element unary algebra with exactly three congruences, $0_A < \alpha < 1_A$, in which $\langle \alpha, 1_A \rangle$ is tame and the implication fails for this tame quotient.)

(4) Construct a three-element algebra with precisely three congruences such that $\mathrm{M}_{\mathbf{A}}(0_A, 1_A) = \binom{A}{2}$ (the set of two-element subsets of A) and $\langle 0_A, 1_A \rangle$ is not tame. Which parts of Theorem 2.8 fail to be true in your example?

(5) Give a detailed proof of the following fact. If B and C are nonvoid subsets of an algebra $\mathbf{A}$ and if $f : B \simeq C$ (implying that $f \in \mathrm{Pol}_1\mathbf{A}$) then $f|_B$ is

an isomorphism between the structures $\langle B,\ (\operatorname{Pol}\mathbf{A})|_B,\ \theta|_B\ (\theta \in \operatorname{Con}\mathbf{A})\rangle$ and $\langle C,\ (\operatorname{Pol}\mathbf{A})|_C,\ \theta|_C\ (\theta \in \operatorname{Con}\mathbf{A})\rangle$.

(6) Let $\langle S,\ \cdot\rangle$ be a finite semigroup (such as $\langle \operatorname{Pol}_1\mathbf{A}, \circ\rangle$ for a finite algebra $\mathbf{A}$—where $\circ$ denotes composition of functions). Show that if $x \in S$ then for some integer $k > 0$, $e = x^k$ is idempotent; i.e., $x^{2k} = x^k$. Moreover, there is an integer k such that $x^{2k} = x^k$ for all $x \in S$.

(7) Let $\langle S,\ \cdot\rangle$ be a monoid (semigroup with identity element 1 satisfying $1 \cdot x = x \cdot 1 = x$ for all elements x). An *ideal* in S is a nonvoid set I such that $S \cdot I \cdot S = I$ ($xuy \in I$ whenever $x, y \in S$ and $u \in I$). A quasi-ordering and an equivalence relation are defined on S by setting $x \leq y$ iff $SxS \subseteq SyS$; and $x \sim y$ iff $SxS = SyS$. We put $x < y$ iff $x \leq y$ and $x \not\sim y$.

Now let $\langle \alpha, \beta\rangle$ be a tame quotient in the finite algebra $\mathbf{A}$, and let $\langle S, \cdot\rangle = \langle \operatorname{Pol}_1\mathbf{A}, \circ\rangle$. Set $I = \{f \in S : f(\beta) \subseteq \alpha\}$ and

$$T = \{f \in S : f(A) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta) \text{ and } f \notin I\}.$$

Show that I is an ideal in S, that

$$T = \{f \in S : f \notin I, \text{ but } g < f \text{ implies } g \in I\},$$

and that $T = \{h \in S : h \sim f\}$ for each $f \in T$.

(8) Let $\mathbf{A}$ be any algebra and let $\langle S,\ \cdot\rangle = \langle \operatorname{Pol}_1\mathbf{A}, \circ\rangle$. A right ideal in S is a nonvoid subset K of S such that $K \cdot S = K$. For any right ideal K of S, define a mapping μ_K of $\operatorname{Con}\mathbf{A}$ by

$$\mu_K(\theta) = \{\langle x, y\rangle \in A^2 : \langle f(x), f(y)\rangle \in \theta \text{ for all } f \in K\}.$$

Then prove:

(i) $\mu_K(\theta) \in \operatorname{Con}\mathbf{A}$, $\mu_K(\theta) \supseteq \theta$ for all $\theta \in \operatorname{Con}\mathbf{A}$; and μ_K is a meet endomorphism of $\operatorname{Con}\mathbf{A}$.

(ii) For right ideals K_0, K_1 in S and $\theta \in \operatorname{Con}\mathbf{A}$,

$$\mu_{K_0}(\theta) = \mu_{SK_0}(\theta),\ \mu_{K_0K_1}(\theta) = \mu_{K_1}\mu_{K_0}(\theta),$$
$$\mu_{K_0K_1}(\theta) \supseteq \mu_{K_0}(\theta) \vee \mu_{K_1}(\theta).$$

The following lemma will be the key for connecting the purely lattice theoretic concept of Definition 1.6 to the concept of tame quotient. This lemma has a precursor in [27].

LEMMA 2.10. *Let* $\mathbf{A}$ *be a finite algebra and let* $\alpha < \beta$ *be congruences of* $\mathbf{A}$ *such that the lattice* $I[\alpha, \beta]$ *has no strictly increasing, non-constant, meet endomorphism. Then every* $\langle \alpha, \beta \rangle$*-minimal set is the range of some member of* $\mathrm{E}(\mathbf{A})$.

PROOF. Suppose that $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. Let $K = \{f \in \mathrm{Pol}_1\mathbf{A} : f(A) \subseteq U\}$. We wish to prove that for some $e \in \mathrm{E}(\mathbf{A})$, $e(A) = U$. Define a mapping μ of $I[\alpha, \beta]$ by

$$\mu(\theta) = \beta \wedge \mu_K(\theta) = \{\langle x, y \rangle \in \beta : \langle f(x), f(y) \rangle \in \theta \quad \text{for all} \quad f \in K\} .$$

K is obviously a right ideal of the monoid $\mathrm{Pol}_1\mathbf{A}$. From the last exercise (it is an easy direct argument) we have that μ is an increasing meet endomorphism of the lattice $I[\alpha, \beta]$. Since $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ there exists $h \in K$ such that $h(A) = U$ and $h(\beta) \not\subseteq \alpha$. Consequently, $\mu(\alpha) < \beta$ and μ is non-constant. Thus, from the hypothesis about $I[\alpha, \beta]$, there must exist $\theta \in I[\alpha, \beta]$, $\theta < \beta$, with $\mu(\theta) = \theta$. Then $\mu\mu(\alpha) \leq \mu\mu(\theta) = \theta < \beta$. Since $\mu\mu(\alpha) = \beta \wedge \mu_{K^2}(\alpha)$, we have that $\beta \not\leq \mu_{K^2}(\alpha)$; and so there exist $f, g \in K$ and $\langle x, y \rangle \in \beta$ such that $\langle fg(x), fg(y) \rangle \notin \alpha$. This implies that $g(\beta) \not\subseteq \alpha$ as well as $fg(\beta) \not\subseteq \alpha$; and since $f(A) \subseteq U$, $g(A) \subseteq U$ it follows that $fg(A) = U = g(A)$ by the $\langle \alpha, \beta \rangle$-minimality of U. We now define $e = f^k$ with the integer $k \geq 1$ chosen so that $e^2 = e$. Now $f(U) = fg(A) = U$ so $e(U) = U$. Since $e \in K$ as well, it follows that $e(A) = U$ as desired. □

THEOREM 2.11. *If* α *and* β *are congruences of a finite algebra* $\mathbf{A}$ *such that* $\alpha < \beta$ *and the lattice* $I[\alpha, \beta]$ *is tight, then* $\langle \alpha, \beta \rangle$ *is tame.*

PROOF. We assume that $I[\alpha, \beta]$ is tight and we choose any $\langle \alpha, \beta \rangle$-minimal set U. By the previous lemma, there exists $e \in \mathrm{E}(\mathbf{A})$ with $e(A) = U$. Then the restriction $|_U$, considered only as a map on $I[\alpha, \beta]$, is a lattice homomorphism by Lemma 2.3. We have $\alpha|_U \neq \beta|_U$ since $U = f(A)$ for an $f \in \mathrm{Pol}_1\mathbf{A}$ such that $f(\beta) \not\subseteq \alpha$. Thus $|_U$ is a non-constant lattice homomorphism on $I[\alpha, \beta]$. It must be 0, 1–separating (by Lemma 1.7). Thus $\langle \alpha, \beta \rangle$ is tame (by Definition 2.6). □

Tame congruence theory, based on Definition 2.6 and Theorems 2.8 and 2.11, fills this book. On the other hand, the circle of ideas introduced in the Exercises 2.9 (7–8) will play no further role in the book. Before passing on, let us remark that it might be very worthwhile to attempt a systematic exploitation of those ideas. But that is a path we have not explored.

Our next topic is to be a detailed study of the "$\langle \alpha, \beta \rangle$-minimal algebras" spawned by tame quotients. The operations of several variables in these algebras are quite interesting, and the study will pay rich dividends. In the remainder of this chapter and in Chapter 3, we introduce the necessary concepts to facilitate the study.

DEFINITION 2.12. A finite algebra $\mathbf{C}$ will be called minimal relative to its congruence quotient $\langle \delta, \theta \rangle$, or simply $\langle \delta, \theta \rangle$-**minimal**, iff $C \in \mathrm{M}_{\mathbf{C}}(\delta, \theta)$.

LEMMA 2.13. *Let $\langle \delta, \theta \rangle$ be a congruence quotient of a finite algebra $\mathbf{A}$.*

(1) *$\mathbf{A}$ is $\langle \delta, \theta \rangle$-minimal iff for all $f \in \mathrm{Pol}_1\mathbf{A}$, either f is a permutation of A or $f(\theta) \subseteq \delta$.*
(2) *If $\mathbf{A}$ is $\langle \delta, \theta \rangle$-minimal then $\langle \delta, \theta \rangle$ is tame.*
(3) *If $\langle \delta, \theta \rangle$ is tame and $U \in \mathrm{M}_{\mathbf{A}}(\delta, \theta)$ then the algebra $\mathbf{A}|_U$ is $\langle \delta|_U, \theta|_U \rangle$-minimal.*

PROOF. This proof is quite easy, and is left as an exercise for the reader. In item (3), "tameness" can be replaced by "there exists $e \in \mathrm{E}(\mathbf{A})$ with $U = e(A)$". □

DEFINITION 2.14. A finite algebra $\mathbf{C}$ is called **minimal** iff $\mathbf{C}$ is $\langle 0_C, 1_C \rangle$-minimal, equivalently, $|C| > 1$ and every non-constant $f \in \mathrm{Pol}_1\mathbf{C}$ is a permutation of C. A finite algebra $\mathbf{C}$ is called E-**minimal** iff $|C| > 1$ and every non-constant $e \in \mathrm{E}(\mathbf{C})$ is equal to id_C.

Minimal algebras were termed "permutational" by P.P. Pálfy. E-minimal algebras will not enter our work until somewhat later. Here are a few examples of minimal algebras. A set of permutations acting on a finite set constitutes a minimal algebra. Any finite vector space of more than one element is minimal. Every two-element algebra is minimal. Pálfy proved that there are (up to polynomial equivalence) no other minimal algebras than these. This result will be proved in Chapter 4, as Theorem 4.7.

DEFINITION 2.15. Let $\mathbf{C}$ be $\langle \delta, \theta \rangle$-minimal, and let $\langle \alpha, \beta \rangle$ be tame in $\mathbf{A}$. By a $\langle \delta, \theta \rangle$-**trace** in $\mathbf{C}$ we mean any set $N \subseteq C$ of the form x/θ such that $x/\theta \neq x/\delta$. By an $\langle \alpha, \beta \rangle$-**trace** of $\mathbf{A}$ we mean any set $N \subseteq A$ such that for some $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, $N \subseteq U$ and N is an $\langle \alpha|_U, \beta|_U \rangle$-trace of the $\langle \alpha|_U, \beta|_U \rangle$-minimal algebra $\mathbf{A}|_U$ (i.e., $N = x/\beta \cap U$ for some $x \in U$ such that $x/\beta \cap U \not\subseteq x/\alpha$). The **body** and the **tail** of $\mathbf{C}$ (with respect to $\langle \delta, \theta \rangle$) are defined in this way:

$$\text{body} = \bigcup \{\langle \delta, \theta \rangle\text{-traces}\} ,$$
$$\text{tail} = C - \text{body} .$$

The body and tail of an $\langle \alpha, \beta \rangle$-minimal set U (with respect to $\langle \alpha|_U, \beta|_U \rangle$) are defined the same way.

In Figure 3, we depict an $\langle \alpha, \beta \rangle$-minimal set with four traces. The vertical strips represent $\beta|_U$-classes; while the $\alpha|_U$-classes are represented by ellipses.

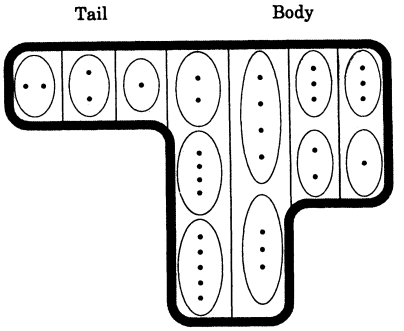


Figure 3
Picture of an $\langle \alpha, \beta \rangle$-minimal set

Here is a lemma relating the concepts introduced in Definitions 2.12, 2.14, and 2.15. For any congruences $\alpha \leq \beta$ in an algebra $\mathbf{A}$, by β/α we understand the congruence θ on $\mathbf{A}/\alpha$ such that $\langle x/\alpha, y/\alpha \rangle \in \theta$ iff $\langle x, y \rangle \in \beta$. For any $f \in \operatorname{Pol} \mathbf{A}$, (say f is n-ary) by f_α we mean the operation on A/α satisfying $f_\alpha(x_0/\alpha, \ldots, x_{n-1}/\alpha) = f(x_0, \ldots, x_{n-1})/\alpha$.

LEMMA 2.16. *Let $\alpha \leq \delta < \theta$ be congruences of a finite algebra $\mathbf{C}$.*

(1) $\operatorname{Pol}\mathbf{C}/\alpha = \{f_\alpha : f \in \operatorname{Pol}\mathbf{C}\}$.

(2) *If $\mathbf{C}$ is $\langle \delta, \theta \rangle$-minimal, then $\mathbf{C}/\alpha$ is $\langle \delta/\alpha, \theta/\alpha \rangle$-minimal.*

(3) *If $\mathbf{C}$ is $\langle \delta, \theta \rangle$-minimal and N is a $\langle \delta, \theta \rangle$-trace, then $\mathbf{C}|_N$ is $\langle \delta|_N, 1_N \rangle$-minimal and $(\mathbf{C}|_N)/(\delta|_N)$ is a minimal algebra isomorphic to $(\mathbf{C}/\delta)|_{(N/\delta)}$.*

PROOF. The set of all operations f on C such that f preserves α and $f_\alpha \in \operatorname{Pol}\mathbf{C}/\alpha$ is easily seen to be closed under compositions, and to contain the constant operations, the trivial projection operations, and the basic operations of $\mathbf{C}$. Thus this set contains $\operatorname{Pol}\mathbf{C}$; and it follows that $f_\alpha \in \operatorname{Pol}\mathbf{C}/\alpha$ whenever $f \in \operatorname{Pol}\mathbf{C}$. By an analogous argument, $\operatorname{Pol}\mathbf{C}/\alpha \subseteq \{f_\alpha : f \in \operatorname{Pol}\mathbf{C}\}$. The two sets are equal, and (1) is proved.

To prove (2), suppose that $\mathbf{C}$ is $\langle \delta, \theta \rangle$-minimal and that $f \in \operatorname{Pol}_1\mathbf{C}/\alpha$ and $f(\theta/\alpha) \not\subseteq (\delta/\alpha)$. By (1), we have that $f = g_\alpha$ for a certain $g \in \operatorname{Pol}_1\mathbf{C}$. There are $x/\alpha, y/\alpha \in \mathbf{C}/\alpha$ such that $\langle x/\alpha, y/\alpha \rangle \in \theta/\alpha$ and $\langle g_\alpha(x/\alpha), g_\alpha(y/\alpha) \rangle \notin \delta/\alpha$. These facts are equivalent to $\langle x, y \rangle \in \theta$, $\langle g(x), g(y) \rangle \notin \delta$. Since $\mathbf{C}$ is $\langle \delta, \theta \rangle$-minimal, g must be a permutation of C. From this it follows that f maps C/α onto itself; since C/α is finite, f is a permutation. This proves that $\mathbf{C}/\alpha$ is $\langle \delta/\alpha, \theta/\alpha \rangle$-minimal.

Now suppose that $\mathbf{C}$ is $\langle \delta, \theta \rangle$-minimal, and let N be a $\langle \delta, \theta \rangle$-trace. Let $f \in \operatorname{Pol}_1\mathbf{C}|_N$ and suppose that $f(N^2) \not\subseteq \delta|_N$. There exists $g \in \operatorname{Pol}_1\mathbf{C}$ with $g(N) \subseteq N$ and $g|_N = f$ (see Exercise 2.5 (2)). Since N is a $\langle \delta, \theta \rangle$-trace, $N^2 \subseteq \theta$; and so $g(\theta) \not\subseteq \delta$, implying

that g is a permutation of C. Thus f is one-to-one on the finite set N, and is itself a permutation of N. This argument shows that $\mathbf{C}|_N$ is $\langle \delta_N, 1_N \rangle$-minimal. Using statement (2) we conclude that $(\mathbf{C}|_N)/(\delta|_N)$ is a minimal algebra. It is easy to see that $(\mathbf{C}|_N)/(\delta|_N) \cong (\mathbf{C}/\delta)|_{N/\delta}$ since $\delta \subseteq \theta$ and N is a θ-equivalence class. □

Here is a simplified picture of an algebra $\mathbf{A}$ with a tame quotient $\langle 0_A, \beta \rangle$. We assume that a $\langle 0_A, \beta \rangle$-minimal set U has exactly three traces and a tail composed of two elements. The vertical lines in the picture accomplish the division of A into the blocks of the equivalence relation β. The $\langle 0_A, \beta \rangle$-traces and tail elements constituting one $\langle 0_A, \beta \rangle$-minimal set are connected by a line in the picture. A number of traces are pictured as white rectangles independently of the $\langle 0_A, \beta \rangle$-minimal set (or sets) which contain them.

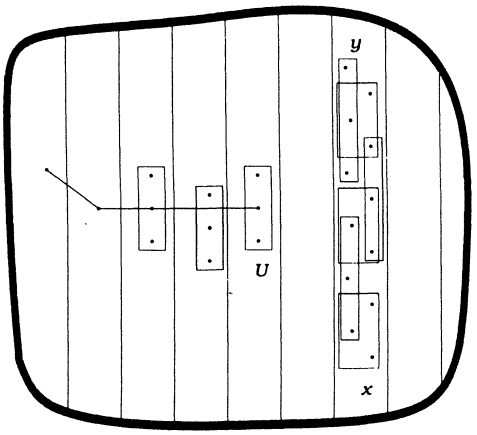


Figure 4

Theorem 2.8 tells us, among other things, that every pair of $\langle 0_A, \beta \rangle$-minimal sets U_0 and U_1 are isomorphic. The isomorphism, induced by a pair of polynomials of $\mathbf{A}$, maps the relation $\beta|_{U_0}$ onto the relation $\beta|_{U_1}$; and thus the traces in U_0 are isomorphic (one for one) with those in U_1. It follows that each $\langle 0_A, \beta \rangle$-minimal set U contains a full representative set of traces with respect to the equivalence relation $\simeq$. Every trace sits inside one block of β. Each block of β is actually *connected* by the traces it contains. That is—in the $\langle 0_A, \beta \rangle$ case—every two elements x and y that are β-equivalent can be connected by a sequence of overlapping traces. (We try to suggest this in Figure 4.) The next lemma formulates this connectivity property more precisely.

LEMMA 2.17. *Let $\langle \alpha, \beta \rangle$ be a tame quotient in a finite algebra $\mathbf{A}$. Define*

$$\rho = \alpha \cup \bigcup \{N^2 : N \text{ is an } \langle \alpha, \beta \rangle\text{-trace}\} .$$

Then β is the transitive closure of ρ.

PROOF. Choose any $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. By 2.8(5), β is the transitive closure of $\rho' = \alpha \cup \{\langle gx, gy \rangle : \langle x, y \rangle \in \beta|_U,\ g \in \mathrm{Pol}_1\mathbf{A}\}$. Suppose that $\langle x, y \rangle \in \beta|_U$, $g \in \mathrm{Pol}_1\mathbf{A}$, and $\langle g(x), g(y) \rangle \notin \alpha$. Then $\langle x, y \rangle \notin \alpha$, and $x/\beta \cap U = N$ is a trace with $x, y \in N$. Also $g : U \simeq g(U)$ by 2.8(3), and $g(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. In this situation, $g(N) = M$ is a trace. Thus $\langle g(x), g(y) \rangle \in \rho$. We conclude that $\rho' \subseteq \rho$, so the transitive closure of ρ contains that of ρ', which is β. Since obviously $\rho \subseteq \beta$, then β is the transitive closure of ρ. □

Our strategy for discovering what the algebras $\mathbf{A}|_U$ ($U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$) determined by a tame quotient $\langle \alpha, \beta \rangle$ may be like, will be to first study a special case. That will be when $\alpha = 0_A$ and U is equal to its only trace, so $\mathbf{A}|_U$ is a minimal algebra. From this we can build toward an understanding of the general case, using Lemma 2.16 and the following lemma.

LEMMA 2.18. *Let $\delta \leq \alpha < \beta$ be congruences of a finite algebra $\mathbf{A}$. Then $\langle \alpha, \beta \rangle$ is a tame quotient of $\mathbf{A}$ iff $\langle \alpha/\delta, \beta/\delta \rangle$ is a tame quotient of $\mathbf{A}/\delta$. If $\langle \alpha, \beta \rangle$ is tame, we have*

$$\mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta) = \{U/\delta : U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)\} .$$

Moreover, for an $\langle \alpha, \beta \rangle$-minimal set U, the $\langle \alpha/\delta, \beta/\delta \rangle$ traces in U/δ are just the sets N/δ where N is an $\langle \alpha, \beta \rangle$ trace in U.

PROOF. Throughout the argument we use the easily proved fact that for any $f \in \mathrm{Pol}_1\mathbf{A}$, $f(\beta) \not\subseteq \alpha$ iff $f_\delta(\beta/\delta) \not\subseteq \alpha/\delta$; and we also use the fact that $\mathrm{Pol}_1\mathbf{A}/\delta = \{f_\delta : f \in \mathrm{Pol}_1\mathbf{A}\}$.

Let us assume that $\langle \alpha, \beta \rangle$ is tame and choose any $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. By 2.8(2), there is $e \in \mathrm{E}(\mathbf{A})$ with $U = e(A)$. We must show that $U/\delta \in \mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta)$. First, note that $e_\delta \in \mathrm{E}(\mathbf{A}/\delta)$ and $e_\delta(A/\delta) = U/\delta$ and $e_\delta(\beta/\delta) \not\subseteq \alpha/\delta$. Second, let f_δ ($f \in \mathrm{Pol}_1\mathbf{A}$) be any unary polynomial of $\mathbf{A}/\delta$ such that $f_\delta(A/\delta) \subseteq U/\delta$ and $f_\delta(\beta/\delta) \not\subseteq \alpha/\delta$. Notice that $f_\delta = e_\delta \circ f_\delta = (ef)_\delta$, and so $ef(\beta) \not\subseteq \alpha$. Thus $ef(A) = U$, and this implies that $f_\delta(A/\delta) = (ef)_\delta(A/\delta) = U/\delta$. We can now conclude that $U/\delta \in \mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta)$.

In order to see that $\langle \alpha/\delta, \beta/\delta \rangle$ is tame, we consider the restriction mapping of $I[\alpha/\delta, \beta/\delta]$ in $\mathrm{Con}\,\mathbf{A}/\delta$ into $\mathrm{Con}((\mathbf{A}/\delta)|_{U/\delta})$. It will be sufficient to show that it is 0,1–separating, since we already know that $U/\delta \in \mathrm{M}_{\mathbf{A}}(\alpha/\delta, \beta/\delta)$ and U/δ is the range of an idempotent polynomial of $\mathbf{A}/\delta$. Every congruence of $\mathbf{A}/\delta$ has the form μ/δ for a $\mu \geq \delta$ in $\mathrm{Con}\,\mathbf{A}$. Suppose that $\alpha \leq \mu < \beta$ in $\mathrm{Con}\,\mathbf{A}$. Since $\langle \alpha, \beta \rangle$ is tame, there exists $\langle x, y \rangle \in \beta|_U - \mu|_U$. We have $\langle x/\delta, y/\delta \rangle \in (\beta/\delta - \mu/\delta) \cap (U/\delta)^2$. This

shows that the restriction map is 1–separating on $I[\alpha/\delta, \beta/\delta]$, and the proof that it is 0–separating is essentially the same. We have now proved that $\langle \alpha/\delta, \beta/\delta \rangle$ is tame and (since U was arbitrary) that $U/\delta \in \mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta)$ whenever $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$.

To get the other inclusion, let W be any member of $\mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta)$. Choose any $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. Applying 2.8 (1) to the tame quotient $(\alpha/\delta, \beta/\delta)$, we get that there is f_δ ($f \in \mathrm{Pol}_1\mathbf{A}$) with $f_\delta : U/\delta \simeq W$. In this situation, $f_\delta(\beta/\delta) \not\subseteq \alpha/\delta$, so $f(\beta) \not\subseteq \alpha$; and by 2.8 (3) $f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. Furthermore, $W = f_\delta(U/\delta) = f(U)/\delta$. This concludes our proof that $\mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta) = \mathrm{M}_{\mathbf{A}}(\alpha, \beta)/\delta$.

We now change our assumptions. Let us suppose that $\langle \alpha/\delta, \beta/\delta \rangle$ is a tame quotient of $\mathbf{A}/\delta$. We choose an arbitrary $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $f \in \mathrm{Pol}_1\mathbf{A}$ such that $f(A) = U$, $f(\beta) \not\subseteq \alpha$. Then $f_\delta(\beta/\delta) \not\subseteq \alpha/\delta$, so by 2.8 (6) applied to $\langle \alpha/\delta, \beta/\delta \rangle$ there is $W \in \mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta)$ with $f_\delta : W \simeq f_\delta(W)$. Thus there exists g_δ ($g \in \mathrm{Pol}_1\mathbf{A}$) such that $f_\delta : W \to f_\delta(W)$, $g_\delta : f_\delta(W) \to W$ are inverse bijections. Let $e = (fg)^n$ be an idempotent power of fg. Now e_δ equals the identity on $f_\delta(W)$, hence $e(\beta) \not\subseteq \alpha$. We conclude that $e(A) = f(A) = U$ since U is $\langle \alpha, \beta \rangle$-minimal. To finish the proof that $\langle \alpha, \beta \rangle$ is tame, we show that U/δ is an $\langle \alpha/\delta, \beta/\delta \rangle$-minimal set, and using the fact that $|_{U/\delta}$ must then be $0, 1$–separating on $I[\alpha/\delta, \beta/\delta]$, we show that $|_U$ is $0, 1$–separating on $I[\alpha, \beta]$. These details are left to the reader. □

Exercises 2.19

(1) Suppose that U is an $\langle \alpha, \beta \rangle$-minimal set for a congruence quotient $\langle \alpha, \beta \rangle$ in a finite algebra $\mathbf{A}$, and that $U = e(A)$ for some $e \in \mathrm{E}(\mathbf{A})$. For every $\alpha|_U \leq \delta' < \gamma' \leq \beta|_U$ ($\delta', \gamma' \in \mathrm{Con}\,\mathbf{A}|_U$), there exists at least one pair $\langle \delta, \gamma \rangle$ of congruences of $\mathbf{A}$ such that $\delta|_U = \delta'$, $\gamma|_U = \gamma'$, $\alpha \leq \delta < \gamma \leq \beta$, and the lattice homomorphism $|_U$ is $0, 1$–separating on $I[\delta, \gamma]$. Show that each such quotient $\langle \delta, \gamma \rangle$ is tame, and that $U \in \mathrm{M}_{\mathbf{A}}(\delta, \gamma) \subseteq \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. (Moreover, $\mathrm{M}_{\mathbf{A}}(\delta, \gamma) = \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ if $\langle \alpha, \beta \rangle$ is tame.)

(2) Suppose that $\alpha \leq \delta \prec \beta$ where α, δ, β are congruences of a finite algebra $\mathbf{A}$. Thus $\langle \delta, \beta \rangle$ is tame, according to Theorem 2.11. Show that if $\langle \alpha, \beta \rangle$ is tame then $\mathrm{M}_{\mathbf{A}}(\alpha, \beta) = \mathrm{M}_{\mathbf{A}}(\delta, \beta)$.

(3) Suppose that $\langle \alpha_i, \beta_i \rangle$ ($i = 0, 1$) are congruence quotients of a finite algebra $\mathbf{A}$ and $\alpha_0 = \beta_0 \wedge \alpha_1$, $\beta_1 = \beta_0 \vee \alpha_1$. Prove that $\mathrm{M}_{\mathbf{A}}(\alpha_0, \beta_0) = \mathrm{M}_{\mathbf{A}}(\alpha_1, \beta_1)$, and $\mathrm{M}_{\mathbf{A}}(\alpha_0, \beta_1) \subseteq \mathrm{M}_{\mathbf{A}}(\alpha_0, \beta_0) \cup \mathrm{M}_{\mathbf{A}}(\alpha_0, \alpha_1)$. Conclude that if $\mathbf{Con}\,\mathbf{A} \cong \mathbf{M}_3$ then (all seven congruence quotients are tame and) $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ is independent of the quotient $\langle \alpha, \beta \rangle$.

(4) Prove that when $\langle \alpha, \beta \rangle$ is tame and $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, then $\alpha \prec \beta$ iff $\alpha|_U \prec \beta|_U$. Thus $\alpha \prec \beta$ if $|U| = 2$. Show that if $\mathbf{A}$ is a finite lattice and $\alpha < \beta$ in $\mathrm{Con}\,\mathbf{A}$ then every $\langle \alpha, \beta \rangle$-minimal set has only two elements—thus $\langle \alpha, \beta \rangle$ is tame iff $\alpha \prec \beta$.

(5) Let $\mathbf{M}$ be a finite module over a finite ring $\mathbf{R}$ with 1, and suppose that $\mathbf{M}$ is unitary, i.e., $1 \cdot x = x$ for $x \in M$. We regard $\mathbf{M}$ as an algebra

$$\langle M, x + y, 0, r \cdot x \,(r \in R)\rangle.$$

Let $\alpha < \beta$ be congruences of $\mathbf{M}$, and let $M_\alpha = 0/\alpha$, $M_\beta = 0/\beta$ be the associated submodules of $\mathbf{M}$. Put $\operatorname{ann}(M_\alpha \mid M_\beta) = \{r \in R : r \cdot M_\beta \subseteq M_\alpha\}$. Then show that $\langle \alpha, \beta \rangle$ is tame iff $\operatorname{ann}(M_\alpha \mid M_\beta)$ is a maximal ideal in $\mathbf{R}$.

(6) Suppose that $\langle \alpha, \beta \rangle$ is a tame quotient of a finite algebra $\mathbf{A}$, that N is an $\langle \alpha, \beta \rangle$-trace (see Definition 2.15), and that $f \in \operatorname{Pol}_1 \mathbf{A}$. Prove that either $f(N^2) \subseteq \alpha$, or $f(N)$ is an $\langle \alpha, \beta \rangle$-trace N' and $f : N \simeq N'$. (See Theorem 2.8 (3).)

3. ABELIAN AND SOLVABLE ALGEBRAS

Our concept of solvability (of algebras and of congruences) is central in tame congruence theory. This concept is a generalization of the one employed in group theory. In otherwords, a group is solvable iff it is solvable in our sense.

This chapter contains only definitions and their trivial consequences. It can be skimmed, or skipped over and revisited when these concepts next appear. Our theorems on solvability are proved in Chapter 7, but the concept will be needed in Chapter 4. The concepts defined here may seem a little strange, but since they have many applications, it is worth an effort to master them.

DEFINITION 3.1. An algebra $\mathbf{A}$ will be called **Abelian** iff for every $n > 1$, and for every n-ary polynomial operation f of $\mathbf{A}$, and for all $u, v, x_1, \ldots, x_{n-1}, y_1, \ldots, y_{n-1}$ in $\mathbf{A}$, this equivalence holds:

$$f(u, x_1, \ldots, x_{n-1}) = f(u, y_1, \ldots, y_{n-1}) \tag{3.1.1}$$
$$\longleftrightarrow f(v, x_1, \ldots, x_{n-1}) = f(v, y_1, \ldots, y_{n-1}) .$$

Exercises 3.2

(1) Prove that a group is Abelian in our sense iff it is commutative. Prove that a ring is Abelian in our sense iff it satisfies $x \cdot y = 0$ (i.e., has a trivial multiplication).

(2) Prove that every module over a ring is Abelian.

(3) Suppose that $\mathbf{A}$ is Abelian and has a polynomial operation $p(x, y, z)$ such that $p(x, x, y) = p(y, x, x) = y$ identically for all $x, y \in A$. Prove that $\mathbf{A}$ is polynomially equivalent to a module, i.e., that there exists a module $\mathbf{M} = \langle A, +, \ldots \rangle$ over some ring satisfying $\mathrm{Pol}\,\mathbf{A} = \mathrm{Pol}\,\mathbf{M}$. [Proof outline: Choose any element in A, call it 0. Define $x + y = p(x, 0, y)$. Letting $f(x, y, z) = p(y, x, z)$ and using that $f(y, y, x) = f(y, x, y)$, and the Abelian property, conclude that $f(z, y, x) = f(z, x, y)$ for all x, y, z. In particular, $x + y = y + x$. Obviously $x + 0 = 0 + x = x$. Show next that $x + p(0, x, 0) = 0$ and that $+$ satisfies the associative law. Thus we have an Abelian group $\langle A, +, 0 \rangle$. To find the ring, observe that if what is to be proved is in fact true, then the $h \in \mathrm{Pol}_1\mathbf{A}$ satisfying $h(0) = 0$ must be precisely the operations expressible in the module in the form $h(x) = r \cdot x$ for some ring element r.]

(4) Let $\mathbf{A}$ be a module and $p(x,y,z)$ be a ternary polynomial of $\mathbf{A}$ satisfying the equations $p(x,x,y) = p(y,x,x) = y$ identically. Show that $p(x,y,z)$ can be none other than $x - y + z$.

(5) Let $\mathbf{A}$ be any algebra and define the **center** of $\mathbf{A}$, or $Z(\mathbf{A})$, to be the set of all pairs $\langle u,v\rangle \in A^2$ such that formula (3.1.1) holds for this u,v and for all $f \in \operatorname{Pol}\mathbf{A}$ and all elements $x_1,\dots,y_1,\dots$ in A. Prove that $Z(\mathbf{A})$ is a congruence of $\mathbf{A}$, and that $\mathbf{A}$ is Abelian iff $Z(\mathbf{A}) = A^2$. Show that if $\mathbf{A} = \langle A,\cdot,^{-1}\rangle$ is a group then

$$Z(\mathbf{A}) = \{\langle u,v\rangle : u\cdot v^{-1}\cdot x = x\cdot u\cdot v^{-1} \text{ for all } x \in A\}.$$

DEFINITION 3.3. Let α,β,δ be congruences of an algebra $\mathbf{A}$. We use the formula $C(\alpha,\beta;\delta)$ (in words, α **centralizes** β **modulo** δ) as an abbreviation for the following property. For every $n > 1$, for every $f \in \operatorname{Pol}_n\mathbf{A}$, and for all $\langle u,v\rangle \in \alpha$ and $\langle x_1,y_1\rangle,\dots,\langle x_{n-1},y_{n-1}\rangle \in \beta$, this equivalence holds:

$$\begin{aligned} f(u,x_1,\dots,x_{n-1}) &\overset{\delta}{\equiv} f(u,y_1,\dots,y_{n-1}) \\ \longleftrightarrow\ f(v,x_1,\dots,x_{n-1}) &\overset{\delta}{\equiv} f(v,y_1,\dots,y_{n-1}). \end{aligned} \tag{3.3.1}$$

PROPOSITION 3.4. *For any algebra* $\mathbf{A}$ *and congruences* α,α_i $(i \in I),\dots,\theta$ *on* $\mathbf{A}$, *the following hold.*

(1) *If* $C(\alpha,\beta;\delta)$ *and* $\alpha' \le \alpha$, $\beta' \le \beta$ *then* $C(\alpha',\beta';\delta)$.

(2) *If* $C(\alpha_i,\beta;\delta)$ *for all* $i \in I$, *then* $C(\bigvee_{i\in I}\alpha_i,\beta;\delta)$.

(3) *If* $C(\alpha,\beta;\delta_j)$ *for all* $j \in J$, *then* $C(\alpha,\beta;\bigwedge_{j\in J}\delta_j)$.

(4) *If* $\alpha\wedge\beta \le \delta \le \alpha$ *or* $(\alpha\vee\delta)\wedge\beta \le \delta$, *then* $C(\alpha,\beta;\delta)$.

(5) *If* $\theta \le \alpha\wedge\beta\wedge\delta$ *then* $C(\alpha,\beta;\delta)$ *is equivalent to* $C(\alpha/\theta,\beta/\theta;\delta/\theta)$ *(holding in* $\mathbf{A}/\theta$*).*

PROPOSITION 3.5. *(Let* $\alpha,\beta,\delta \in \operatorname{Con}\mathbf{A}$.*)* $C(\alpha,\beta;\delta)$ *is equivalent to the following property. For all positive integers* k,m *and for all* $f \in \operatorname{Pol}_{k+m}\mathbf{A}$ *and all* $\bar u,\bar v \in A^k$ *and* $\bar x,\bar y \in A^m$ *such that* $u_i \overset{\alpha}{\equiv} v_i$ *(for* $i < k$*) and* $x_j \overset{\beta}{\equiv} y_j$ *(for* $j < m$*) we have:* $f(\bar u,\bar x) \overset{\delta}{\equiv} f(\bar u,\bar y)$ *iff* $f(\bar v,\bar x) \overset{\delta}{\equiv} f(\bar v,\bar y)$. *Pictorially*

DEFINITION 3.6. Let α and β be congruences of an algebra $\mathbf{A}$ with $\alpha \leq \beta$.

(1) β is **Abelian over** α iff $C(\beta, \beta; \alpha)$.
(2) β is **Abelian** iff $C(\beta, \beta; 0_A)$.
(3) β is **solvable over** α iff there exists a finite chain of congruences $\alpha_0 \leq \alpha_1 \leq \cdots \leq \alpha_n$ such that $\alpha_0 = \alpha$, $\alpha_n = \beta$ and α_{i+1} is Abelian over α_i for each $i < n$.
(4) β is **solvable** iff β is solvable over 0_A.
(5) $\mathbf{A}$ is **solvable** iff 1_A is a solvable congruence of $\mathbf{A}$.
(6) A quotient $\langle \delta, \gamma \rangle$ is called **Abelian** (or **solvable**) iff γ is Abelian (or solvable) over δ.

PROPOSITION 3.7. *For congruences over any algebra* $\mathbf{A}$*, these statements are valid.*

(1) *If* $\langle \alpha, \beta \rangle$ *and* $\langle \beta, \delta \rangle$ *are solvable quotients, then so is* $\langle \alpha, \delta \rangle$.
(2) *If* $\alpha \leq \delta \leq \beta$ *and* β *is solvable (Abelian) over* α*, then* δ *is solvable (Abelian) over* α *and* $\beta \wedge \gamma$ *is solvable (Abelian) over* $\alpha \wedge \gamma$ *for every congruence* γ.
(3) *If* $\delta \leq \alpha \leq \beta$ *then* β *is solvable (Abelian) over* α *iff* β/δ *is solvable (Abelian) over* α/δ.
(4) $\mathbf{A}/\delta$ *is solvable (or Abelian) iff* 1_A *is solvable (or Abelian) over* δ.

Exercises 3.8

(1) Prove all the assertions in Propositions 3.4, 3.5 and 3.7.
(2) Show that 3.4 (2) implies that for any congruences β and δ of an algebra $\mathbf{A}$, there is a largest congruence α, which we might denote by $\operatorname{ann}(\delta \mid \beta)$, satisfying $C(\alpha, \beta; \delta)$. Notice that $\operatorname{ann}(0_A \mid 1_A) = Z(\mathbf{A})$, the central congruence defined in Exercise 3.2 (5). Find a definition of the statement "$\langle u, v \rangle \in \operatorname{ann}(\delta \mid \beta)$," which parallels the definition of "$\langle u, v \rangle \in Z(\mathbf{A})$" .
(3) Show that 3.4 (3) implies that for any congruences α and β of an algebra $\mathbf{A}$, there is a smallest congruence δ satisfying $C(\alpha, \beta; \delta)$. Denote this congruence by $[\alpha, \beta]$ and call it the **commutator** of α and β. There is an extensive and rather deep theory of this operation $[\ ,\ ]$ for congruences of algebras that belong to congruence modular varieties. (As a first reference, consult [11] or [16].) If $\mathbf{A}$ belongs to such a variety then $[\ ,\ ]$, as a binary operation on $\operatorname{Con}\mathbf{A}$, is monotone, commutative, and completely join preserving in each of its variables. But for algebras not belonging to congruence modular varieties, this commutator operation cannot be expected to be particularly well-behaved. The exercise is to show that for any group $\mathbf{A} = \langle A, \cdot, ^{-1} \rangle$ and for any two congruences α, β of $\mathbf{A}$ with associated normal subgroups N_α, N_β (i.e., $\alpha = \{\langle u, v \rangle : u \cdot v^{-1} \in N_\alpha\}$, etc.), the commutator $[\alpha, \beta]$ has for its associated normal subgroup the subgroup generated by $\{u^{-1}v^{-1}uv : u \in N_\alpha,\ v \in N_\beta\}$.

(4) Let $\mathbf{A}$ be an algebra with a polynomial $p(x, y, z)$ satisfying $p(x, x, y) = y = p(y, x, x)$ identically. Show that for any congruences α, β, δ of $\mathbf{A}$, $C(\alpha, \beta; \delta)$ is equivalent to $C(\beta, \alpha; \delta)$. Thus $[\alpha, \beta] = [\beta, \alpha]$.

(5) Show that an absolutely free algebra of the type of groups, with infinitely many free generators, has the following properties: $\mathbf{F}$ is Abelian; $\mathbf{F}$ has non-solvable homomorphic images. (In Chapter 7, we prove that an algebra with these properties cannot be finite.)

(6) Any group whose lattice of normal subgroups is $\mathbf{M}_3$ must be Abelian; in fact, must be a four-element group isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$. There exists a non-Abelian algebra $\mathbf{A}$ satisfying $\mathbf{Con}\,\mathbf{A} \cong \mathbf{M}_3$. (In Corollary 5.8, we shall find that every such algebra is infinite.) Prove that if $\mathbf{Con}\,\mathbf{A} \cong \mathbf{M}_3$ then each of the prime quotients $\langle 0_A, \alpha \rangle$ of $\mathbf{A}$ is Abelian.

DEFINITION 3.9. Let α and β be congruences of an algebra $\mathbf{A}$ such that $\alpha \leq \beta$. We say that β is **strongly Abelian over** α (or if $\alpha < \beta$, we say that $\langle \alpha, \beta \rangle$ is **strongly Abelian**) iff the following property holds. For every $n > 1$, for every $f \in \mathrm{Pol}_n \mathbf{A}$, and for all $x_0 \overset{\beta}{\equiv} y_0$, $x_1 \overset{\beta}{\equiv} y_1 \overset{\beta}{\equiv} z_1, \ldots, x_{n-1} \overset{\beta}{\equiv} y_{n-1} \overset{\beta}{\equiv} z_{n-1}$, this implication is valid:

$$(3.9.1) \qquad f(x_0, \ldots, x_{n-1}) \overset{\alpha}{\equiv} f(y_0, \ldots, y_{n-1}) \rightarrow f(x_0, z_1, \ldots, z_{n-1}) \overset{\alpha}{\equiv} f(y_0, z_1, \ldots, z_{n-1}) .$$

DEFINITION 3.10.

(1) A congruence $\beta \in \mathrm{Con}\,\mathbf{A}$ is **strongly Abelian** iff β is strongly Abelian over 0_A.

(2) An algebra $\mathbf{A}$ is **strongly Abelian** iff 1_A is a strongly Abelian congruence.

(3) If $\alpha \leq \beta$ we say that β is **strongly solvable over** α iff there is a finite chain of congruences $\alpha = \alpha_0 \leq \alpha_1 \leq \cdots \leq \alpha_n = \beta$ with α_{i+1} strongly Abelian over α_i for all $i < n$.

The notions of strongly solvable congruence and of strongly solvable algebra are defined in the obvious fashion.

PROPOSITION 3.11. *For congruences over any algebra* $\mathbf{A}$, *these statements are valid.*

(1) *If* β *is strongly Abelian over* α, *then* β *is Abelian over* α.

(2) *If* β *is strongly Abelian over* α, *and over each of* α_i $(i \in I)$, *and if* $\alpha \leq \beta' \leq \beta$, *then* β' *is strongly Abelian over* α *and* β *is strongly Abelian over* $\bigwedge_{i \in I} \alpha_i$.

(3) *If* $\delta \leq \alpha \leq \beta$, *then* β *is strongly Abelian over* α *iff* β/δ *is strongly Abelian over* α/δ.

Strongly Abelian congruence quotients $\langle\alpha,\beta\rangle$, $\alpha < \beta$, do not occur in most "normal" algebras. For example, they do not occur in groups, rings, modules, or lattices. They do occur, however, in semigroups (see Exercise 9.20 (7)). Every congruence quotient of a unary algebra is strongly Abelian. The strongly Abelian prime quotients lie at one extreme end of the discrete spectrum of quotient types depicted by tame congruence theory. The concept is important in our theory, but primarily in the negative sense of a bad example we wish to exclude. The non-appearance of strongly Abelian prime quotients in the finite algebras of a locally finite variety $\mathcal{V}$ is equivalent to a rather weak condition on the set of equations that hold in $\mathcal{V}$ (see Theorem 9.6).

Exercises 3.12

(1) Prove Proposition 3.11.

(2) Prove that no congruence quotient $\langle\alpha,\beta\rangle$, $\alpha < \beta$, of a group, ring, or lattice can be strongly Abelian.

(3) Construct a five-element algebra $\mathbf{E} = \langle E, \circ\rangle$ with one binary operation, such that $\mathbf{E}$ is strongly Abelian and has a four-element homomorphic image which is not Abelian.

(4) Let $\mathbf{A}$ be an algebra, k be a positive integer. Construct an algebra $\mathbf{A}^{[k]} = \langle A^k, \dots\rangle$ in such a way that the basic operations of $\mathbf{A}^{[k]}$ are those of the algebra $\mathbf{A}^k$ (Cartesian power) together with two new operations d (k-ary) and p (unary) defined as follows (where $\bar{x}^i = \langle x_0^i, \dots, x_{k-1}^i\rangle$):

$$d(\bar{x}^0, \dots, \bar{x}^{k-1}) = \langle x_0^0, x_1^1, \dots, x_{k-1}^{k-1}\rangle ,$$
$$p(\langle x_0, \dots, x_{k-1}\rangle) = \langle x_1, \dots, x_{k-1}, x_0\rangle .$$

Prove that if $\mathbf{Q}$ is a unitary module over a ring $\mathbf{R}$, and if $\mathbf{Q}'$ is Q^k construed in the natural fashion as a module over the k-by-k matrix ring $\mathbf{M}_k(\mathbf{R})$, then $\operatorname{Clo}\mathbf{Q}^{[k]} = \operatorname{Clo}\mathbf{Q}'$, and hence $\operatorname{Pol}\mathbf{Q}^{[k]} = \operatorname{Pol}\mathbf{Q}'$. (For any algebra $\mathbf{A}$, we call $\mathbf{A}^{[k]}$ the k-th **matrix power** of $\mathbf{A}$.)

(5) (Notation as in the last exercise.) For any algebra $\mathbf{A}$, characterize $\operatorname{Clo}\mathbf{A}^{[k]}$ (the clone of term operations) and $\operatorname{Pol}\mathbf{A}^{[k]}$ (the clone of polynomial operations), and show that $\mathbf{A}$ is Abelian or strongly Abelian iff $\mathbf{A}^{[k]}$ has the same property.

4. THE STRUCTURE OF MINIMAL ALGEBRAS

In this chapter, we delineate the five basic types of relative minimal algebras (i.e., $\langle \delta, \theta \rangle$-minimal algebras). Our five-fold classification will extend to a five-fold classification of tame congruence quotients. The first task is to classify minimal algebras, and show that the minimal algebras derived from the traces of a $\langle \delta, \theta \rangle$-minimal algebra must all have the same type. The detailed information about the structure of $\langle \delta, \theta \rangle$-minimal algebras compiled in this chapter is a basic and essential component of tame congruence theory. (All concepts mentioned in this paragraph were defined near the end of Chapter 2.)

We begin with three basic lemmas which will be needed in this chapter. To state and prove the first one, we require some special notation. Let $A_0, \ldots, A_{n-1}, A$ be sets and $I \subseteq \{0, 1, \ldots, n-1\}$, $g : \prod\{A_i : i \in I\} \to A$. The variables of g are x_i ranging over A_i, for $i \in I$. Suppose that $J \subseteq I$ and $\bar{a} \in \prod\{A_i : i \in J\}$. Then by $g[\bar{a}, J]$ we mean the function $g' : \prod\{A_i : i \in I - J\} \to A$ such that $g'(\bar{b}) = g(\bar{a} \cup \bar{b})$ where $\bar{a} \cup \bar{b}$ is a_j for $j \in J$ and b_i for $i \in I - J$. In case $J = \{j\}$ and $a \in A_j$ we simply write $g[a, j]$ for $g[\langle a \rangle, \{j\}]$. The variables of $g[\bar{a}, J]$ are x_i, $i \in I - J$. We say that g **depends on** x_i, where $i \in I$, iff there exists $\bar{a} \in \prod\{A_k : k \in I,\ k \neq i\}$ such that $g[\bar{a}, I - \{i\}]$ is not constant. The first lemma is due to A. Salomaa [31].

LEMMA 4.1. *Let $f : A_0 \times \cdots \times A_{n-1} \to A$ depend on all its variables, where $n \geq 2$. There exist $i < j < n$ and $a \in A_i$, $b \in A_j$, such that $f[a, i]$ and $f[b, j]$ each depend on all their variables.*

PROOF. For any $i < n$ and $a \in A_i$, let $D(a, i)$ be the set of all $j < n$, $j \neq i$ such that $f[a, i]$ depends on x_j. If $|\{i_0, i_1, i_2\}| = 3$ and $a \in A_{i_0}$, $b \in A_{i_1}$ are such that $i_1 \notin D(a, i_0)$, $i_2 \in D(a, i_0)$, then it is easy to see that $i_2 \in D(b, i_1)$. In other words, $i_1 \notin D(a, i_0)$, $i_1 \neq i_0$ imply $D(a, i_0) \subseteq D(b, i_1)$. We shall use this observation several times. A second observation is that for all $i \neq j$ there is $a \in A_i$ such that $j \in D(a, i)$ (since f depends on x_j).

For any $j < n$, choose $i < n$ and $a \in A_i$ such that $j \in D(a, i)$ and $|D(a, i)| \geq |D(b, k)|$ whenever $k < n$, $b \in A_k$ and $j \in D(b, k)$. (In other words, $|D(a, i)|$ is maximal for $j \in D(a, i)$.) We claim that $k \in D(a, i)$ for all $k < n, k \neq i$. Suppose that this fails, say $k \neq i, k \notin D(a, i)$. Then we can choose $b \in A_k$ with $i \in D(b, k)$. Now $\{i\} \cup D(a, i) \subseteq D(b, k)$, which contradicts the choice of a and i. The claim is valid, and so $f[a, i]$ depends on all $n - 1$ of its variables, including x_j.

From the above considerations, there must exist $i_0 < n$, $b \in A_{i_0}$ for which $f[b, i_0]$ depends on all $n-1$ variables. Taking $j = i_0$, there must exist $i_1 \neq i_0$, $a \in A_{i_1}$ for which $f[a, i_1]$ depends on all its variables. □

COROLLARY 4.2. *Let* $\mathbf{A}$ *be an algebra and* n *be a positive integer, and suppose that* $\mathbf{A}$ *has a polynomial operation that depends on at least* n *variables. For each* k, $1 \leq k \leq n$, $\mathbf{A}$ *has a* k*-ary polynomial operation that depends on all* k *variables.*

If f is any n-ary operation on a set A, $i < n$, and $\bar{a} = \langle a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{n-1} \rangle \in A^{n-1}$, we can form the unary operation $g = f[\bar{a}, \{j < n : j \neq i\}]$ by substituting a_j for the j-th variable of f, for all $j \neq i$ (see the preliminaries to Lemma 4.1). In otherwords, $g(x) = f(a_0, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_{n-1})$. We will be dealing with iterates of this operation.

DEFINITION 4.3. Let f be an n-ary operation and $i < n$. We define an operation $f^k_{(i)}(x_0, \ldots, x_{n-1})$ by induction on $k \geq 0$. We put $f^0_{(i)}(x_0, \ldots, x_{n-1}) = x_i$, and $f^1_{(i)}(x_0, \ldots, x_{n-1}) = f(x_0, \ldots, x_{n-1})$, and for each k,

$$f^{k+1}_{(i)}(x_0, \ldots, x_{n-1}) = f(x_0, \ldots, x_{i-1}, f^k_{(i)}(x_0, \ldots, x_{n-1}), x_{i+1}, \ldots, x_{n-1}).$$

LEMMA 4.4. *Let* f *be an* n*-ary operation on a finite set* A *and let* $i < n$. *There exists an integer* $k > 0$ *such that*

$$\begin{aligned} f^k_{(i)}(x_0, \ldots, x_{n-1}) &= f^{2k}_{(i)}(x_0, \ldots, x_{n-1}) \\ &= f^k_{(i)}(x_0, \ldots, x_{i-1}, f^k_{(i)}(x_0, \ldots, x_{n-1}), x_{i+1}, \ldots, x_{n-1}) \end{aligned}$$

for all $x_0, \ldots, x_{n-1}$ *in* A.

PROOF. We can suppose that A has cardinality m. Let $g \in A^A$ be any function mapping A into A. For each $a \in A$ there is a repetition in the sequence $a, g(a), g^2(a), \ldots, g^m(a)$. Thus for some $u < m$ and $1 \leq v \leq m$ we have $g^u(a) = g^{u+v}(a)$. This implies that where $k = m!$ we have $g^k(a) = g^{2k}(a)$ for all $a \in A$. Thus the equation $g^k = g^{2k}$ holds for all $g \in A^A$.

Now let $x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{n-1} \in A$ and put

$$g(x) = f(x_0, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_{n-1})$$

for all x. By an obvious induction, we have

$$g^r(x) = f^r_{(i)}(x_0, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_{n-1})$$

for all r. The assertion of this lemma is now obvious. □

DEFINITION 4.5. A ternary operation $q(x, y, z)$ on a set A is said to be a **Mal'cev operation** if the equations $q(x, x, y) = y = q(y, x, x)$ are valid for all $x, y \in A$. An algebra $\mathbf{A}$ is called **Mal'cev** iff $\mathbf{A}$ has a Mal'cev term operation; i.e., there exists a Mal'cev operation $q \in \mathrm{Clo}_3\mathbf{A}$. An algebra $\langle A, f\rangle$ with one binary operation is called a **quasigroup** iff every equation $f(x, c) = a$ with $a, c \in A$ has one and only one solution x in A, and likewise every equation $f(c, x) = a$ has a unique solution.

LEMMA 4.6. *Every finite quasigroup is Mal'cev.*

PROOF. Let $\langle A, f\rangle$ be a finite quasigroup. Choose, by 4.4, a $k > 0$ such that $f^k_{(0)}(x, y) = f^k_{(0)}(f^k_{(0)}(x, y), y)$. Regarded as functions of x, with y held fixed, $f(x, y)$ and its iterate $f^k_{(0)}(x, y) = f(\cdots f(f(x, y), y), \ldots, y)$ are both permutations of A. Thus $f^k_{(0)} = f^{2k}_{(0)}$ implies that $f^k_{(0)}(x, y) = x$. We can obviously suppose that $k > 1$. Define $d_0(x, y) = f^{k-1}_{(0)}(x, y)$. Then $f(d_0(x, y), y) = f^k_{(0)}(x, y) = x$ for all x, y.

Repeating this argument with the focus on the second variable, we obtain a term operation $d_1(x, y)$ which satisfies $f(x, d_1(x, y)) = y$. We now define

$$q(x, y, z) = f(d_0(x, d_1(y, y)), d_1(y, z)).$$

Since $f(y, d_1(y, y)) = y$ and $f(d_0(y, d_1(y, y)), d_1(y, y)) = y$, it follows that $y = d_0(y, d_1(y, y))$. Thus $q(y, y, z) = f(y, d_1(y, z)) = z$. It is also easy to show that $q(y, z, z) = y$. Thus the operation $q(x, y, z)$ is Mal'cev □

Minimal (or permutational) algebras were defined in Definition 2.14. Here is the theorem of Pálfy which serves to characterize them. Recall that two algebras are called **polynomially equivalent** iff they have the same set of elements and precisely the same clone of polynomial operations.

THEOREM 4.7. *(P.P. Pálfy [26]) Every minimal algebra of at least three elements, that has a polynomial operation which depends on more than one variable, is polynomially equivalent with a vector space over a finite field.*

PROOF. Let $\mathbf{M}$ be minimal, $|M| \geq 3$, and assume that $\mathbf{M}$ does have a polynomial operation depending on more than one variable. By Corollary 4.2, $\mathbf{M}$ has a binary polynomial operation that depends on both its variables. We denote the group of all permutations of the set M by $\mathrm{Sym}\, M$, and remark that every non-constant unary polynomial of $\mathbf{M}$ belongs to $\mathrm{Sym}\, M$. The proof proceeds through a series of assertions.

Claim 1. If $f \in \mathrm{Pol}_2\mathbf{M}$ and $a, b, c, d \in M$ and $f(a, c) = f(a, d)$, then $f(b, c) = f(b, d)$.

To prove the claim we suppose otherwise, that $f(a, c) = f(a, d)$ and $f(b, c) \neq f(b, d)$. We iterate f in the second variable. By Lemma 4.4, choose $k > 0$ so that

$g(x,y) = f^k_{(1)}(x,y)$ satisfies $g(x,g(x,y)) = g(x,y)$. Since $f(b,c) \neq f(b,d)$ and $\mathbf{M}$ is a minimal algebra, the polynomial $h(x) = f(b,x)$ is a permutation of M. We have $g(b,y) = h^k(y)$, and so $h^k(y) = h^{2k}(y)$, implying that $y = h^k(y) = g(b,y)$. This holds for all elements y in M. By the same token, $g(a,c) = g(a,d) = g(a,y)$ for all elements $y \in M$. (The unary function $g(a,y)$ is not a permutation, so it must be constant.) We denote $g(a,c)$ by e.

Each column of the multiplication table of g has either just one element appearing, or has different elements appearing on every two different places. (Each column describes a unary polynomial of $\mathbf{M}$.) Each row of the table either has only one element appearing, or describes the identity function on M. (We proved this above for the "a" and "b" rows, and it's true in general, since $g(x,y) = g(x,g(x,y))$.) Choosing elements w, u of M such that $w \neq e$ and $u \notin \{a,b\}$ (which we can do because $|M| \geq 3$), we see that the table of g contains the fragment below.

	e	w	y
a	e	e	e
b	e	w	y
u	e	?	
x	e		$g(x,y)$

Figure 5

Since $g(a,e) = e = g(b,e)$ it follows that only e's appear in the "e" column. Now the "u" row is constant or identical with the "b" row. Therefore the unfilled box in the table contains either w or e. Either way, the "w" column cannot be constant and cannot be a permutation. This amounts to a contradiction, and Claim 1 is now proved.

Claim 2. If f belongs to $\mathrm{Pol}_2\mathbf{M}$ and depends on both variables, then $\langle M, f\rangle$ is a quasigroup.

This claim follows immediately from the previous claim and the fact that $\mathbf{M}$ is minimal. (Note that if $f(a,c) \neq f(b,c)$, then by applying Claim 1 to f' where $f'(x,y) = f(y,x)$, we get that $f(a,d) \neq f(b,d)$ holds for all d, and then $f(x,d)$ as a function of x must be a permutation, for each d.)

Since $\mathbf{M}$ does have a binary polynomial which depends on both variables, it follows by Claim 2 and Lemma 4.6 that we can choose a Mal'cev operation δ in $\mathrm{Pol}_3\mathbf{M}$. $\delta(x,y,z)$ will turn out to be the same as $x - y + z$ in the vector space we are going to construct. From Claim 1 we also deduce the next claim.

Claim 3. If $f \in \mathrm{Pol}_{n+1}M$ and $\bar{a}, \bar{b} \in M^n$ while $c,\ d \in M$, then $f(\bar{a},c) = f(\bar{a},d)$ implies $f(\bar{b},c) = f(\bar{b},d)$.

This follows by applying Claim 1 in an obvious fashion to n binary polynomials derived from f. Thus we obtain, from the assumption

$$f(a_0, \ldots, a_{n-1}, c) = f(a_0, \ldots, a_{n-1}, d),$$

that

$$f(a_0, \ldots, a_{n-2}, b_{n-1}, c) = f(a_0, \ldots, a_{n-2}, b_{n-1}, d),$$

and we can next replace a_{n-2} by b_{n-2} and so on, up the line. Notice that the property asserted in this claim is not the same as the "Abelian" property of an algebra defined in Chapter 3. "Abelian" is in general a stronger property. (But since our algebra is, in fact, a vector space, it will turn out to be Abelian.)

We now choose one element of M, call it 0, and define for $x, y \in M$:

$$x + y = \delta(x, 0, y), \quad -x = \delta(0, x, 0)$$

where δ is our Mal'cev operation.

Claim 4. $\langle M, +, -, 0\rangle$ is an Abelian group.

To prove it, we define three auxiliary operations.

$$\delta_1(x, y, z, u) = \delta(\delta(x, 0, u), 0, \delta(y, u, z))$$
$$\delta_2(x, u) = \delta(x, u, \delta(u, x, 0))$$
$$\delta_3(x, y, u) = \delta(u, 0, \delta(x, u, y)).$$

We notice that $\delta_1(0, b, 0, b) = \delta_1(0, b, 0, 0)$ and then by Claim 3, $(a + b) + c = \delta_1(a, b, c, b) = \delta_1(a, b, c, 0) = a + (b + c)$. Similarly, $\delta_2(0, a) = \delta_2(0, 0)$, implying $a + (-a) = \delta_2(a, 0) = \delta_2(a, a) = 0$. And again, $\delta_3(0, 0, b) = b + (-b) = 0$ and $\delta_3(0, 0, 0) = 0$, implying $b + a = \delta_3(a, b, b) = \delta_3(a, b, 0) = a + b$. We have established the associative and commutative laws for $+$ and that $-b$ is an inverse element for b. It is obvious that $b + 0 = b$. Thus Claim 4 is established.

Claim 5. If $f \in \mathrm{Pol}_n\mathbf{M}$ and $x_0, \ldots, x_{n-1}$ belong to M, then

$$f(x_0, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} f_i(x_i) - (n-1) \cdot f(0, \ldots, 0)$$

where $f_i(x_i) = f(0, \ldots, 0, x_i, 0, \ldots, 0)$ (x_i occuring in the expected place).

This claim is obvious for $n = 1$. And if $n = 2$, it follows from the true equation $f(0, y) - f(0, y) = f(0, 0) - f(0, 0)$ by applying Claim 3 to the operation $g(x, y, z) = f(x, z) - f(y, z)$. The claim can now be proved for all $n > 2$ by induction. (Assume that it holds for all $n < k$, let $f \in \mathrm{Pol}_k\mathbf{M}$, and consider one of the $k-1$-ary operations

that one obtains by holding the first variable fixed in f. The induction assumption gives

$$f(x, x_1, \ldots, x_{k-1}) = \\ f(x, x_1, 0, \ldots, 0) + \cdots + f(x, 0, \ldots, 0, x_{k-1}) - (k-2)f(x, 0, \ldots, 0) .$$

The desired conclusion will then follow by re-writing each of $f(x, x_1, 0, \ldots, 0), \ldots,$ $f(x, 0, \ldots, 0, x_{k-1})$, using the binary case of the claim, which we proved already.)

To uncover the field over which $\mathbf{M}$ is a vector space, define F to be the set of all $\alpha \in \mathrm{Pol}_1\mathbf{M}$ such that $\alpha(0) = 0$. For each $\alpha \in F$, we see immediately that α is an endomorphism of the group $\langle M, + \rangle$, by applying Claim 5 to the operation $f(x, y) = \alpha(x + y)$. This gives

$$\alpha(x + y) = \alpha(x + 0) + \alpha(0 + y) - \alpha(0 + 0),$$

or $\alpha(x + y) = \alpha(x) + \alpha(y)$.

Since F is closed under composition, $\circ$, and pointwise addition, $+$, it is a subring of the ring of all endomorphisms of $\langle M, + \rangle$. Since $\mathbf{M}$ is minimal, if $\alpha \in F$ and α is not identically zero, then $\alpha^k = \mathrm{id}$ for some k. Thus $\mathbf{F} = \langle F, +, \circ \rangle$ is a finite division ring, and so a field. By defining $\alpha \cdot x = \alpha(x)$ for $\alpha \in F$, $x \in M$, we clearly have a vector space $\mathbf{V} = \langle M, x + y, -x, \alpha \cdot x (\alpha \in F) \rangle$.

The operations of this vector space belong to Pol $\mathbf{M}$, hence $\mathrm{Pol}\,\mathbf{V} \subseteq \mathrm{Pol}\,\mathbf{M}$. On the other hand, Claim 5 shows that for each $f \in \mathrm{Pol}_n\mathbf{M}$, we have

$$f(x_0, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} \alpha_i \cdot x_i + c$$

where $\alpha_i(x) = f_i(x) - f_i(0)$ (note that $\alpha_i \in F$) and $c = f(0, \ldots, 0)$. We conclude that $\mathrm{Pol}\,\mathbf{M} = \mathrm{Pol}\,\mathbf{V}$; and our proof is now complete. □

The minimal algebras in which each operation depends on at most one variable are easily determined, up to polynomial equivalence. If $\mathbf{M}$ is such an algebra, then $\Pi = \mathrm{Pol}_1\mathbf{M} \cap \mathrm{Sym}\,M$ is a group of permutations on M (a subgroup of $\mathrm{Sym}\,M$); and any n-ary operation, f, on M belongs to Pol $\mathbf{M}$ iff either f is constant or for some $i < n$ and $\alpha \in \Pi$ we have $f(\bar{x}) = \alpha(x_i)$ for all $\bar{x} = (x_0, \ldots, x_{n-1}) \in M^n$. In other words, $\mathbf{M}$ is polynomially equivalent to the algebra $\langle M, \Pi \rangle$.

One of the principal insights of tame congruence theory is that a number of properties of any finite algebra are directly correlated with the "types" of the minimal algebras induced by the prime congruence quotients of the algebra. A minimal algebra of the kind described above, essentially unary, will be said to be of "unary type". A minimal algebra polynomially equivalent to a vector space will be said to have "affine type". The other types of minimal algebras are two-element algebras. We

shall now show that up to polynomial equivalence, precisely seven distinct algebras can be built on the universe $\{0,1\}$. We remark that E.L. Post [29] proved in 1941 that the set of all clones of operations on $\{0,1\}$ is a denumerably infinite set. What we will prove is that there are precisely seven distinct clones on $\{0,1\}$ that contain the constant operations. We can also observe that the situation changes radically when one more element is added to the universe. I. Agoston, J. Demetrovic and L. Hannák prove in [1] that the set of clones on $\{0,1,2\}$ containing the constant operations has cardinality equal to that of the set of real numbers.

A two-element algebra with the largest possible set of polynomial operations is, of course, the Boolean algebra,

$$\mathbf{E}_3 = \langle \{0,1\}, \vee, \wedge, ' \rangle,$$

where we have $x \vee y = \max\{x,y\}$, $x \wedge y = \min\{x,y\}$, and $x' = 1 - x$. Let $x + y$ denote the sum of x and y modulo 2.

LEMMA 4.8. *Every algebra* $\mathbf{M} = \langle \{0,1\}, \dots \rangle$ *is polynomially equivalent to one of the following, no two of which are polynomially equivalent:*

$$\mathbf{E}_0 = \langle \{0,1\} \rangle, \ \mathbf{E}_1 = \langle \{0,1\}, ' \rangle, \ \mathbf{E}_2 = \langle \{0,1\}, + \rangle, \ \mathbf{E}_3 = \langle \{0,1\}, \vee, \wedge, ' \rangle,$$
$$\mathbf{E}_4 = \langle \{0,1\}, \vee, \wedge \rangle, \ \mathbf{E}_5 = \langle \{0,1\}, \vee \rangle, \ \mathbf{E}_6 = \langle \{0,1\}, \wedge \rangle.$$

Remark. The algebras $\mathbf{E}_0, \dots, \mathbf{E}_6$ can be ordered by the inclusion relations among their polynomial clones. The result is the lattice pictured below.

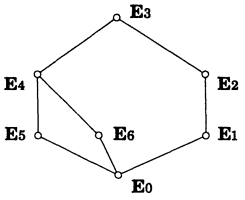


Figure 6

PROOF. If $\mathbf{M}$ is essentially unary, then it is polynomially equivalent to $\mathbf{E}_0$ or $\mathbf{E}_1$ because $\mathrm{Sym}\{0,1\}$ has only two subgroups. We assume that $\mathbf{M}$ is not essentially unary. By Corollary 4.2 it has a binary polynomial operation f that depends on both variables.

Consider first the case where all binary polynomial operations of $\mathbf{M}$ satisfy Claim 1 in the proof of Theorem 4.7. The table of f can then only be one of the following.

	0	1	y
0	0	1	
1	1	0	
x			$x+y$

	0	1
0	1	0
1	0	1

If the second table describes f, then $x' = f(0,x)$ and $x + y = f(x,y)'$. Thus in either case, addition modulo 2 is a polynomial of $\mathbf{M}$. Now the proof of Theorem 4.7 can be followed through to show that $\operatorname{Pol}\mathbf{M} = \operatorname{Pol}\mathbf{E}_2$. (A simpler direct argument may be found.)

Consider now the case contrary to the one just considered. We can assume that the table of f has a constant row and a non-constant row. If f fails to be order preserving, then $'$ is a polynomial of $\mathbf{M}$ (a row or a column of f) and the two rows of the table of f can be switched to get a new polynomial operation $f(x',y)$. The entries in the table can be permuted, resulting in $f(x,y)'$. Through a series of such changes, one can produce both $\vee$ and $\wedge$. Thus $\operatorname{Pol}\mathbf{M} \supseteq \operatorname{Pol}\mathbf{E}_3$; and we must have equality of polynomial sets, since every operation on $\{0,1\}$ is a polynomial of $\mathbf{E}_3$ (see Exercise 4.9 (2)).

If $\operatorname{Pol}\mathbf{M}$ contains some operation that is not order preserving, then it contains $'$ (see Exercise 4.9 (1)), and we can complete the proof just as above. Therefore we now assume that all operations of M are order preserving. There are just two order preserving binary operations on $\{0,1\}$ that depend on both variables, namely $\vee$ and $\wedge$. Therefore, one or the other, let us say $\wedge$, is in $\operatorname{Pol}_2\mathbf{M}$.

Assume that $\operatorname{Pol}\mathbf{M} > \operatorname{Pol}\mathbf{E}_6$ (proper inclusion). Let h be an n-ary polynomial of $\mathbf{M}$ which is not a polynomial of $\mathbf{E}_6$. Then $\{0,1\} \subseteq \text{range } h$. For any subset I of $\{0,1,\ldots,n-1\}$, let $x_I \in 2^n$ be its characteristic function; $x_I = \langle x_0,\ldots,x_{n-1}\rangle$ with $x_i = 1$ iff $i \in I$, and $x_i = 0$ otherwise. Since we are now assuming that all polynomials of $\mathbf{M}$ are order-preserving, $I \subseteq J \subseteq \{0,\ldots,n-1\}$ implies $h(x_I) \leq h(x_J)$. Since $1 \in \text{range } h$, there is at least one minimal member of $\{I : h(x_I) = 1\}$. If there is only one such minimal set I_0, then clearly $h(x_I) = 1$ iff $I \supseteq I_0$. In this case,

$$h(x_0,\ldots,x_{n-1}) = \bigwedge_{i\in I_0} x_i,$$

which contradicts our assumption that $h \notin \operatorname{Pol}\mathbf{E}_6$. Thus there exist two distinct sets $I_0, I_1 \subseteq \{0,\ldots,n-1\}$ such that $h(x_{I_0}) = h(x_{I_1}) = 1$ and $h(x_J) = 0$ whenever J is a proper subset of I_0 or of I_1. We can derive a binary operation $b(x,y)$ from $h(x_0,\ldots,x_{n-1})$ by substituting x for x_i whenever $i \in I_0 - I_1$, y for x_i when $i \in I_1 - I_0$, 0 for x_i when $i \notin I_0 \cup I_1$, and 1 for x_i when $i \in I_0 \cap I_1$. Now $b(1,0) = h(x_{I_0}) = 1$ and $b(0,1) = h(x_{I_1}) = 1$ while $b(0,0) = h(x_{I_0\cap I_1}) = 0$. Thus $b(x,y) = x \vee y$; and so $\vee$ and $\wedge$ are in $\operatorname{Pol}\mathbf{M}$. We now have that $\operatorname{Pol}\mathbf{E}_4 \subseteq \operatorname{Pol}\mathbf{M}$. We ask the reader to complete the proof of this lemma by showing that $\operatorname{Pol}\mathbf{E}_4$ is identical with the

set of all order preserving operations on $\{0,1\}$, and that $\mathbf{E}_0, \dots, \mathbf{E}_6$ are polynomially inequivalent. □

Exercises 4.9

(1) Show that if $\mathbf{A} = \langle A, \dots \rangle$ is an algebra and $\leq$ a partial order on A and $\operatorname{Pol}\mathbf{A}$ is not contained in the set of operations on A that preserve $\leq$ (equivalently, $\leq$ is not a subalgebra of $\mathbf{A}^2$), then there exists $f \in \operatorname{Pol}_1\mathbf{A}$ which does not preserve $\leq$.

(2) Show that every operation on $\{0,1\}$ is a polynomial of the Boolean algebra $\mathbf{E}_3$.

(3) Show that $\operatorname{Pol}\mathbf{E}_4$ is the set of all order preserving operations on $\{0,1\}$.

(4) Show that $\operatorname{Pol}\mathbf{E}_2$ is the set of all operations f on $\{0,1\}$ such that f and all its variants obtained by permuting variables satisfy the formula (3.1.1).

The algebras $\mathbf{E}_5$ and $\mathbf{E}_6$ are isomorphic, and any algebra isomorphic to one of them is called a *two-element semilattice.* An algebra is a *two-element lattice* (or *Boolean algebra*) iff it is isomorphic to $\mathbf{E}_4$ (or to $\mathbf{E}_3$, respectively).

DEFINITION 4.10. Let $\mathbf{M}$ be a minimal algebra.

(1) $\mathbf{M}$ is of type **1**, or **unary type**, iff $\operatorname{Pol}\mathbf{M} = \operatorname{Pol}\langle M, \Pi\rangle$ for a subgroup $\Pi \subseteq \operatorname{Sym} M$.

(2) $\mathbf{M}$ is of type **2**, or **affine type**, iff $\mathbf{M}$ is polynomially equivalent to a vector space.

(3) $\mathbf{M}$ is of type **3**, or **Boolean type**, iff $\mathbf{M}$ is polynomially equivalent to a two-element Boolean algebra.

(4) $\mathbf{M}$ is of type **4**, or **lattice type**, iff $\mathbf{M}$ is polynomially equivalent to a two-element lattice.

(5) $\mathbf{M}$ is of type **5**, or **semilattice type**, iff $\mathbf{M}$ is polynomially equivalent to a two-element semilattice.

COROLLARY 4.11. *A finite algebra is minimal iff it is of one of the types* **1–5**.

PROOF. This is an immediately corollary of Theorem 4.7 and Lemma 4.8. □

The minimal algebras were easy to classify, given Pálfy's theorem. The algebras minimal relative to a congruence quotient also divide naturally into five types. To see this, a somewhat more elaborate argument seems necessary. It is contained in the next six lemmas.

Suppose that $\mathbf{C}$ is minimal relative to $\langle \delta, \theta \rangle$. By 2.12–2.13, this means that δ and θ are congruences of $\mathbf{C}$, that $\delta < \theta$, and that every $f \in \mathrm{Pol}_1\mathbf{C} - \mathrm{Sym}\,\mathbf{C}$ satisfies $f(\theta) \subseteq \delta$; i.e., $\langle f(x), f(y) \rangle \in \delta$ whenever $\langle x, y \rangle \in \theta$. The traces, body, and tail of $\mathbf{C}$ (with respect to $\langle \delta, \theta \rangle$) were defined in Definition 2.15. (See Figure 3.) By a trace (i.e., a $\langle \delta, \theta \rangle$-trace) is meant any θ-equivalence class which contains at least two δ-equivalence classes. For each trace N, $(\mathbf{C}|_N)/(\delta|_N)$ is a minimal algebra. By the *type* of N (with respect to $\langle \delta, \theta \rangle$) we shall mean, of course, the type of this minimal algebra, which, according to our definition, is an integer between one and five.

Let us examine for a moment what it means for N to be of type **3**, **4** or **5**. Notice that the polynomial operations of $\mathbf{C}|_N$ are the same as its basic operations, and this must remain true of $(\mathbf{C}|_N)/(\delta|_N)$. [We defined $\mathbf{C}|_N$ to be $\langle N, (\mathrm{Pol}\,\mathbf{C})|_N \rangle$, and the set $(\mathrm{Pol}\,\mathbf{C})|_N$, which consists of all $g|_N$ such that g is an n-ary polynomial of $\mathbf{C}$ for some n and $g(N^n) \subseteq N$, is obviously closed under composition and contains the constant operations.] Now a minimal algebra has its type among **3**, **4**, **5** (see Definition 4.10) iff it is a two-element algebra and has a semilattice operation among its polynomials. [Incidentally, it follows easily from Lemma 4.8 that an algebra $\mathbf{M}$ is a minimal algebra of type **3**, **4** or **5** if and only if $\mathbf{M}$ is a two-element non-Abelian algebra.] Thus the trace N has type **3**, **4** or **5** iff N is the union of two disjoint δ-equivalence classes, O and I, such that for some $g \in \mathrm{Pol}_2\mathbf{C}$, we have $g(O \times O) \subseteq O, g(O \times I) \subseteq O$, $g(I \times O) \subseteq O$, and $g(I \times I) \subseteq I$.

LEMMA 4.12. *Let* $\mathbf{C}$ *be* $\langle \delta, \theta \rangle$*-minimal. If* $\mathbf{C}$ *contains two distinct* $\langle \delta, \theta \rangle$*-traces, then all of its* $\langle \delta, \theta \rangle$*-traces are of type* **1** *or* **2.**

PROOF. We assume that $\mathbf{C}$ has a trace N of type either **3**, **4** or **5**. By 2.16 (2), $\mathbf{C}/\delta$ is $\langle 0, \theta/\delta \rangle$-minimal, and its $\langle 0, \theta/\delta \rangle$-traces are obviously just the sets K/δ where K is a $\langle \delta, \theta \rangle$-trace. Moreover, K and K/δ have the same type, namely that of the minimal algebra $(\mathbf{C}|_K)/(\delta|_K)$. Thus it suffices to prove the lemma for $\mathbf{C}/\delta$ in place of $\mathbf{C}$. Simpler, we change notation and assume that $\delta = 0_C$.

Now N is a two-element set, and we denote its elements by 0 and 1, with the notation chosen so that $\mathbf{C}$ has a binary polynomial $g(x, y)$ such that $g(x, y) = x \wedge y$ for $x, y \in N = \{0, 1\}$. Letting $d(x) = g(x, x)$, we have that $d \in \mathrm{Sym}\,C$ since $d(0) \neq d(1)$ and $\langle 0, 1 \rangle \in \theta$. ($\mathbf{C}$ is $\langle 0_C, \theta \rangle$-minimal.) Choose a $k > 1$ such that $d^k(x) = x$ for all $x \in C$, and define $h(x, y) = d^{k-1}g(x, y)$. Now $h(x, x) = x$ for all $x \in C$, and $h|_{\{0,1\}} = g|_{\{0,1\}} = \wedge$. We iterate h in its first variable, and choose an $l > 0$ such that $h^l_{(0)}(h^l_{(0)}(x, y), y) = h^l_{(0)}(x, y)$ for all $x, y \in C$ (by Lemma 4.4). Writing $f(x, y) = h^l_{(0)}(x, y)$, we have

$$f(x, x) = x, \quad f(f(x, y), y) = f(x, y)$$
$$\text{for all} \quad x, y \in C; \quad \text{and}$$
$$f(x, y) = x \wedge y \quad \text{for} \quad x, y \in \{0, 1\}.$$

Now suppose, to obtain a contradiction, that $\mathbf{C}$ has a $\langle 0_C, \theta\rangle$-trace K distinct from N. Since $f(0,1) = 0$ and $f(1,1) = 1$, it follows that $f(x,1)$ is a permutation of C. Thus $f(x,1) = x$ for all x, since $f(f(x,1),1) = f(x,1)$. Similarly, since $f(0,0) = f(1,0)$, we must have $f(x,0) = f(y,0)$ whenever $\langle x,y\rangle \in \theta$.

Since K and N are equivalence classes of θ and $f(x,x) = x = f(x,1)$ and $1 \in N$, it follows that $f(K\times K)\cup f(K\times N) = K$. Since $f(x,0) = f(y,0)$ whenever $x,y \in K$, we can choose an element $u \in K$ with $u \neq f(u,0)$. Thus $f(u,0) \neq f(u,1)$ and from this it follows that $\alpha(x) = f(u,x)$ defines a permutation of C. We have $\alpha(K \cup N) \subseteq K$ since $u \in K$. This is absurd, because $|K \cup N| = |K| + 2$. □

The preceding lemma is part of our proof (which will be completed with Lemma 4.20) that all traces of any $\langle \delta, \theta\rangle$-minimal algebra possess the same type. The next two lemmas deal with the situations in which the traces are of types **1** or **2**. Recall the definitions of Abelian algebra, Abelian congruence, and Abelian congruence quotient, in Definitions 3.1, 3.3, and 3.6.

LEMMA 4.13. *Let* $\mathbf{C}$ *be* $\langle 0,\theta\rangle$*-minimal. Then* θ *is an Abelian congruence iff for every* $\langle 0,\theta\rangle$*-trace* N, $\mathbf{C}|_N$ *is an Abelian algebra, i.e.,* N *has type* **1** *or* **2**.

PROOF. The congruence θ is, by definition, Abelian iff formula (3.1.1) holds for every $f \in \mathrm{Pol}_n\mathbf{C}$ (and for all n) whenever $u \equiv v, x_1 \equiv y_1, \ldots, x_{n-1} \equiv y_{n-1} \pmod\theta$. If θ is Abelian, N is a trace, and $f(N^n) \subseteq N$ where $f \in \mathrm{Pol}_n\mathbf{C}$, then (3.1.1) holds for this f and for all $u, v, x_1, \ldots, y_{n-1}$ in N. Thus if θ is Abelian, then the induced algebras $\mathbf{C}|_N$, for N a trace, are Abelian. It is easy to check that minimal algebras of type **1** and of type **2** are Abelian, and those of other types are not.

Conversely, let us suppose that θ fails to be Abelian. Thus we have $f \in \mathrm{Pol}_n\mathbf{C}$, and elements $u \equiv v, x_1 \equiv y_1, \ldots, x_{n-1} \equiv y_{n-1} \pmod\theta$, such that $f(u,\bar{x}) = f(u,\bar{y})$ and $f(v,\bar{x}) \neq f(v,\bar{y})$. We can assume that n is the least integer for which such a situation exists. Then $n > 1$ and $u \neq v$, $x_i \neq y_i$ for each $i < n$. We put $N_0 = u/\theta, N_1 = x_1/\theta, \ldots, N_{n-1} = x_{n-1}/\theta$, and $K = f(u, x_1, \ldots, x_{n-1})/\theta$. Thus, $N_0, N_1, \ldots, N_{n-1}$, and K are traces, and $f(N_0 \times \cdots \times N_{n-1}) \subseteq K$. Writing $\overline{N}$ for the product set $N_0 \times \cdots \times N_{n-1}$, $f|_{\overline{N}}$ must depend on each of its variables, or else we could replace one of the variables by a constant and contradict the minimality of n. Thus there exists $\bar{c} = \langle c_0, \ldots, c_{n-2}\rangle \in N_0 \times \cdots \times N_{n-2}$ such that $\alpha_{n-1}(x) = f(c_0, \ldots, c_{n-2}, x)$ defines a unary polynomial α_{n-1} which is not constant on N_{n-1}. Since $\mathbf{C}$ is $\langle 0,\theta\rangle$-minimal, $\alpha_{n-1} \in \mathrm{Sym}\, C$. Similarly, there exist $\alpha_i \in \mathrm{Pol}_1\mathbf{C} \cap \mathrm{Sym}\, C$ with $\alpha_i(N_i) \subseteq K$, for $i = 0, \ldots, n-1$. Now $\alpha_i^{-1} \in \mathrm{Pol}_1 C$, and so we have $\alpha_i(N_i) = K$, since α_i must permute the equivalence classes of θ.

Let us define another polynomial operation of $\mathbf{C}$ as follows:

$$g(z_0, \ldots, z_{n-1}) = f(\alpha_0^{-1}(z_0), \ldots, \alpha_{n-1}^{-1}(z_{n-1})) \,.$$

Now $g(K^n) = K$; and where $u' = \alpha_0(u)$, $v' = \alpha_0(v), \ldots, y'_{n-1} = \alpha_{n-1}(y_{n-1})$, we have $u', v', \ldots, y'_{n-1} \in K$ and $g(u', \bar{x}') = g(u', \bar{y}')$ $(= f(u, \bar{x}))$ while $g(v', \bar{x}') \neq g(v', \bar{y}')$. Thus the induced algebra $\mathbf{A}|_K$ is not Abelian, and the type of the trace K cannot be **1** or **2**. □

LEMMA 4.14. *Let* $\mathbf{C}$ *be* $\langle \delta, \theta \rangle$*-minimal. Then* $\langle \delta, \theta \rangle$ *is an Abelian congruence quotient iff for every* $\langle \delta, \theta \rangle$*-trace* N, $(\mathbf{C}|_N)/(\delta|_N)$ *is an Abelian minimal algebra, i.e.,* N *has type* **1** *or* **2**.

PROOF. By Proposition 3.7 (3), $\langle \delta, \theta \rangle$ is Abelian iff θ/δ is an Abelian congruence of $\mathbf{C}/\delta$. By Lemma 2.16 (2), $\mathbf{C}/\delta$ is $\langle 0, \theta/\delta \rangle$-minimal. A subset K of C/δ is a $\langle 0, \theta/\delta \rangle$-trace iff it has the form N/δ for a $\langle \delta, \theta \rangle$-trace N. If N is a $\langle \delta, \theta \rangle$-trace, then the type of N equals the type of the $\langle 0, \theta/\delta \rangle$-trace N/δ, and equals the type of the minimal algebra $(\mathbf{C}|_N)/(\delta|_N)$. Given all this, Lemma 4.14 follows directly from Lemma 4.13. □

Our study of algebras minimal relative to Abelian quotients covers many pages. Before beginning it, we shall deduce some further useful information about the non-Abelian case. In any two-element semilattice $\langle \{a, b\}, f \rangle$ there is an *absorbing element* a, and a *neutral element* b. The correspondence of a with 0, and b with 1, is an isomorphism between $\langle \{a, b\}, f \rangle$ and $\langle \{0, 1\}, \wedge \rangle$. (In the semilattice $\langle \{0, 1\}, \vee \rangle$, 0 is the neutral element, and 1 the absorbing element.) We prefer to think of our semilattices as meet semilattices, and to use the symbols 0 and 1 for the absorbing and neutral elements, respectively. Thus the symbols for the first two natural numbers will do multiple duty, often denoting the two elements constituting the unique trace of a $\langle 0, \theta \rangle$-minimal algebra in which θ is non-Abelian. We shall say that a $\langle \delta, \theta \rangle$-minimal algebra has type **3** (or **4** or **5**, respectively) iff $\langle \delta, \theta \rangle$ is non-Abelian and the unique $\langle \delta, \theta \rangle$-trace has type **3** (or **4** or **5**). (This definition will later be incorporated into the general definition of the type of a $\langle \delta, \theta \rangle$-minimal algebra.)

LEMMA 4.15. *Let* $\mathbf{C}$ *be minimal of type* **5** *relative to* $\langle \delta, \theta \rangle$*. Let* N *be the unique* $\langle \delta, \theta \rangle$*-trace of* $\mathbf{C}$ *(equally, the body of* $\mathbf{C}$*). There is an element* $1 \in N$ *and an operation* $p \in \mathrm{Pol}_2\mathbf{C}$ *satisfying the following:*

(1) $N = I \cup O$ *(disjoint union), where* I *and* O *are* δ*-equivalence classes and* $I = \{1\}$.

(2) N *is closed under* p *and* $\langle N, p \rangle/(\delta|_N)$ *is a semilattice with neutral element* $\{1\}$*, polynomially equivalent to* $(\mathbf{C}|_N)/(\delta|_N)$.

(3) *For all* $x \in C - \{1\}$, $\langle \{x, 1\}, p \rangle$ *is a semilattice with neutral element* 1*; i.e.,* $p(x, 1) = p(1, x) = p(x, x) = x$ *for all* $x \in C$.

(4) *For all* $x \in C$ *such that* $x \neq 1$ *and for all* $u \in O$, $p(x, u) \overset{\delta}{\equiv} p(u, x) \overset{\delta}{\equiv} x$.

(5) *For all* $x, y \in C$, $p(x, p(x, y)) = p(x, y)$.

Remark. Here is a picture of the situation. T denotes the tail ($= C - N$), and the δ-classes are represented as boxes. Where $\beta = \theta/\delta$, $\mathbf{C}/\delta$ is a typical $\langle 0, \beta \rangle$-minimal algebra of type **5**. The β-classes in $\mathbf{C}/\delta$ are again represented as boxes.

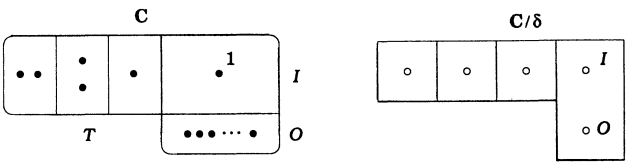


Figure 7

PROOF. We repeat part of the proof of Lemma 4.12. There is an operation $g \in \mathrm{Pol}_2\mathbf{C}$ such that $g(N^2) \subseteq N$ and $\langle N, g|_N \rangle/\delta$ is a two-element semilattice. Let O and I be the two δ-classes contained in N, with I the neutral element of the semilattice. Thus

$$g(I \times I) \subseteq I\ ,\ \ g(I \times O) \cup g(O \times I) \cup g(O \times O) \subseteq O\ .$$

Letting $d(x) = g(x, x)$, we have that $d \in \mathrm{Sym}\, C$. The operation $h(x, y) = d^{-1}(g(x, y))$ belongs to $\mathrm{Pol}_2\mathbf{C}$, $h(x, x) = x$ for all x, and h has the same properties as g regarding I and O. Letting $l > 0$ be such that the operation $f(x, y) = h^l_{(0)}(x, y)$ satisfies $f(f(x, y), y) = f(x, y)$, we have that $f(x, x) = x$ for all x and f behaves with respect to O and I just in the same way as g and h. For $z \in I, u \in O$, we have $\langle f(z, z), f(u, z) \rangle \notin \delta$, and so the function $\alpha(x) = f(x, z)$ must be a permutation of C. Then $\alpha^2 = \alpha$ implies $\alpha = \mathrm{id}$. Thus $f(x, z) = x$ for all $x \in C, z \in I$. Now we choose an $m > 0$ such that the operation $p(x, y) = f^m_{(1)}(x, y)$ satisfies $p(x, p(x, y)) = p(x, y)$. It is easy to check that $p(x, z) = p(x, x) = x$ for $x \in C$, $z \in I$ using that $f(x, z) = x = f(x, x)$. And just as above, we can prove that $p(z, x) = x$ also (for $x \in C$, $z \in I$). Now if $z_1, z_2 \in I$, then $z_2 = p(z_1, z_2) = z_1$. Thus I has just a single element, which we denote by 1.

The truth of the statements (1), (3), (5) now falls out of the construction of p. Statement (2) is true, because $\langle N, p \rangle/(\delta|_N)$ is a semilattice, and $\langle N,\ (\mathrm{Pol}\,\mathbf{C})|_N \rangle/(\delta|_N)$ is a two-element semilattice with its full clone of polynomials, and a two-element semilattice has only one polynomial operation under which it is a semilattice.

To prove (4), let $x \in C - I$, $u \in O$. If $x \in O$ then $p(x, u)$, $p(u, x) \in O$ (a δ-class) and there is nothing to prove. If $x \notin N$ then $p(x, u) \equiv p(x, 1) \pmod{\theta}$ and $p(x, 1) = x$. The sets x/θ and x/δ are equal in this case, else x/θ would be a trace distinct from N. Thus $p(x, u) \equiv x \pmod{\delta}$. and similarly, $p(u, x) \equiv x \pmod{\delta}$. This ends the proof. □

DEFINITION 4.16. Any polynomial operation, p, in an algebra $\mathbf{C}$ minimal of type **5** relative to a quotient $\langle \delta, \theta \rangle$, which satisfies 4.15 (2–5), will be called a **pseudo-meet operation of C (with respect to $\langle \delta, \theta \rangle$)**.

LEMMA 4.17. *Let $\mathbf{C}$ be minimal of type* **3** *or* **4** *relative to $\langle \delta, \theta \rangle$. Let N be the unique trace of $\mathbf{C}$ (with respect to $\langle \delta, \theta \rangle$). There exist operations $p, q \in \mathrm{Pol}_2\mathbf{C}$ satisfying the following*

(1) *$N = \{0, 1\}$ for two elements 0 and 1 that are δ-inequivalent.*

(2) *N is closed under p and q and $\langle N, q|_N, p|_N \rangle$ is a two-element lattice.*

(3) *For all $x \in C$, $p(x, 1) = p(1, x) = p(x, x) = x = q(x, x) = q(x, 0) = q(0, x)$.*

(4) *For all $x \in C - N$, $p(x, 0) \equiv p(0, x) \equiv x \equiv q(x, 1) \equiv q(1, x)$ (mod δ).*

(5) *For all $x, y \in C$, $p(x, p(x, y)) = p(x, y)$ and $q(x, q(x, y)) = q(x, y)$.*

Remark. Here is a picture of a $\langle \delta, \theta \rangle$-minimal algebra of type **3** or **4**. The trace is the set $\{0, 1\}$ and T denotes the tail.

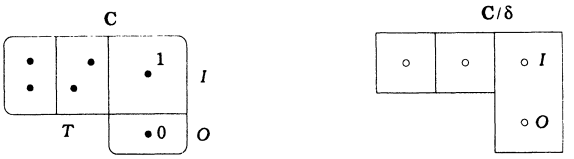


Figure 8

PROOF. The proof is the same as for Lemma 4.15. There are polynomials g_1 and g_2 of C under which $N/\delta = \{O, I\}$ is a two-element lattice. The argument for Lemma 4.15 can be applied to each of g_1 and g_2, producing p and q. Now O is forced to be a one-element set, as well as I, for the same reason as before. □

DEFINITION 4.18. Let p and q be polynomial operations of a $\langle \delta, \theta \rangle$-minimal algebra $\mathbf{C}$ of type **3** or **4**, which satisfy 4.17 (2–5). Then p and q will respectively be called **pseudo-meet** and **pseudo-join operations of C (with respect to $\langle \delta, \theta \rangle$)**.

The preceding pictures of $\langle \delta, \theta \rangle$-minimal algebras of the non-Abelian types **3**, **4** and **5** will be quite useful when we consider the $\langle \alpha, \beta \rangle$-minimal sets U for a prime quotient $\langle \alpha, \beta \rangle$ in a finite algebra $\mathbf{A}$. The quotient $\langle \alpha, \beta \rangle$ will be of type **3** (the Boolean type) iff an $\langle \alpha, \beta \rangle$-minimal set U has a single trace $N = \{0, 1\}$ and the $\langle \alpha|_U, \beta|_U \rangle$-minimal algebra $\mathbf{A}|_U$ has not only pseudo-meet and pseudo-join operations with respect to $\langle \alpha|_U, \beta|_U \rangle$, but has also a unary polynomial f satisfying $f(0) = 1$ and $f(1) = 0$.

Exercises 4.19

(1) Let C be a finite set and $N_1, \ldots, N_k$ be pairwise disjoint subsets of C, each possessing at least two elements. Let Π be a group of permutations of C such that whenever $\alpha \in \Pi$ and $1 \leq i \leq k$, there exists j, $1 \leq j \leq k$, with $\alpha(N_i) = N_j$. Show that the algebra $\mathbf{C} = \langle C, \Pi \rangle$ has a congruence θ such that $\mathbf{C}$ is $\langle 0, \theta \rangle$-minimal and $N_1, \ldots, N_k$ are precisely the $\langle 0, \theta \rangle$-traces in $\mathbf{C}$. The traces are all of type **1**.

(2) Let $\mathbf{C}$ be a finite vector space. Show that $\mathbf{C}$ is minimal, and consequently is $\langle \delta, \theta \rangle$-minimal for each pair of its congruences $\delta < \theta$. Show that the $\langle \delta, \theta \rangle$-traces are of type **2**.

(3) Suppose that $\mathbf{C}$ is $\langle \delta, \theta \rangle$-minimal. Prove that θ is strongly Abelian over δ iff all $\langle \delta, \theta \rangle$-traces have type **1**. (See Definition 3.9 and copy the proof of Lemma 4.14.)

(4) Show that if $\mathbf{C}$ is $\langle \delta, \theta \rangle$-minimal of type **3**, **4** or **5**, then $\delta \prec \theta$ (i.e., θ covers δ in the lattice **Con** $\mathbf{C}$).

(5) Construct three-element $\langle \delta, \theta \rangle$-minimal algebras $\mathbf{C}_3, \mathbf{C}_4, \mathbf{C}_5$ of types **3**, **4**, **5** respectively, such that $\mathbf{C}_5$ is equal to its trace.

The most interesting case of an algebra minimal relative to a quotient is the one dealt with in the next lemma.

LEMMA 4.20. *Let* $\mathbf{C}$ *be an algebra minimal relative to a quotient* $\langle \delta, \theta \rangle$ *and having at least one* $\langle \delta, \theta \rangle$*-trace of type* **2**, *and let* B *be the body of* $\mathbf{C}$ *(i.e., the union of the* $\langle \delta, \theta \rangle$*-traces). Then all of the* $\langle \delta, \theta \rangle$ *traces are of type* **2**, *and* $\mathbf{C}$ *has a 3-ary polynomial* d *satisfying:*

(1) $d(x, x, x) = x$, *for all* $x \in C$.

(2) $d(x, x, y) = y = d(y, x, x)$, *for all* $x \in B$ *and* $y \in C$.

(3) *for every* $a, b \in B$, *the unary polynomials* $d(x, a, b)$, $d(a, x, b)$, $d(a, b, x)$ *are permutations of* C.

(4) B *is closed under* d.

(5) *any two* $\langle \delta, \theta \rangle$*-traces* N *and* N' *are isomorphic in* $\mathbf{C}$, *i.e.,* $N \simeq N'$.

Every 3-ary polynomial of $\mathbf{C}$ *satisfying (1) and (2) also satisfies (3) and (4).*

Remark: Here is a picture of the situation. As usual, T denotes the tail, and the δ-equivalence classes are represented by boxes. The traces in $\mathbf{C}/\delta$ are represented as tall boxes.

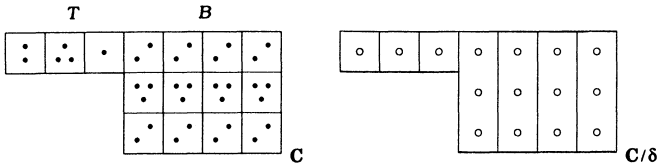


Figure 9

PROOF. Let N be a trace of type **2**, so that $(\mathbf{C}|_N)/(\delta|_N)$ is a vector space. There exists a 3-ary polynomial f of $\mathbf{C}$ such that N is closed under f and $f_\delta(x/\delta, y/\delta, z/\delta) = x/\delta - y/\delta + z/\delta$ (for $x,\ y,\ z \in N$) in this vector space. We denote by Φ the set of all $f \in \mathrm{Pol}_3\mathbf{C}$ which possess this property.

Claim 1. If $f \in \Phi$ then for all $a, b \in N$ the functions $f(x,a,b)$, $f(a,x,b)$ and $f(a,b,x)$ are permutations of C.

This follows immediately from the $\langle\delta,\theta\rangle$-minimality of $\mathbf{C}$, since these functions, restricted to N, become permutations of the vector space when δ is factored out.

We define

$$\Phi_1 = \{f \in \Phi \ : f(x,x,x) = x \text{ for all } x\}$$
$$\Phi_2 = \{f \in \Phi_1 : f(x,x,y) = y \text{ for all } x \in B\ ,\ y \in C\}$$
$$\Phi_3 = \{f \in \Phi_2 : f(y,x,x) = y \text{ for all } x \in B\ ,\ y \in C\}.$$

Our immediate concern is to prove that Φ_3 is non-empty. It is easy to see that Φ_1 is non-empty. For if $f \in \Phi$, the function $d(x) = f(x,x,x)$ must be a permutation of C (since $d(N)$ is not included in a δ-class). Thus $d^{-1}(x) = d^n(x)$ for some $n > 0$; and $f'(x,y,z) = d^{-1}f(x,y,z)$ defines an operation $f' \in \Phi_1$.

Claim 2. If $f \in \Phi_1$ and $a \in B$ (the body) then the functions $f(x,a,a)$ and $f(a,a,x)$ are permutations of C.

To prove it, let $f \in \Phi_1$ and $a \in B$. We shall only prove that $f(x,a,a)$ is one-to-one, the other claim being symmetric to this. The assertion falls under Claim 1 if $a \in N$; so assume that $a \in N'$ where N' is a trace different (and therefore disjoint) from N. Choose $n \geq 1$ so that $g(x,y,z) = f^n_{(0)}(x,y,z)$ satisfies $g(g(x,y,z),y,z) = g(x,y,z)$ for all x,y,z. (See Lemma 4.4.) Then for $b,c \in N$ we have that $g(x,b,c)$ is a one-to-one function of x, since $f(x,b,c)$ is; and this implies that $g(x,b,c) = x$ (for $b,c \in N$ and $x \in C$). We also have $g(x,x,x) = x$, obviously. Thus $g(N'\times N\times N)\cup g(N'\times N'\times N') \subseteq N'$, since N and N' are congruence classes of θ. Therefore, for any $a' \in N'$, the function $G(x) = g(a',x,x)$ satisfies $G(N \cup N') \subseteq N'$. This function cannot be a permutation; hence $G(\theta) \subseteq \delta$; consequently $g(a',v,v) \overset{\delta}{\equiv} g(a',a',a') = a'$ for all $v \in N'$ (and for all $a' \in N'$). Choosing $a' \in N'$ with $\langle a',a\rangle \notin \delta$, we now have that

$g(a', a, a) \overset{\delta}{\equiv} a' \overset{\delta}{\not\equiv} a = g(a, a, a)$. Therefore $g(x, a, a)$ must be a permutation of C, and this implies that $f(x, a, a)$ is also a permutation.

Claim 3. Φ_2 is non-empty.

To prove it, choose any $f \in \Phi_1$. Define $u(x, y) = f(x, x, y)$ and choose $n > 1$ so that $u'(x, y) = u^n_{(1)}(x, y)$ satisfies $u'(x, u'(x, y)) = u'(x, y)$. Define $f'(x, y, z) = u^{n-1}_{(1)}(x, f(x, y, z))$. By working in the vector space $(\mathbf{C}|_N)/(\delta|_N)$, it is easy to see that for $x, y, z \in N$,

$$y \equiv u(x, y) \equiv u^2_{(1)}(x, y) \equiv \cdots \equiv u^{n-1}_{(1)}(x, y)$$

and $f'(x, y, z) \equiv f(x, y, z) \pmod{\delta}$. Thus $f' \in \Phi$. It is also obvious that $f'(x, x, x) = x$ for all x. Notice that $f'(x, x, y) = u'(x, y)$ for all x and y. Now let $a \in B$. By Claim 2, $u(a, y)$ is a permutation of C, consequently $u'(a, y) = y$ for all y. Thus $f'(a, a, y) = u'(a, y) = y$ for all y. We have proved that $f' \in \Phi_2$.

Claim 4. Φ_3 is non-empty.

To prove it, choose any $f \in \Phi_2$. Define $v(x, y) = f(x, y, y)$, and choose $k > 1$ such that $v'(x, y) = v^k_{(0)}(x, y)$ satisfies $v'(v'(x, y), y) = v'(x, y)$, and define $f'(x, y, z) = v^{k-1}_{(0)}(f(x, y, z), z)$. Arguing as in the proof of Claim 3, we see that $f' \in \Phi_1$ and $f'(y, x, x) = y$ whenever $y \in C, x \in B$. Also, for $y \in C$, $x \in B$, we have $f'(x, x, y) = v^{k-1}_{(0)}(y, y) = y$ since $f(x, x, y) = y$. Thus $f' \in \Phi_3$.

The more difficult half of the proof is now behind us. Let d be a 3-ary polynomial of $\mathbf{C}$ satisfying (1) and (2). (There is at least one, since any member of Φ_3 satisfies (1) and (2).) In the next paragraphs, we shall use the fact that $\langle \delta, \theta \rangle$ is Abelian (which follows from Lemma 4.12 and Lemma 4.14).

We wish to prove (3). So let $a, b \in B$ and define $f_0(x) = d(x, a, b)$, $f_1(x) = d(a, x, b)$, $f_2(x) = d(a, b, x)$. Assume that $a \in N_0$ and $b \in N_1$, where N_0 and N_1 are traces. We do not rule out the possibility that $N_0 = N_1$.

Claim 5. Either $f_i \in \operatorname{Sym} C$ for all $i \in \{0, 1, 2\}$, or $f_i(\theta) \subseteq \delta$ for all $i \in \{0, 1, 2\}$.

To prove the claim, we assume first that f_0 is a permutation. Then $\langle x, y \rangle \in \delta$ iff $\langle f_0(x), f_0(y) \rangle \in \delta$ (for all x, y in C). Choose $u \in N_0$ such that $\langle u, a \rangle \notin \delta$. Then $\langle f_0(a), f_0(u) \rangle \notin \delta$; i.e., $b = d(a, a, b) \not\equiv d(u, a, b) \pmod{\delta}$. Written another way, $d(u, u, b) = b \not\equiv d(u, a, b) \pmod{\delta}$; and since $\langle \delta, \theta \rangle$ is Abelian, we can replace the first and third occurrence of u in this formula by a, obtaining that $f_1(u) \not\equiv f_1(a) \pmod{\delta}$. therefore $f_1(\theta) \not\subseteq \delta$ and f_1 must be a permutation. All steps of this argument are reversible. Hence we can conclude that $f_0 \in \operatorname{Sym} C$ iff $f_1 \in \operatorname{Sym} C$. That $f_1 \in \operatorname{Sym} C$ iff $f_2 \in \operatorname{Sym} C$ is proved in exactly the same way.

Continuing with the proof of statement (3), suppose that one of the f_i fails to be a permutation, so that they all fail to be. Define $\beta(x) = d(a, d(a, x, b), x)$. If $x \in N_0$ then $d(a, x, b) = f_1(x) \overset{\delta}{\equiv} f_1(a) = b$, and so $\beta(x) \overset{\delta}{\equiv} d(a, b, x) = f_2(x)$. Therefore $(\beta(N_0))^2 \subseteq \delta$, implying that $\beta \notin \operatorname{Sym} C$ and $(\beta(N_1))^2 \subseteq \delta$. On the other hand, for $x \in N_1$, we have $d(a, x, b) = f_1(x) \overset{\delta}{\equiv} f_1(b) = a$, and so $\beta(x) \overset{\delta}{\equiv} d(a, a, x) = x$. Thus, for $x, y \in N_1$, we have $x \equiv \beta(x) \equiv \beta(y) \equiv y \pmod{\delta}$, contradicting that N_1 is a trace. This contradiction concludes our proof of (3).

Statement (4) is an immediately corollary of (3). If a and b belong to the body then $f_2(x) = f(a, b, x)$ defines a permutation $f_2 \in \operatorname{Pol}_1 \mathbf{C} \cap \operatorname{Sym} C$. This f_2 must map traces onto traces and must map B onto itself, and consequently $d(a, b, c) = f_2(c)$ is in B whenever $c \in B$.

Statement (5) also follows immediately from (3). For any two traces N_0 and N_1, we can choose $a \in N_0$ and $b \in N_1$ and consider the polynomial f_2 of the last paragraph. Since $f_2(b) = a$ and f_2^{-1} is a polynomial, it is obvious that $f_2(N_1) = N_0$ and that $f_2^{-1} : N_0 \simeq N_1$ (in the sense of Definition 2.7).

The above defined isomorphism leaves δ invariant, consequently $(f_2^{-1})_\delta$ is an isomorphism between the two minimal algebras $(\mathbf{C}|_{N_i})/(\delta|_{N_i})$. Thus we can conclude that all the traces are of type **2**. The operation d, restricted to any trace K, must define the ternary difference operation $x - y + z$ in the vector space $(\mathbf{C}|_K)/(\delta|_K)$, since this is the only Mal'cev polynomial in a vector space. □

DEFINITION 4.21. Let $\mathbf{C}$ be any algebra minimal relative to a congruence quotient $\langle \delta, \theta \rangle$. Let $\mathbf{i}$ be any of **1**, **2**, **3**, **4** or **5**. We say that $\mathbf{C}$ **has type i relative to** $\langle \delta, \theta \rangle$ iff for each $\langle \delta, \theta \rangle$-trace N, $(\mathbf{C}|_N)/(\delta|_N)$ is a minimal algebra of type **i**. (Equivalent phrases are: "The type of $\langle \delta, \theta \rangle$ in $\mathbf{C}$ is **i**." "$\mathbf{C}$ is $\langle \delta, \theta \rangle$-minimal of type **i**.")

DEFINITION 4.22. Suppose that $\mathbf{C}$ is a $\langle \delta, \theta \rangle$-minimal algebra of type **2** and that $d \in \operatorname{Pol}_3 \mathbf{C}$. Then d is a **pseudo-Mal'cev operation of** $\mathbf{C}$ **(with respect to** $\langle \delta, \theta \rangle$**)** iff it satisfies 4.20 (1–4).

THEOREM 4.23. *Every finite algebra* $\mathbf{C}$ *that is minimal with respect to a congruence quotient* $\langle \delta, \theta \rangle$ *is of one of the types* **1**, **2**, ..., **5** *relative to* $\langle \delta, \theta \rangle$. *Moreover, if the type is* **3**, **4** *or* **5** *then* θ *covers* δ. *The type is* **1** *or* **2** *iff* θ *is Abelian over* δ; *and the type is* **1** *iff* θ *is strongly Abelian over* δ.

PROOF. The first statement follows from Lemmas 4.12 and 4.20, the others from Lemma 4.14 and Exercises 4.19 (3 and 4). □

The unary type (i.e., type **1**) is in several respects an anomaly. We have seen that when $\mathbf{C}$ is $\langle \delta, \theta \rangle$-minimal of type other than **1**, a very "tight" internal structure prevails, relative to $\langle \delta, \theta \rangle$. In type **1**, all we can say is that the correlated minimal algebras are in a sense trivial (no operations depending on more than one variable),

and that $\langle \delta, \theta \rangle$ is strongly Abelian. However, we shall see that the following is true when $\langle \alpha, \beta \rangle$ is a tame quotient of $\mathbf{A}$ and $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$: The algebra $\mathbf{A}|_U$ has type **1** relative to $\langle \alpha|_U , \beta|_U \rangle$ iff β is strongly Abelian over α. What this means, in practice, is that type **1** never enters the picture if $\mathbf{A}$ satisfies any "non-trivial Mal'cev condition" (to be defined in Chapter 9). We think of type **1** as the black sheep of the family, and hope to exclude it whenever possible.

In the remainder of this chapter, we study E-minimal algebras, and probe deeper into the structure of $\langle \delta, \theta \rangle$-minimal algebras of type **2**. Most of the information to be obtained will not be needed until much later, so the reader may sensibly skip directly to Chapter 5 and return to these pages when the need arises.

LEMMA 4.24. *Let* $\mathbf{C}$ *be minimal of type* **2** *relative to its quotient* $\langle \delta, \theta \rangle$, *and let* N *be any* $\langle \delta, \theta \rangle$*-trace. The interval lattice* $I[\delta, \theta]$ *contained in* $\mathbf{Con}\,\mathbf{C}$ *is isomorphic to the congruence lattice of the vector space* $(\mathbf{C}|_N)/(\delta|_N)$.

PROOF. The congruence lattice of the vector space is isomorphic to the interval $I[\delta|_N , 1_N]$ in $\mathbf{Con}\,\mathbf{C}|_N$. By Lemma 2.4 (taking $A = U = C$ and $e = \mathrm{id}$), restriction is a homomorphism of $I[0_C, \theta]$ onto $\mathbf{Con}\,\mathbf{C}|_N$. Therefore, restriction maps $I[\delta, \theta]$ homomorphically onto $I[\delta|_N , 1_N]$. We have only to see that this homomorphism is one-to-one, i.e., that when $\delta \leq \alpha < \beta \leq \theta$ $(\alpha, \beta \in \mathrm{Con}\,\mathbf{C})$ then $\alpha|_N < \beta|_N$. To do this, choose any pair $\langle c, d \rangle \in \beta - \alpha$. Since $\langle c, d \rangle \in \theta - \delta$ too, there exists a $\langle \delta, \theta \rangle$-trace N' with $c,\ d \in N'$. By Lemma 4.20 (5), there exists $f \in \mathrm{Pol}_1\mathbf{C} \cap \mathrm{Sym}\,C$ such that $f(N') = N$. All congruences of $\mathbf{C}$ are invariant under f; hence $\langle f(c), f(d) \rangle \in \beta|_N - \alpha|_N$. This ends the proof. □

LEMMA 4.25. *Let* $\mathbf{C}$ *be minimal of type* **2** *relative to* $\langle \delta, \theta \rangle$. *Let* B *be the body,* T *be the tail, and* d *be a pseudo-Mal'cev operation, with respect to* $\langle \delta, \theta \rangle$. *There do not exist elements* $b \in B$ *and* $t \in T$ *such that* $d(t, t, b) \equiv b \pmod{\theta}$ *(or* $d(b, t, t) \equiv b \pmod{\theta}$*).*

PROOF. Suppose otherwise, say t is in the tail, while b and $d(t, t, b) = c$ lie in the same trace N. Define a unary polynomial, h, by setting

$$h(x) = d(x, d(t, d(t, x, b), b), c).$$

The properties assumed of d are, by Definition 4.22, enumerated in Lemma 4.20. Notice that for any $u, v \in N$ we have $t = d(t, u, u) \equiv d(t, u, v) \pmod{\theta}$, which implies that $t \equiv d(t, u, v) \pmod{\delta}$ since t is in the tail. For any $x \in N$, we calculate that $d(t, x, b) \equiv t \pmod{\delta}$, then

$$d(t, d(t, x, b), b) \overset{\delta}{\equiv} d(t, t, b) = c,$$

and therefore

$$h(x) \overset{\delta}{\equiv} d(x, c, c) = x.$$

This fact implies that $h(\theta) \not\subseteq \delta$ and so h is a permutation. Therefore $h(t) \notin B$. But

$$h(t) = d(t, d(t, c, b), c) \overset{\theta}{\equiv} d(t, d(t, b, b), b) = c,$$

implying that $h(t) \in B$. This contradiction proves the lemma. □

LEMMA 4.26. *Let* $\mathbf{C}$ *be minimal of type* **2** *relative to* $\langle \delta, \theta \rangle$. *There do not exist elements* t, a, b *and a 3-ary polynomial* f *of* $\mathbf{C}$ *satisfying:* t *is in the tail,* $\langle a, b \rangle \in \theta - \delta$, *and*

$$f(t, t, a) = f(a, a, a) = a, \quad f(t, a, a) = t, \quad f(b, a, a) = b.$$

PROOF. Assuming that these elements and polynomial exist, we define

$$h(x) = f(x, f(t, f(t, x, a), a), a),$$

calculate that $h(t) = h(a) = a$ while $h(b) \equiv b \pmod{\delta}$, and reach the same contradiction as in the last proof. □

LEMMA 4.27. *Let* $\mathbf{C}$ *be minimal of type* **2** *relative to* $\langle \delta, \theta \rangle$, *and let* B *be the body and* T *be the tail of* $\mathbf{C}$ *with respect to* $\langle \delta, \theta \rangle$.

(1) *The formula:* $\langle a, b \rangle \in \beta \leftrightarrow$ "*for all* $f \in \mathrm{Pol}_2\mathbf{C}$, $f(a, x) \in \mathrm{Sym}\, C$ *iff* $f(b, x) \in \mathrm{Sym}\, C$," *defines a congruence* β *of* $\mathbf{C}$ *satisfying* $\beta \subseteq B^2 \cup T^2$.

(2) *For all* $f \in \mathrm{Pol}_1\mathbf{C}$, *if* $f \notin \mathrm{Sym}\, C$ *then* $f(B) \times f(B) \subseteq \beta$.

(3) *The relation* $B^2 \cup \beta$ *is a congruence having* B *as an equivalence class. Thus, if* $f \in \mathrm{Pol}_n\mathbf{C}$ *(for any* n*) then either* $f(B^n) \subseteq B$ *or* $f(B^n) \subseteq T$.

(4) *The largest congruence,* $\bar{\beta}$, *included in* $B^2 \cup T^2$ *satisfies:*
   (i) For all $\lambda \in \mathrm{Con}\, \mathbf{C}$, *either* $\lambda \leq \bar{\beta}$ *or* $\delta \vee \lambda \geq \theta$.
   (ii) For every quotient $\langle \gamma, \lambda \rangle$ *of* $\mathbf{C}$, *if* $\gamma \leq \bar{\beta}$ *and* $\lambda \not\leq \bar{\beta}$ *then* $\langle \gamma, \lambda \rangle$ *is non-Abelian.*

PROOF. It is easy to check that β is a congruence. Let d be the pseudo-Mal'cev operation. If $b \in B$ and $t \in T$, and we put $f(x, y) = d(x, b, y)$, then $f(b, x) \in \mathrm{Sym}\, C$ and $f(t, x) \notin \mathrm{Sym}\, C$. Therefore $\beta \subseteq B^2 \cup T^2$.

To prove (2), let $f \in \mathrm{Pol}_1\mathbf{C}$, $f \notin \mathrm{Sym}\, C$. Let $a, b \in B$ and choose $a', b' \in B$ such that $\langle a, a' \rangle \in \theta - \delta$, $\langle b, b' \rangle \in \theta - \delta$. We are to show that $\langle f(a), f(b) \rangle \in \beta$. Let $h \in \mathrm{Pol}_2\mathbf{C}$ be such that $h(f(a), x)$ is a permutation. Defining $h'(x) = h(f(x), x)$, we have

$$h'(a') = h(f(a'), a') \equiv h(f(a), a') \not\equiv h(f(a), a) = h'(a) \pmod{\delta}.$$

Therefore $h' \in \mathrm{Sym}\, C$, and

$$h(f(b), b) \not\equiv h(f(b'), b') \equiv h(f(b), b') \pmod{\delta};$$

consequently, $h(f(b), x)$ is a permutation. This proves that $\langle f(a), f(b)\rangle \in \beta$.

To prove (3), note that $\beta \cup B^2$ is an equivalence relation having B as an equivalence class, since $\beta \cap (T \times B) = \emptyset$. If $f \in (\mathrm{Pol}_1\mathbf{C}) \cap (\mathrm{Sym}\, C)$, then clearly f leaves this equivalence relation invariant. If $f \in \mathrm{Pol}_1\mathbf{C} - \mathrm{Sym}\, C$ then, again, f preserves the equivalence, by (2). Thus $\beta \cup B^2$ is a congruence.

To prove (4i), assume that $\lambda \in \mathrm{Con}\,\mathbf{C}$ and $\lambda \not\subseteq B^2 \cup T^2$. Let $\langle b, t\rangle \in \lambda \cap (B \times T)$. For any $a \equiv b \pmod{\theta}$ we have $a = d(b, b, a) \overset{\lambda}{\equiv} d(t, b, a) \overset{\delta}{\equiv} t$. Thus $N^2 \subseteq \delta \vee \lambda$, where $N = b/\theta$. By Lemma 4.20 (5), we have $\theta \leq \delta \vee \lambda$.

To prove (4ii), assume that $\gamma \leq \lambda \wedge \bar{\beta}$, $\lambda \not\leq \bar{\beta}$, and $\langle \gamma, \lambda\rangle$ is Abelian. We shall derive a contradiction. We choose a pair $\langle b, u\rangle \in \lambda \cap (B \times T)$. Since $d(u, u, u) = d(b, b, u)$ and $\langle \gamma, \lambda\rangle$ is Abelian, it follows that $d(u, u, b) \equiv d(b, b, b) = b \pmod{\gamma}$. Since $\gamma \leq \bar{\beta}$, the element $c = d(u, u, b)$ belongs to the body. We consider, once again, the polynomial $h(x) = d(x, d(u, d(u, x, b), b), b)$. Choose a so that $\langle a, b\rangle \in \theta - \delta$. Notice that

$$h(b) = d(b, c, b), \quad \text{and}$$
$$h(a) \equiv d(a, c, b) (\mathrm{mod}\ \delta)\ .$$

By Lemma 4.20, it follows that $\langle h(a), h(b)\rangle \in \theta - \delta$. Thus h is a permutation. But since $\langle b, c\rangle \in \gamma$, modulo γ we have

$$h(u) \equiv d(u, u, b) = c\ .$$

Since $\gamma \leq \bar{\beta}$, it follows that $h(u) \in B$, which is impossible. This contradiction finishes the proof. □

Recall that $\mathrm{E}(\mathbf{C})$ denotes the set of all $f \in \mathrm{Pol}_1\mathbf{C}$ satisfying $f^2 = f$. The algebra $\mathbf{C}$ is called E-*minimal* iff $\mathbf{C}$ has at least two elements and $\mathrm{E}(\mathbf{C})$ contains only constants and the identity function (Definition 2.14).

LEMMA 4.28. *Let $\mathbf{C}$ be a finite algebra of at least two elements. Then $\mathbf{C}$ is* E-*minimal iff $\mathbf{C}$ is minimal relative to every one of its prime congruence quotients.*

PROOF. Suppose that $\mathbf{C}$ is E-minimal, and let δ and θ be congruences of $\mathbf{C}$ such that $\delta \prec \theta$. Then $\langle \delta, \theta\rangle$ is tame (by Theorem 2.11), hence there exists $e \in \mathrm{E}(\mathbf{C})$ such that $e(C)$ is a $\langle \delta, \theta\rangle$-minimal set. Obviously, e cannot be constant, so $e = \mathrm{id}_C$ and $C = e(C)$ is $\langle \delta, \theta\rangle$-minimal—i.e., the algebra $\mathbf{C}$ is minimal relative to $\langle \delta, \theta\rangle$.

Second, suppose that $\mathbf{C}$ is not E-minimal, and pick $e \in \mathrm{E}(\mathbf{C})$ satisfying $1 < |e(C)| < |C|$. Let δ be the largest congruence μ of $\mathbf{C}$ satisfying $\mu|_{e(C)} = 0_{e(C)}$. We have $\delta < 1_C$ since $e(C)$ has more than one element. Choose for θ any congruence that covers δ. There exists $\langle x, y\rangle \in \theta|_{e(C)}$ with $x \neq y$. We have $\langle e(x), e(y)\rangle = \langle x, y\rangle \in \theta - \delta$; consequently $e(\theta) \not\subseteq \delta$, and it follows that $\mathbf{C}$ is not $\langle \delta, \theta\rangle$-minimal, since e is not a permutation. □

LEMMA 4.29. *If an* E*-minimal algebra* $\mathbf{C}$ *has a prime quotient of type* **3**, **4** *or* **5**, *then* $|C| = 2$.

PROOF. Let $\mathbf{C}$ be E-minimal and $\langle \delta, \theta \rangle$ be a non-Abelian prime quotient of $\mathbf{C}$. (This means a quotient of type **3**, **4** or **5**.) The structure of $\mathbf{C}$ with respect to $\langle \delta, \theta \rangle$ is described in Lemma 4.15 or Lemma 4.17.

We assume first that Lemma 4.17 applies ($\langle \delta, \theta \rangle$ has type **3** or **4**), and we use the notation of that lemma. Let $e(x) = p(0, x)$ and note that by Lemma 4.17 (3 and 5), $e \in \mathrm{E}(\mathbf{C})$ and $e(1) = e(0) = 0$, while $e(x) \equiv x \pmod{\delta}$ for all $x \in C - N$. Since $\mathbf{C}$ is E-minimal, these facts imply that e is constant and $C = N = \{0, 1\}$.

Now we assume that Lemma 4.15 applies ($\langle \delta, \theta \rangle$ has type **5**). Choose $u \in O$ and put $e(x) = p(u, x)$. From the E-minimality of $\mathbf{C}$ and the facts expressed in Lemma 4.15, it follows that e is constant, $e(x) = u$ for all x, and $C = N = O \cup \{1\}$. Since this holds for all $u \in O$, we have that $p(x, y) = x$ for all $x, y \in O$. But now the operation $f(x) = p(x, u)$, where $u \in O$ is fixed, satisfies: $f(1) = u$, $f(x) = x$ for all $x \neq 1$. Thus $f \in \mathrm{E}(\mathbf{C})$ and f is constant, implying that $C = N = \{1, u\}$. □

LEMMA 4.30. *Let* $\mathbf{C}$ *be minimal of type* **2** *relative to* $\langle \delta, \theta \rangle$, *and let* B *be the* $\langle \delta, \theta \rangle$*-body of* $\mathbf{C}$. *If* $e \in \mathrm{E}(\mathbf{C})$ *and* $e \neq \mathrm{id}_C$, *then* $|e(C) \cap B| \leq 1$.

PROOF. Suppose that $e \in \mathrm{E}(\mathbf{C})$, $e \neq \mathrm{id}$, and e has a fixed point b (i.e., $e(b) = b$) belonging to B. We show that there are no other fixed points of e in B. Let d be a pseudo-Mal'cev operation relative to $\langle \delta, \theta \rangle$. Define a polynomial h by setting $h(x) = d(b, e(x), x)$. Then letting N denote the trace which contains b, we have $e(N) \subseteq N$. In fact, $e(N) \subseteq b/\delta$, since otherwise e would have to be a permutation (implying $e = \mathrm{id}$). Therefore for $x \in N$, we have $h(x) \equiv x \pmod{\delta}$; and it follows that h is a permutation. Now if b' is any fixed point of e lying inside B, then $h(b') = b = h(b)$, consequently $b' = b$. □

THEOREM 4.31. *Let* $\mathbf{C}$ *be minimal of type* **2** *relative to* $\langle \delta, \theta \rangle$, *and let* B *be the* $\langle \delta, \theta \rangle$*-body of* $\mathbf{C}$. *Then* $\mathbf{C}|_B$ *is an* E*-minimal algebra, and it is minimal of type* **2** *relative to* $\langle \delta|_B, \theta|_B \rangle$. *Moreover, these statements are equivalent: (1)* $C = B$; *(2)* $\mathbf{C}$ *is* E*-minimal; (3)* $\mathbf{C}|_C$ *is Mal'cev.*

PROOF. Lemma 4.30 easily implies that $\mathbf{C}|_B$ is E-minimal. To see it, let $e \in \mathrm{E}(\mathbf{C}|_B)$. We can find $f \in \mathrm{Pol}_1\mathbf{C}$ with $f|_B = e$. Choose $n > 0$ such that $f^n \in \mathrm{E}(\mathbf{C})$. We have $e = f^n|_B$ since $e = e^2$. Now apply Lemma 4.30 to f^n.

By a similar calculation, $\mathbf{C}|_B$ is minimal relative to $\langle \delta|_B, \theta|_B \rangle$. It is easily seen that the type must still be **2**.

Now (3) implies (1) by Lemma 4.26 (Mal'cev algebras are defined in Definition 4.5); and we have seen in the first paragraph of this proof that (1) implies (2). Also, (1) implies (3) by Lemma 4.20; i.e., $\mathbf{C}|_B$ is Mal'cev. All that remains is to prove that (2) implies (1).

We assume that (2) holds and (1) fails, and derive a contradiction. Let $\bar{\beta}$ be the largest congruence of $\mathbf{C}$ included in $B^2 \cup T^2$ where T is the tail. (See Lemma 4.27.) Obviously, $\theta \leq \bar{\beta} < 1_C$. Let λ be any congruence covering $\bar{\beta}$. By Lemma 4.28, $\mathbf{C}$ is minimal relative to $\langle \bar{\beta}, \lambda \rangle$. What is the type relative to $\langle \bar{\beta}, \lambda \rangle$? Since $B \neq C$, we have $|C| \geq 3$; hence Lemma 4.28 implies that this type can only be **1** or **2**. By Theorem 4.23, $\langle \bar{\beta}, \lambda \rangle$ is Abelian. We have a contradiction to Lemma 4.27 (4(ii)). □

THEOREM 4.32. *Every* E*-minimal algebra possesses one of the types defined below:*

(1) $\mathbf{C}$ *has type* **1** *iff all of its prime congruence quotients have type* **1**.

(2) $\mathbf{C}$ *has type* **2** *iff all of its prime congruence quotients have type* **2**. *Any finite algebra with more than one element is* E*-minimal of type* **2** *iff it has a Mal'cev 3-ary polynomial and is minimal of type* **2** *relative to one of its congruence quotients.*

(3) $\mathbf{C}$ *has type* **3** *(or* **4** *or* **5***) iff it is a two-element minimal algebra of type* **3** *(or* **4** *or* **5**, *respectively).*

PROOF. Let $\mathbf{C}$ be E-minimal. By Lemma 4.28, relative to each of its prime congruence quotients, $\mathbf{C}$ is minimal and the quotient has a type. It is immediate from Lemma 4.29 that if $\mathbf{C}$ has a quotient of type **3**, **4** or **5**, then it is a two-element minimal algebra of the same type, and therefore $\mathbf{C}$ has one of the types defined in part (3) of this theorem. An algebra of one of these types has, of course, no quotients of type **1** or **2**.

Suppose that $\mathbf{C}$ has a prime quotient of type **2**. Since (2) implies (3) in Theorem 4.31, $\mathbf{C}$ has a Mal'cev polynomial d. Then every induced algebra $(\mathbf{C}|_N)/(\delta|_N)$, where N is a congruence class and δ a congruence in $\mathbf{C}$, has a Mal'cev polynomial. Therefore $\mathbf{C}$ certainly cannot be minimal of type **1** relative to any quotient; and it follows that all prime quotients of $\mathbf{C}$ are of type **2**.

The only remaining possibility is that all prime quotients have type **1**.

The assertion in part (2) of the theorem is an easy consequence of Theorem 4.31 and the considerations just concluded. □

LEMMA 4.33. *Any* E*-minimal algebra of type* **2** *is solvable. Any* E*-minimal algebra of type* **1** *is strongly solvable.*

PROOF. Let $\mathbf{C}$ be E-minimal of type **2**. Let $0_C = \theta_0 \prec \theta_1 \prec \cdots \prec \theta_n = 1_C$ be any maximal chain in the congruence lattice of $\mathbf{C}$. For each $i < n$, $\mathbf{C}$ is minimal of type **2** relative to $\langle \theta_i, \theta_{i+1} \rangle$. Therefore θ_{i+1} is Abelian over θ_i, by Theorem 4.23. Now $\mathbf{C}$ is solvable, by Definition 3.6. The proof of strong solvability when the type is **1** follows the same pattern. (Use Definition 3.10.) □

COROLLARY 4.34. *Let* $\mathbf{C}$ *be minimal of type* **2** *relative to* $\langle \delta, \theta \rangle$, *with body* B. *Let* β *be the congruence of* $\mathbf{C}$ *defined in Lemma 4.27. Then* B *is an equivalence class of* β.

PROOF. By Lemma 4.27, B is a union of β-equivalence classes. Suppose that $\langle u, v \rangle \in B^2 - \beta$. This means that there exists $f \in \mathrm{Pol}_2\mathbf{C}$ such that $f(u, x) \in \mathrm{Sym}\, C$ and $f(v, x) \notin \mathrm{Sym}\, C$ (or the same condition with u and v interchanged). Let λ be the congruence of $\mathbf{C}|_B$ generated by $\langle u, v \rangle$, and τ be a subcover of λ in $\mathbf{Con}\, \mathbf{C}|_B$. Note that $\langle u, v \rangle \notin \tau$. By Theorems 4.31 and 4.32 , $\mathbf{C}|_B$ is minimal of type **2** relative to its prime quotient $\langle \tau, \lambda \rangle$; and therefore $\langle \tau, \lambda \rangle$ is Abelian. Since $f(u, x) \in \mathrm{Sym}\ C$, we have $f(u, u) \in B$. Therefore, by Lemma 4.27 (3), $f(B^2) \subseteq B$, and $f|_B$ is a polynomial of $\mathbf{C}|_B$. Letting $h(x) = f(v, x)$, we have that $h \notin \mathrm{Sym}\, C$, implying that $h(\theta) \subseteq \delta$, which implies that $h|_B \notin \mathrm{Sym}\, B$, and that $h(\lambda) \subseteq \tau$. Therefore $f(v, u) = h(u) \overset{\tau}{\equiv} h(v) = f(v, v)$. Now since $\langle \tau, \lambda \rangle$ is Abelian, we have $f(u, u) \overset{\tau}{\equiv} f(u, v)$. But this is impossible; the function $h'(x) = f(u, x)$, restricted to B, belongs to $\mathrm{Sym}\, B \cap \mathrm{Pol}_1\mathbf{C}|_B$ and must satisfy $h'^{-1}(\tau) = \tau$. The contradiction proves the corollary. □

The next result asserts that E-minimal algebras of type **2** are nilpotent. These algebras are very interesting to us, due to the role that they play in our subdirect representation theorem for congruence lattices of finite algebras in congruence modular varieties (Theorem 8.7). In Chapter 13, we shall finish the work begun in Lemma 4.20 by showing how every E-minimal algebra of type **2** can be constructed from a vector space (Theorem 13.9); the cardinality of such an algebra is always a prime power. In Exercise 4.37 (6), we outline a proof that every finite group of order p^k, p a prime and $k > 0$, is an E-minimal algebra of type **2**.

DEFINITION 4.35. Let $\mathbf{A}$ be any algebra. For congruences α, β we define $[\alpha, \beta]$ to be the smallest congruence δ such that $C(\alpha, \beta; \delta)$. (See Exercises 3.8 (2–4).) Inductively, we define $(1]^1 = [1)^1 = 1_A$, $(1]^{n+1} = [1_A, (1]^n]$, $[1)^{n+1} = [\,[1)^n, 1_A]$. We say that $\mathbf{A}$ is **left** (**right**) **nilpotent** iff for some n, $(1]^n = 0_A$ (or $[1)^n = 0$).

If $\mathbf{A}$ has a Mal'cev polynomial then, by the result of Exercise 3.8 (4), $[\alpha, \beta] = [\beta, \alpha]$ and the two concepts of nilpotency coincide.

LEMMA 4.36. *Every* E*-minimal algebra of type* **2** *is nilpotent.*

PROOF. Let $\mathbf{C}$ be E-minimal of type **2**. We begin the proof by defining a special congruence of $\mathbf{C}$.

$$\lambda = \bigcap \{\mathrm{ann}(\delta \mid \theta) \ : \ \delta \prec \theta \text{ and } \delta, \theta \in \mathrm{Con}\, \mathbf{C}\} \ .$$

A pair $\langle u, v\rangle$ in C^2 belongs to λ iff for all prime quotients $\langle \delta, \theta\rangle$ and for all $f \in \mathrm{Pol}_n \mathbf{C}$ (for any n) and for all $x_1, y_1, \ldots, x_{n-1}, y_{n-1}$ in $\mathbf{C}$ such that $\{\langle x_i, y_i\rangle : 1 \leq i < n\} \subseteq \theta$, we have

$$f(u, \bar{x}) \equiv f(u, \bar{y}) \pmod{\delta} \leftrightarrow f(v, \bar{x}) \equiv f(v, \bar{y}) \pmod{\delta}\,. \tag{4.36.1}$$

We claim that $\lambda = 1_C$. To prove it, assume to the contrary that we have a pair $\langle u, v\rangle \in C^2 - \lambda$. Choose a Mal'cev 3-ary polynomial $d(x, y, z)$ of $\mathbf{C}$. (By Theorem 4.32, such a polynomial exists.) Choose a prime quotient $\langle \delta, \theta\rangle$, a polynomial f, and pairs $\langle a_1, b_1\rangle, \ldots, \langle a_n, b_n\rangle$ in θ, witnessing a failure of (4.36.1); say $\langle f(u, \bar{a}), f(u, \bar{b})\rangle \in \delta$ and $\langle f(v, \bar{a}), f(v, \bar{b})\rangle \notin \delta$.

Now define

$$f'(x, \bar{z}) = d(f(x, \bar{z}), f(x, \bar{b}), f(v, \bar{b})).$$

Notice that

$$f(v, \bar{b}) = f'(v, \bar{b}) = f'(u, \bar{b}) \overset{\delta}{\equiv} f'(u, \bar{a})$$

and $f(v, \bar{a}) = f'(v, \bar{a})$. Therefore $\langle f'(u, \bar{a}), f'(v, \bar{a})\rangle \notin \delta$ while $f'(u, \bar{b}) = f'(v, \bar{b})$. One can transform the pair $\langle f'(u, \bar{b}), f'(v, \bar{b})\rangle$ into the pair $\langle f'(u, \bar{a}), f'(v, \bar{a})\rangle$ by changing b_1 to a_1, then b_2 to a_2, and so on. At some i^{th} step in this process, the pair moves from inside δ to outside δ. Then with $g(x, y) = f'(y, a_1, \ldots, a_{i-1}, x, b_{i+1}, \ldots, b_n)$, and $\langle a, b\rangle = \langle a_i, b_i\rangle$, we have: $g(b, u) \equiv g(b, v) \pmod{\delta}$, and $g(a, u) \not\equiv g(a, v) \pmod{\delta}$, and $\langle a, b\rangle \in \theta$.

Using the binary polynomial g just constructed, we define another:

$$h(x, y) = d(g(x, y), g(x, v), g(a, v)). \tag{4.36.2}$$

Notice that $h(a, u) = g(a, u)$ and

$$h(b, u) \overset{\delta}{\equiv} d(g(b, v), g(b, v), g(a, v)) = g(a, v).$$

Thus $\langle h(a, u), h(b, u)\rangle \in \theta - \delta$, and we conclude that $h^u(x) = h(x, u)$ is a permutation of C, since $\mathbf{C}$ is $\langle \delta, \theta\rangle$-minimal. On the other hand, $h^v(x) = h(x, v)$ is constant $(= g(a, v))$. This contradicts Corollary 4.34, since $\mathbf{C}$ is its own body with respect to $\langle \delta, \theta\rangle$. Therefore $\lambda = 1_C$, and it follows by Definition 4.35 that $\mathbf{C}$ is nilpotent. □

Exercises 4.37

(1) Let $\mathbf{C}$ be minimal of type **1** relative to its quotient $\langle \delta, \theta\rangle$. Let $N_0, \ldots, N_{k-1}$ be $\langle \delta, \theta\rangle$-traces of $\mathbf{C}$ such that $N_i \not\simeq N_j$ for $0 \leq i < j < k$, and every $\langle \delta, \theta\rangle$-trace N satisfies $N \simeq N_i$ for some i. Prove that the interval $I[\delta, \theta]$ is isomorphic to $\prod\{\mathbf{Con}\,((\mathbf{C}|_{N_i})/(\delta|_{N_i})) : 0 \leq i < k\}$. (See the proof of Lemma 4.24 for how to proceed.)

(2) Construct an algebra minimal of type **2** relative to a quotient $\langle 0, \theta \rangle$, and possessing a non-empty tail. Here is a recipe. Let $\mathbf{B} = \langle B, +, -, 0 \rangle$ be a finite Abelian group satisfying $px = 0$ for a certain prime p. Let T be a finite set disjoint from B, having an element $t_0 \in T$. Define an operation on $C = B \cup T$ by

$$d(x,y,z) = \begin{cases} x - y + z & \text{if } \{x,y,z\} \subseteq B; \\ u & \text{if } \{x,y,z\} \cap T = \{u\}; \\ t_0 & \text{otherwise .} \end{cases}$$

Define $\theta = 0_C \cup B^2$. Prove that $\mathbf{C} = \langle C, d \rangle$ is minimal of type **2** relative to $\langle 0_C, \theta \rangle$ with body B and tail T. (The exercise involves proving some easy facts about all the polynomial operations of $\mathbf{C}$.) Note that if $\mathbf{B}$ is a two-element group and $|T| = 1$ then $\mathbf{C}$ is polynomially equivalent to a three-element semigroup formed by adjoining a zero element to $\mathbf{B}$.

(3) Suppose that $\mathbf{C}$ is minimal of type **3** relative to $\langle \delta, \theta \rangle$. (See Lemma 4.17.) Prove that $\mathbf{C}$ has a pseudo-Mal'cev operation with respect to $\langle \delta, \theta \rangle$. Show that Lemmas 4.25, 4.26 and 4.27 are valid in this situation. (So is Lemma 4.30, but this lemma is now trivial.)

(4) Let $\mathbf{C}$ be an algebra minimal with respect to quotients $\langle \delta_i, \theta_i \rangle$ $(i = 0, 1)$ and of type **2** or **3** relative to each. Let B_i be the $\langle \delta_i, \theta_i \rangle$-body. Prove that either $B_0 = B_1$ or $B_0 \cap B_1 = \emptyset$. (Use Lemma 4.26 and the previous exercise.)

(5) Prove the result of statement 4(i) in Lemma 4.27 under the assumption that $\mathbf{C}$ is minimal of type **3** or **4** relative to $\langle \delta, \theta \rangle$; and prove the result of statement 4(ii) under the assumption that $\mathbf{C}$ is minimal of type **3**, **4** or **5** relative to $\langle \delta, \theta \rangle$.

(6) Let p be a prime integer and $\mathbf{G}$ be a group of order p^k. Prove that $\mathbf{G}$ is E-minimal of type **2**. [Letting $h \in \mathrm{E}(\mathbf{G})$ be nonconstant, it must be shown that $h(x) = x$. Choose $c \in h(G)$ and define $e(x) = h(xc)c^{-1}$. Then $e = e^2$, $e(1) = 1$, and e is non-constant. Show that there exist $a_1, \ldots, a_n \in G$ with $e(x) = a_1^{-1} x a_1 a_2^{-1} x a_2 \cdots a_n^{-1} x a_n$. Let $G^{(0)} = G, \ldots, G^{(m)} = \{1\}$ be the upper central series of G, so that $[G, G^{(i)}] = G^{(i+1)}$. Now show that $p \mid n(n-1)$ and, inducting on i, show that $e(x) \equiv x \pmod{G^{(i)}}$ if $p \mid n - 1$, and that $e(x) \equiv 1 \pmod{G^{(i)}}$ if $p \mid n$.]

5. THE TYPES OF TAME QUOTIENTS

We are now ready to define and study the five types of tame congruence quotients. In this chapter, we will delineate the distinct characters of these types, primarily in relation to the "polynomial structure" of an algebra. In the next two chapters, we shall consider the congruence lattice of an algebra as a labeled graph, where all of the prime quotients are labeled with their respective types. We shall be concerned with the ways in which this labeling is influenced by the unlabeled congruence lattice, construed purely as an abstract lattice.

DEFINITION 5.1.

(1) Let $\langle \alpha, \beta \rangle$ be a tame quotient of congruences in a finite algebra $\mathbf{A}$. Let U be any element of $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. We define the **type of** $\langle \alpha, \beta \rangle$, written $\mathrm{typ}(\alpha, \beta)$, to be the type of $\mathbf{A}|_U$ relative to $\langle \alpha|_U, \beta|_U \rangle$.

(2) Let $\langle \gamma, \lambda \rangle$ be any quotient of congruences in a finite algebra $\mathbf{A}$. By $\mathrm{typ}\{\gamma, \lambda\}$ we denote the set $\{\mathrm{typ}(\alpha, \beta) : \gamma \leq \alpha \prec \beta \leq \lambda\}$.

(3) Let $\mathbf{A}$ be any finite algebra. We call $\mathbf{A}$ **tame** iff the quotient $\langle 0_A, 1_A \rangle$ is tame (implying that $|A| > 1$). If $\mathbf{A}$ is tame, we put $\mathrm{typ}(\mathbf{A}) = \mathrm{typ}(0_A, 1_A)$.

(4) Let $\mathbf{A}$ be any finite algebra. By $\mathrm{typ}\{\mathbf{A}\}$ we denote the set $\mathrm{typ}\{0_A, 1_A\}$ of types.

The type of a tame quotient $\langle \alpha, \beta \rangle$ in a finite algebra $\mathbf{A}$ is well-defined by the above. To verify this, let U_0 and U_1 be $\langle \alpha, \beta \rangle$-minimal sets. According to Theorem 2.8 (1) and Exercise 2.9 (5), there exists an isomorphism between the structures $\langle U_0, \mathrm{Pol}\,\mathbf{A}|_{U_0}, \alpha|_{U_0}, \beta|_{U_0} \rangle$ and $\langle U_1, \mathrm{Pol}\,\mathbf{A}|_{U_1}, \alpha|_{U_1}, \beta|_{U_1} \rangle$. Therefore the type of $\mathbf{A}|_{U_i}$ relative to $\langle \alpha|_{U_i}, \beta|_{U_i} \rangle$ is the same for $i = 0$ and $i = 1$.

A first corollary of this definition and of our earlier work is worth noting. Recall that for a tame quotient $\langle \alpha, \beta \rangle$ in $\mathbf{A}$, an $\langle \alpha, \beta \rangle$-trace is simply any set N such that for some $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $x \in U$, we have $N = (x/\beta) \cap U \neq (x/\alpha) \cap U$.

COROLLARY 5.2. *Let $\langle \alpha, \beta \rangle$ be a tame quotient in a finite algebra $\mathbf{A}$.*

(1) *For every $\langle \alpha, \beta \rangle$-trace N, the algebra $\mathbf{M} = (\mathbf{A}|_N)/(\alpha|_N)$ is a minimal (and therefore tame) algebra, and $\mathrm{typ}(\alpha, \beta) = \mathrm{typ}(\mathbf{M})$.*

(2) *If $\mathrm{typ}(\alpha, \beta) \neq \mathbf{1}$ or if $\alpha \prec \beta$, then for every pair of $\langle \alpha, \beta \rangle$-traces N_0 and N_1, we have $N_0 \simeq N_1$ and $\mathbf{M}_0 \cong \mathbf{M}_1$, where $\mathbf{M}_i = (\mathbf{A}|_{N_i})/(\alpha|_{N_i})$.*

PROOF. Let U be any $\langle \alpha, \beta \rangle$-minimal set and let N be an $\langle \alpha|_U, \beta|_U \rangle$-trace. Put $\mathbf{C} = \mathbf{A}|_U$ and $\langle \delta, \theta \rangle = \langle \alpha|_U, \beta|_U \rangle$. Note that $\mathbf{C}|_N = \mathbf{A}|_N$, since U is the range of some unary polynomial e of $\mathbf{A}$ with $e = e^2$. Thus $\mathbf{M} = (\mathbf{A}|_N)/(\alpha|_N) = (\mathbf{C}|_N)/(\delta|_N)$. The type of $\mathbf{C}$ relative to $\langle \delta, \theta \rangle$ (equal to $\operatorname{typ}(\alpha, \beta)$ by Definition 5.1) was defined in Definition 4.21 to be the type of the minimal algebra $\mathbf{M}$. (Recall from Chapter 4 that this is independent of N.) Since M is the only $\langle 0_M, 1_M \rangle$ trace in $\mathbf{M}$, this type is the same as $\operatorname{typ}(\mathbf{M})$. This concludes the proof of (1).

For $i \in \{0, 1\}$, let N_i be an $\langle \alpha|_{U_i}, \beta|_{U_i} \rangle$-trace, where $U_i \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. We have $U_0 \simeq U_1$ in $\mathbf{A}$, so $N_1 \simeq N'$ in $\mathbf{A}$ for some $\langle \alpha|_{U_0}, \beta|_{U_0} \rangle$-trace N'. Suppose that $\operatorname{typ}(\alpha, \beta) \neq \mathbf{1}$. Then by Lemmas 4.12 and 4.20 (5) all $\langle \alpha_0, \beta_0 \rangle$-traces are $\simeq$ in $\mathbf{A}|_{U_0}$. This implies that $N_0 \simeq N' \simeq N_1$ in $\mathbf{A}$. (For the definition of polynomial isomorphism, $\simeq$, see Definition 2.7 and the remarks following it.) If $\alpha \prec \beta$, then Lemma 2.3 implies that $\alpha|_{U_0} \prec \beta|_{U_0}$. Thus $\alpha|_{U_0} \vee \Theta(N_0^2) = \beta|_{U_0}$, and this implies that there is $f \in \operatorname{Pol}_1 \mathbf{A}|_{U_0}$ such that $f(N_0) \cap N' \neq \emptyset$ and $f(N_0)^2 \not\subseteq \alpha$. By 2.8 (3), $f \in \operatorname{Sym} U_0$, and it follows that $f(N_0) = N'$ and $N_0 \simeq N'$ as before. □

To avoid monotony, we shall sometimes refer to the types by their names, introduced in Definition 4.10. These are, in the order $\mathbf{1}, \ldots, \mathbf{5}$: **unary, affine, Boolean, lattice,** and **semilattice** type. The **lattice of types** is pictured below:

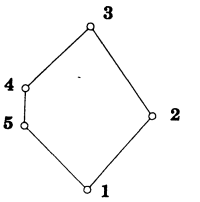


Figure 10

This lattice is obtained from the lattice pictured below Lemma 4.8 by identifying two-element algebras which have the same type, namely $\mathbf{E}_5$ and $\mathbf{E}_6$, $\mathbf{E}_0$ and $\mathbf{E}_1$. (This identification is *not* a lattice homomorphism.) The ordering of types pictured in Figure 10 is in terms of the richness of the set of binary operations depending on both variables, in the polynomial clone of a two-element algebra of the type. For each of the six proper order ideals in the lattice of types, we shall prove in Chapter 9 an *omitting types theorem.* These theorems will characterize locally finite varieties which have no prime quotients of a type belonging to a given ideal, in terms of several equivalent conditions not involving tame congruence theory. For example, a locally finite variety omits the types **1**, **2**, **5** if and only if the congruence lattices of its finite algebras are semi-distributive.

Here is an important corollary of our earlier work.

COROLLARY 5.3. *Let $\delta \leq \gamma \leq \alpha < \beta \leq \lambda$ be congruences of a finite algebra $\mathbf{A}$ and assume that $\langle \alpha, \beta \rangle$ is tame. Then* $\operatorname{typ}(\alpha, \beta) = \operatorname{typ}(\alpha/\delta, \beta/\delta)$ *(computed in* $\mathbf{A}/\delta$*) and* $\operatorname{typ}\{\gamma, \lambda\} = \operatorname{typ}\{\gamma/\delta, \lambda/\delta\}$.

PROOF. This is an easy consequence of Lemma 2.18, Definition 4.21, Theorem 4.23, and Definition 5.1. □

Remark 5.4. The structure of an $\langle \alpha, \beta \rangle$-minimal set, when $\langle \alpha, \beta \rangle$ is tame of type **5** in $\mathbf{A}$, is largely defined in Lemma 4.15. When the type is **3** or **4**, Lemma 4.17 defines the situation. When the type is **2**, Lemma 4.20 applies, and Lemmas 4.24–4.27, 4.30, 4.31, 4.34, and 4.36 provide supplementary information for this case. We shall make frequent use of these Lemmas. Notice that when $\operatorname{typ}(\alpha, \beta) = \mathbf{3}$ or **4**, all the $\langle \alpha, \beta \rangle$-traces are two-element sets (by Lemma 4.17). When $\operatorname{typ}(\alpha, \beta) = \mathbf{2}$, the induced algebras on the traces are Mal'cev (by Lemma 4.20).

The first substantial theorem of this chapter characterizes tame quotients of affine type. It was first proved by the authors, but the argument used here is due to P.P. Pálfy.

THEOREM 5.5. *A tame quotient has affine type if and only if it is Abelian and not strongly Abelian.*

PROOF. Let $\langle \alpha, \beta \rangle$ be a tame quotient in a finite algebra $\mathbf{A}$. If $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{3}, \mathbf{4}, \mathbf{5}\}$ then, choosing any pair of elements u and v in an $\langle \alpha, \beta \rangle$-trace N, such that $\langle u, v \rangle \in \beta - \alpha$, it follows from Lemma 4.15 or Lemma 4.17 that $\mathbf{A}|_{\{u,v\}}$ is a non-Abelian algebra. (In fact, $\mathbf{A}$ has a binary polynomial f such that $f(u, u) = u = f(u, v)$ and $f(v, u) = u$, while $f(v, v) = v$, or the same equations with u and v interchanged.)

If $\operatorname{typ}(\alpha, \beta) = \mathbf{2}$, then $\langle \alpha, \beta \rangle$ cannot be strongly Abelian because for every $\langle \alpha, \beta \rangle$-trace N, the algebra $\mathbf{A}|_N$ is Mal'cev. (See Definition 3.9 and Lemma 4.20.)

In the next theorem, we will prove that $\langle \alpha, \beta \rangle$ is strongly Abelian if $\operatorname{typ}(\alpha, \beta) = \mathbf{1}$. Assuming this fact, it follows that if $\langle \alpha, \beta \rangle$ is Abelian and not strongly Abelian, then $\operatorname{typ}(\alpha, \beta) = \mathbf{2}$ (as all other possibilities are ruled out). To prove Theorem 5.5, all we have to do is prove that $\operatorname{typ}(\alpha, \beta) = \mathbf{2}$ implies $\langle \alpha, \beta \rangle$ is Abelian. Since both properties are invariant under factoring out α, we can assume that $\alpha = 0_A$. (See Proposition 3.7 and Corollary 5.3.)

Now assume that $\langle 0_A, \beta \rangle$ is tame in $\mathbf{A}$ of affine type, i.e., $\operatorname{typ}(0_A, \beta) = \mathbf{2}$. It must be shown that β is an Abelian congruence, i.e., $C(\beta, \beta; 0_A)$ holds (in the notation of Definition 3.3). Letting $f \in \operatorname{Pol}_{n+1}\mathbf{A}$ for some n, and $\langle c_1, d_1 \rangle, \ldots, \langle c_n, d_n \rangle \in \beta$, our task is to prove that for all $\langle a, b \rangle \in \beta$, if $f(a, c_1, \ldots, c_n) = f(a, d_1, \ldots, d_n)$ then $f(b, c_1, \ldots, c_n) = f(b, d_1, \ldots, d_n)$ (or more briefly, $f(a, \bar{c}) = f(a, \bar{d}) \to f(b, \bar{c}) = f(b, \bar{d})$). Note that if the implication $f(b_0, \bar{c}) = f(b_0, \bar{d}) \to f(b_1, \bar{c}) = f(b_1, \bar{d})$ holds

whenever $\{b_0, b_1\}$ is contained in a $\langle 0_A, \beta\rangle$-trace, then it must hold whenever $\langle b_0, b_1\rangle \in \beta$. (See Lemma 2.17 and the remarks proceeding it.)

Thus, we can assume that N is a $\langle 0_U, \beta|_U\rangle$-trace for a certain $U \in \mathrm{M}_{\mathbf{A}}(0_A, \beta)$, that $\{a, b\} \subseteq N$, and that $f(a, \bar{c}) = f(a, \bar{d})$ while $f(b, \bar{c}) \neq f(b, \bar{d})$. We shall derive a contradiction from these assumptions, and that will finish the proof.

By Theorem 2.8 (4), there exists $h \in \mathrm{Pol}_1\mathbf{A}$ such that $h(A) = U$ and $h(f(b, \bar{c})) \neq h(f(b, \bar{d}))$. Replacing f by $h \circ f$, we now have that $f(A^{n+1}) \subseteq U$ and the other assumptions are unaltered. The elements $f(a, \bar{c})$, $f(b, \bar{c})$, $f(b, \bar{d})$ all belong to a $\langle 0_U, \beta|_U\rangle$-trace N'. Note that Lemma 4.20 applies to the algebra $\mathbf{A}|_U$ relative to $\langle \delta, \theta\rangle = \langle 0_U, \beta|_U\rangle$. By 4.20 (5), there is a unary polynomial g of $\mathbf{A}$ such that $g(U) \subseteq U$ (i.e., $g|_U \in \mathrm{Pol}_1\mathbf{A}|_U$) and g maps N' bijectively onto N. Replacing f by $g \circ f$, we now have that

$$\{a, b, f(a, \bar{c}), f(b, \bar{c}), f(b, \bar{d})\} \subseteq N$$

and the other assumptions are unaltered. Pálfy's argument begins at this point.

We define $T_i = c_i/\beta$ $(1 \leq i \leq n)$, and observe that

$$f(N \times T_1 \times \cdots \times T_n) \subseteq U \cap f(a, \bar{c})/\beta = N.$$

Using Lemma 2.17 again, we choose, for each $i \in \{1, \ldots, n\}$ a sequence $N(i, 0), \ldots, N(i, k_i)$ of $\langle 0_A, \beta\rangle$-traces such that

$$c_i \in N(i, 0) \text{ and } d_i \in N(i, k_i), \quad \text{and } N(i, j) \cap N(i, j+1) \neq \emptyset \tag{5.5.1}$$

for all $j < k_i$. Obviously, we can arrange that all of the k_i have the same value k. Notice that $\bigcup\{N(i, j) : j \leq k\} \subseteq T_i$ for each i.

We choose, by Corollary 5.2 (2), for each i and j a function α_{ij} in $\mathrm{Pol}_1\mathbf{A}$ such that

$$\alpha_{ij}(N) = N(i, j) \quad \text{and} \quad \alpha_{ij}|_N \text{ is one-to-one}. \tag{5.5.2}$$

We now define some polynomials of the algebra $\mathbf{A}|_N$ by setting

$$f_j(x, x_1, \ldots, x_n) = f(x, \alpha_{1j}(x_1), \ldots, \alpha_{nj}(x_n)) \quad \text{for} \quad 0 \leq j \leq k\,. \tag{5.5.3}$$

Notice that for $j \leq k$ and $x, x_1, \ldots, x_n \in N$, we have $\alpha_{ij}(x_i) \in N_{ij} \subseteq T_i$ for all i, and hence $f_j(x, x_1, \ldots, x_n) \in N$. Each operation $f_j|_N$ is therefore a polynomial operation of $\mathbf{A}|_N$.

The algebra $\mathbf{A}|_N = (\mathbf{A}|_U)|_N$ is a minimal algebra of type **2**; it is polynomially equivalent to a vector space over a finite field $\mathbf{F}$. Thus there exist elements $e_0, \ldots, e_k \in N$, and elements $\mu_{ij} \in F$ $(i \leq n,\ j \leq k)$ such that, expressed in terms of the vector space operations of $\mathbf{A}|_N$, we have

$$\begin{aligned} &\text{for} \quad 0 \leq j \leq k \quad \text{and for all} \quad x_0, x_1, \ldots, x_n \in N, \\ &\qquad f_j(x_0, x_1, \ldots, x_n) = \mu_{0j} \cdot x_0 + \cdots + \mu_{nj} \cdot x_n + e_j\,. \end{aligned} \tag{5.5.4}$$

Claim. For all $j < k$, $\mu_{0j} = \mu_{0\,j+1}$.

To prove this claim, choose elements $u_1, v_1, \ldots, u_n, v_n$ in N such that $\alpha_{ij}(u_i) = \alpha_{i\,j+1}(v_i)$ for $1 \leq i \leq n$ (which can be done, by (5.5.1) and (5.5.2)). For all $x \in N$, we have

$$f_j(x, u_1, \ldots, u_n) = f_{j+1}(x, v_1, \ldots, v_n)$$

by (5.5.3), and so

$$\mu_{0j} \cdot x + \mu_{1j} \cdot u_1 + \cdots + \mu_{nj} \cdot u_n + e_j = \mu_{0\,j+1} \cdot x + \mu_{1\,j+1} \cdot v_1 + \cdot + \mu_{n\,j+1} \cdot v_n + e_{j+1}$$

by (5.5.4). Thus $(\mu_{0j} - \mu_{0\,j+1}) \cdot x$ is constant, independent of $x \in N$, implying that $\mu_{0j} = \mu_{0\,j+1}$, as claimed.

We can now bring this proof to a conclusion. Let $\mu = \mu_{00} = \mu_{0k}$. Choose, by (5.5.1) and (5.5.2), elements $c_1', d_1', \ldots, c_n', d_n'$ in N such that $\alpha_{i0}(c_i') = c_i$ and $\alpha_{ik}(d_i') = d_i$ for $1 \leq i \leq n$. By (5.5.3), $f_0(a, c_1', \ldots, c_n') = f(a, \bar{c}) = f(a, \bar{d}) = f_k(a, d_1', \ldots, d_n')$. Written another way,

$$\mu \cdot a + \mu_{10} \cdot c_1' + \cdots + \mu_{n0} \cdot c_n' + e_0 = \mu \cdot a + \mu_{1k} \cdot d_1' + \cdots + \mu_{nk} \cdot d_n' + e_k \ .$$

Obviously, this equation must remain valid when we replace a by b. But that means that $f(b, \bar{c}) = f(b, \bar{d})$. This contradicts our starting assumption, and ends the proof of this theorem. □

THEOREM 5.6. *A tame quotient has unary type if and only if it is strongly Abelian.*

PROOF. In the first two paragraphs of the preceding proof, we noted that $\langle \alpha, \beta \rangle$ tame and strongly Abelian implies $\mathrm{typ}(\alpha, \beta) = \mathbf{1}$. We shall now prove the converse. As in the last proof, it suffices to derive the result in the case $\alpha = 0_A$. We now assume that $\langle 0_A, \beta \rangle$ is tame in $\mathbf{A}$, of unary type.

Claim 1. If N, N_0, N_1 are $\langle 0_A, \beta \rangle$-traces and $f \in \mathrm{Pol}_2\mathbf{A}$ and $f(N_0 \times N_1) \subseteq N$, then $f|_{N_0 \times N_1}$ depends on at most one variable.

To prove it, suppose, to the contrary, that for some $x_0, x_1, u \in N_0$ and $y_0, y_1, v \in N_1$ we have $f(x_0, v) \neq f(x_1, v)$ and $f(u, y_0) \neq f(u, y_1)$. Then by Exercise 2.19 (6), we have that $\alpha_i : N_i \simeq N$ $(i = 0, 1)$, where $\alpha_0(x) = f(x, v)$ and $\alpha_1(x) = f(u, x)$. There are unary polynomials β_i such that $\alpha_i\beta_i|_N = \mathrm{id}_N$ and $\beta_i\alpha_i|_{N_i} = \mathrm{id}_{N_i}$ $(i = 0, 1)$. The polynomial $h(x, y) = f(\beta_0(x), \beta_1(y))$, restricted to N, is a polynomial of $\mathbf{A}|_N$. Since $\mathbf{A}|_N$ is a minimal algebra and $\mathrm{typ}(\mathbf{A}|_N) = \mathrm{typ}(0_A, \beta) = \mathbf{1}$, the operation $h|_N$ can depend on only one variable. But, clearly, like $f|_{N_0 \times N_1}$ it depends on both, so we have a contradiction, establishing the claim.

Claim 2. If N is a $\langle 0_A, \beta \rangle$-trace, T_0 and T_1 are β-equivalence classes, $f \in \mathrm{Pol}_2\mathbf{A}$, and $f(T_0 \times T_1) \subseteq N$, then $f|_{T_0 \times T_1}$ depends on at most one variable.

To prove it, suppose, to the contrary, that for some $u \in T_0$ and $v \in T_1$, the functions $\alpha_0(x) = f(x,v)$ and $\alpha_1(x) = f(u,x)$ are non-constant on T_0 and on T_1, respectively. By an obvious application of Lemma 2.17, there must exist $\langle 0_A, \beta\rangle$-traces $N_i \subseteq T_i$ such that $\alpha_i|_{N_i}$ is non-constant ($i = 0,1$). We claim that for any $v' \in T_1$, $f(x,v') = \alpha_0(x)$ on N_0. Use Lemma 2.17 to get $\langle 0_A, \beta\rangle$-traces $M_0, \ldots, M_k$ such that $v \in M_0$, $v' \in M_k$ and $M_i \cap M_{i+1} \neq \emptyset$ for all $i < k$. Let $v_1 \in M_0 \cap M_1$. By Claim 1, $\alpha_0(x) = f(x,v) = f(x,v_1)$ for $x \in N_0$. An easy induction along these lines yields $f(x,v') = \alpha_0(x)$.

A similar argument implies that for any $u' \in T_0$, $f(u',y) = \alpha_1(y)$ for all y in N_1. But now if $\langle x,y\rangle \in N_0 \times N_1$, then

$$\alpha_0(x) = f(x,y) = \alpha_1(y);$$

and so $\alpha_0|_{N_0}$ is constant, a contradiction.

Claim 3. If N is an $\langle 0_A, \beta\rangle$-trace, $f \in \mathrm{Pol}_n\mathbf{A}$ (for any integer n), $T = T_0 \times \cdots \times T_{n-1}$ where $T_0, \ldots, T_{n-1}$ are β-equivalence classes, and $f(T) \subseteq N$, then $f|_T$ depends on at most one variable.

This claim reduces to Claim 2 through obvious applications of Lemma 4.1. If $f|_T$ depends on two or more variables, then at most $n-2$ applications of the lemma will produce a binary polynomial f' (which is f with constants substituted for $n-2$ of its variables) that contradicts Claim 2.

We can now finish the proof of this theorem. By Definitions 3.9 and 3.10, our task is to prove the following. Letting $f \in \mathrm{Pol}_n\mathbf{A}$ (for any n) and $c_0, d_0, c_1, d_1, e_1, \ldots, c_{n-1}, d_{n-1}, e_{n-1} \in A$, and *assuming* that $c_0 \equiv d_0 \pmod\beta$ and $c_i \equiv d_i \equiv e_i \pmod\beta$ for $1 \leq i < n$, and that

$$f(c_0, \bar{e}) = f(c_0, e_1, \ldots, e_{n-1}) \neq f(d_0, e_1, \ldots, e_{n-1}) = f(d_0, \bar{e}),$$

then we must have that

$$f(\bar{c}) = f(c_0, \ldots, c_{n-1}) \neq f(d_0, \ldots, d_{n-1}) = f(\bar{d})\,.$$

To prove this (under the stated assumptions), let $T_i = c_i/\beta$ (for $0 \leq i < n$). Notice that $f(c_0,\bar{e}) \equiv f(d_0,\bar{e}) \pmod\beta$. We apply Theorem 2.8(4) and obtain a set $U \in \mathrm{M}_{\mathbf{A}}(0_A, \beta)$ and a polynomial $h \in \mathrm{Pol}_1\mathbf{A}$ such that $h(A) = U$ and $hf(c_0,\bar{e}) \neq hf(d_0,\bar{e})$. Let N be the $\langle 0_U, \beta|_U\rangle$-trace containing $hf(c_0,\bar{e})$. Let $f'(x_0, \ldots, x_{n-1}) = hf(x_0, \ldots, x_{n-1})$, and observe that, since $f'(A^n) \subseteq U$ and $f'(c_0,\bar{e}) \in N$, we have $f'(T_0 \times \cdots \times T_{n-1}) \subseteq N$.

By Claim 3, $f'|_{T_0 \times \cdots \times T_{n-1}}$ depends on at most one variable. Since $f'(c_0,\bar{e}) \neq f'(d_0,\bar{e})$, it must depend on the first variable, and no other. Therefore $f'(\bar{c}) = f'(c_0,\bar{e})$

and $f'(\bar{d}) = f'(d_0, \bar{e})$, implying that $f'(\bar{c}) \neq f'(\bar{d})$; a fortiori, $f(\bar{c}) \neq f(\bar{d})$, as desired. This ends the proof that β is strongly Abelian. □

The two theorems above generalize Lemma 4.14 and Exercise 4.19 (3) (which treated the special case where $A \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$). These results can be neatly reformulated as a local reduction principle for the Abelian property—a tame quotient $\langle \alpha, \beta \rangle$ is Abelian (or strongly Abelian) iff the corresponding minimal algebras, obtained by factoring the trace algebras, are Abelian (or strongly Abelian). We shall see a similar principle later in this chapter, concerning prime quotients of lattice or semilattice type, which involves an orderability property in place of the Abelian properties.

The **Abelian types** are **1** and **2**; the **non-Abelian types** are **3**, **4** and **5**. The next theorem summarizes what we have learned thus far about the types, and contains a new result that has some interesting corollaries. After looking at these corollaries, we shall begin a study of the non-Abelian types. Recall that a quotient $\langle \alpha, \beta \rangle$ is called *prime* iff $\alpha \prec \beta$, i.e., β covers α.

THEOREM 5.7. *Let* $\mathbf{A}$ *be a finite algebra.*

(1) *Every prime congruence quotient of* $\mathbf{A}$ *is tame.*

(2) *For any quotient* $\langle \alpha, \beta \rangle$ *of* $\mathbf{A}$*, the following are equivalent:*
   (i) $\langle \alpha, \beta \rangle$ *is prime and non-Abelian.*
   (ii) $\langle \alpha, \beta \rangle$ *is tame and* $\mathrm{typ}(\alpha, \beta) \in \{\mathbf{3}, \mathbf{4}, \mathbf{5}\}$.

(3) *A tame quotient* $\langle \alpha, \beta \rangle$ *has type* **1** *iff it is strongly Abelian, and has type* **2** *iff it is Abelian but not strongly Abelian.*

(4) *For any quotient* $\langle \alpha, \beta \rangle$ *of* $\mathbf{A}$ *that is not strongly Abelian, the following are equivalent:*
   (i) $\langle \alpha, \beta \rangle$ *is tame.*
   (ii) *The interval lattice* $I[\alpha, \beta]$ *is tight.*
   (iii) $I[\alpha, \beta]$ *is* $0,1$*-simple and complemented.*
   (iv) $I[\alpha, \beta]$ *admits a* $0,1$*–separating homomorphism onto the congruence lattice of a vector space. (This homomorphism is essentially unique.)*

PROOF. Statement (1) follows from Theorem 2.11 and Definition 1.6. Any two-element lattice is tight.

Statement (3) reiterates Theorems 5.5 and 5.6. The implication "(i) implies (ii)" in statement (2) follows from this and from (1). The implication "(ii) implies (i)" in statement (2) is proved in this way. Let $\langle \alpha, \beta \rangle$ be tame and of non-Abelian type, i.e., **3**, **4** or **5**. Let $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. The $\langle \alpha|_U, \beta|_U \rangle$-minimal algebra $\mathbf{A}|_U$ of type **3**, **4** or **5** has, by examination of Lemma 4.15 or 4.17, the property that $\alpha|_U \prec \beta|_U$ in the congruence lattice $\mathbf{Con}\ \mathbf{A}|_U$. By Definition 2.6 and Theorem 2.8 (2), the restriction map $|_U$ is a 0,1–separating lattice homomorphism of $I[\alpha, \beta]$ onto the interval $I[\alpha|_U, \beta|_U]$ in $\mathbf{Con}\ \mathbf{A}|_U$. Only a two-element lattice can have a 0,1–separating homomorphism

onto a two-element lattice. Therefore $\alpha \prec \beta$ in **Con A**. We know that $\langle \alpha, \beta \rangle$ is non-Abelian, from (3).

To prove (4), observe that if $\alpha \prec \beta$ then statements (ii), (iii) and (iv) are trivially true (take a vector space of dimension 1 over a two-element field to prove (iv)) and (i) is true by (1). Thus, we assume that $|I[\alpha, \beta]| \geq 3$. Now (iv) implies (iii) by Exercises 1.14 (1, 3); and (iii) implies (ii) by Example 1.11. By Theorem 2.11, we have that (ii) implies (i).

To show (i) implies (iv), let us now assume that $\langle \alpha, \beta \rangle$ is not strongly Abelian (and is not prime) and that (i) holds. Thus $\mathrm{typ}(\alpha, \beta) = \mathbf{2}$; the other possibilities are ruled out by (2) and (3). We choose $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, and we put $\mathbf{C} = \mathbf{A}|_U$ and $\langle \delta, \theta \rangle = \langle \alpha|_U, \beta|_U \rangle$. Thus $\mathbf{C}$ is minimal of type **2** relative to $\langle \delta, \theta \rangle$. Let N be any $\langle \delta, \theta \rangle$-trace (i.e., a $\langle \alpha|_U, \beta|_U \rangle$-trace). By Lemma 4.24, $I[\delta, \theta]$ is isomorphic to the congruence lattice of the vector space $(\mathbf{C}|_N)/(\delta|_N) = (\mathbf{A}|_N)/(\alpha|_N)$. By Theorem 2.8 (2), the restriction $|_U$ is a 0,1–separating homomorphism of $I[\alpha, \beta]$ onto $I[\delta, \theta]$. This completes the proof that 4(i) implies 4(iv) when $\langle \alpha, \beta \rangle$ is not strongly Abelian. The essential uniqueness comes from Lemma 1.10 (2). □

Here is a very easy and noteworthy corollary of Theorem 5.7.

COROLLARY 5.8. *Let* **A** *be any finite algebra having at least three congruences. If* **Con A** *is a tight lattice, then* **A** *is Abelian. If* **Con A** *is tight, and does not admit a* 0, 1*-separating homomorphism onto the congruence lattice of a vector space, then* **A** *is strongly Abelian.*

Remark 5.9. The simplest lattices for which Corollary 5.8 is interesting are the height two lattices $\mathbf{M}_n$ ($n \geq 3$) with n atoms, pictured in Figure 1. $\mathbf{M}_n$ is tight, and has a 0, 1–separating homomorphism "onto a vector space" iff $n - 1$ is a power of a prime.

Here is another, not so immediate, corollary of Theorem 5.7. The result is obtained by applying Corollary 5.8 to a finitely generated free algebra of a locally finite variety, augmented by a substitution operation. We omit the proof, since it would take us somewhat out of our way to develop the required concepts at this point. The proof can be found in [22].

COROLLARY 5.10. *If* $\mathcal{V}$ *is a locally finite variety that possesses more than two subvarieties, its lattice of subvarieties is not a finite tight lattice.*

Exercises 5.11

(1) Let $\langle \alpha, \beta \rangle$ be a tame quotient in a finite algebra **A**. Prove that the following are equivalent.

(i) $\langle \alpha, \beta \rangle$ is Abelian.

(ii) For each β-equivalence class T, the algebra $(\mathbf{A}|_T)/(\alpha|_T)$ is Abelian.

(iii) For each two-element set $\{u, v\} \subseteq A$ with $\langle u, v \rangle \in \beta - \alpha$, the algebra $\mathbf{A}|_{\{u,v\}}$ is Abelian.

(iv) There does not exist a pair $\langle u, v \rangle \in \beta - \alpha$ and a binary polynomial f of $\mathbf{A}$ such that $\{u, v\}$ is closed under f and $\langle \{u, v\}, f \rangle$ is a semilattice.

(Sufficient hints for the solution of this exercise can be found in the proof of Theorem 5.5.)

(2) Let $\langle \alpha, \beta \rangle$ be a tame quotient in a finite algebra $\mathbf{A}$. Prove that the following are equivalent.

(i) $\langle \alpha, \beta \rangle$ is strongly Abelian.

(ii) $(\mathbf{A}|_T)/(\alpha|_T)$ is a strongly Abelian algebra, for each β-equivalence class T.

(iii) There do not exist a pair $\langle u, v \rangle \in \beta - \alpha$ and a binary polynomial f of $\mathbf{A}$ satisfying $f(u, v) = f(v, u) = u$ and $f(v, v) = v$.

(iv) For every $f \in \mathrm{Pol}_n \mathbf{A}$ (for any n), and for every set $T = T_0 \times \cdots \times T_{n-1}$, where $T_0, \ldots, T_{n-1}$ are β-equivalence classes, if $f(T)$ is contained in a single $\langle \alpha, \beta \rangle$-trace then $f|_T$ depends, modulo α, on at most one variable.

(See the proof of Theorem 5.6. For the equivalence of (i) and (iii), notice that if a trace algebra $\mathbf{A}|_N$ has a Mal'cev polynomial $d(x, y, z)$ and if $u, v \in N$, then the polynomial $f(x, y) = d(x, v, y)$ satisfies $f(u, v) = f(v, u) = u$ and $f(v, v) = v$.)

(3) Let $\langle \alpha, \beta \rangle$ be a tame quotient in a finite algebra $\mathbf{A}$ with $\mathrm{typ}(\alpha, \beta) \neq \mathbf{1}$. Prove a version of Theorem 2.8 for the traces, modified as follows: Replace $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ by $\{N : N \text{ is an } \langle \alpha, \beta \rangle\text{-trace}\}$. In (2), delete the existence of e. In (4), replace "$f(A) = U$" by "$f(x/\beta) = N$". Change (5) to read: For each N, β is the transitive closure of $\alpha \cup \bigcup \{(g(N))^2 : g \in \mathrm{Pol}_1 \mathbf{A}\}$.

(4) Using the result of the last exercise, show that *if* $\langle \alpha, \beta \rangle$ is tame, of non-unary type, and $T = x/\beta \neq x/\alpha$, *then* $\langle \alpha|_T, 1_T \rangle$ is tame in $\mathbf{A}|_T$, $\mathrm{typ}(\alpha|_T, 1|_T) = \mathrm{typ}(\alpha, \beta)$, and the $\langle \alpha|_T, 1_T \rangle$-minimal sets are precisely the $\langle \alpha, \beta \rangle$-traces contained in T.

(5) Show that when $\langle \alpha, \beta \rangle$ is tame in $\mathbf{A}$ and $\mathrm{typ}(\alpha, \beta) \neq \mathbf{2}$, then $\mathrm{typ}\{\alpha, \beta\} = \{\mathrm{typ}(\alpha, \beta)\}$. (See Definition 5.1 for the notation. This result is trivial unless $\mathrm{typ}(\alpha, \beta) = \mathbf{1}$; but in this case, the result of Exercise 2 above does the trick.) Stronger: if $\alpha \leq \gamma < \lambda \leq \beta$ and $\langle \alpha, \beta \rangle$, $\langle \gamma, \lambda \rangle$ are tame, then $\mathrm{typ}(\alpha, \beta) = \mathrm{typ}(\gamma, \lambda)$ unless $\mathrm{typ}(\alpha, \beta) = \mathbf{2}$.

Exercises 2.19 (1–2) may be useful for (5), and also for the next exercise.

(6) Suppose that $\alpha \leq \gamma < \lambda \leq \beta$, that $\langle \alpha, \beta \rangle$ and $\langle \gamma, \lambda \rangle$ are tame in $\mathbf{A}$, and that $\mathrm{typ}(\alpha, \beta) = \mathbf{2}$. Prove that $\langle \gamma, \lambda \rangle$ is Abelian; and that $\mathrm{typ}(\gamma, \lambda) = \mathbf{2}$ if, for an $\langle \alpha, \beta \rangle$-trace N, we have $\gamma|_N < \lambda|_N$. In particular, $\mathrm{typ}(\gamma, \lambda) = \mathbf{2}$ if $\gamma = \alpha$ or if $\lambda = \beta$.

(7) This exercise complements the last two by constructing a ten-element tame algebra of type **2** that has a tame quotient of type **1**. We take $A = \{0, 1, \ldots, 9\}$ and put $U_0 = \{0, 1, 2, 3\}$, $U_1 = \{3, 4, 5, 6\}$, $U_2 = \{6, 7, 8, 9\}$. These sets will be the $\langle 0_A, 1_A \rangle$-minimal sets of our algebra. We define two equivalence relations, γ with equivalence classes $\{0, 3, 6, 9\}$, $\{1, 2\}$, $\{4, 5\}$, $\{7, 8\}$, and λ with equivalence classes $\{0, 3, 6, 9\}$, $\{1, 2, 7, 8\}$, $\{4, 5\}$.

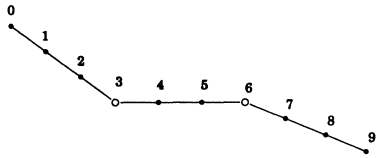


Figure 11

We define F to be the set of all functions f from A to A such that $f = \mathrm{id}$; or f is constant; or $f(A) = U_i$ for some $i \in \{0, 1, 2\}$, $f^2 = f$, and f is one-to-one or constant on each U_j and f preserves γ and λ. If we think of A as a ruler in three rigid segments with hinges at corners 3 and 6 (see Figure 11), then we can find three members of F which consist in "folding" all segments onto one segment without violating the physical integrity of the ruler. Call these functions e_0, e_1, e_2 (with $e_i(A) = U_i$). There are two other obvious members of F, e_0' which maps 4, 5, 6 to 3, maps 7 to 2, 8 to 1, and 9 to 0, and leaves U_0 pointwise fixed; and e_2' which projects A onto U_2 in a similar fashion. Define a 3-ary operation $d_0(x, y, z)$ on U_0 by the rules: $d_0(x_0, x_1, x_2) = x_i$ if $\{i, j, k\} = \{0, 1, 2\}$ and $x_j = x_k$; $d_0(x_0, x_1, x_2) =$ "the fourth element of U_0 if x_0, x_1, x_2 are distinct ". Note that U_0 is the universe of a four-element vector space over the two-element field, in which $d_0(x, y, z) = x + y + z$. Define $d(x, y, z)$ on A so that $d(x, y, z) = d_0(e_0(x), e_0(y), e_0(z))$. Define $\mathbf{A} = \langle A, d, e_0, e_1, e_2, e_0', e_2' \rangle$. Now prove that $\langle 0_A, 1_A \rangle$ and $\langle \gamma, \lambda \rangle$ are tame quotients of $\mathbf{A}$, and that $\mathrm{typ}(0_A, 1_A) = \mathbf{2}$ while $\mathrm{typ}(\gamma, \lambda) = \mathbf{1}$.

(8) Let $0 \prec \beta$ in $\mathbf{A}$ with $\mathrm{typ}(0, \beta) = \mathbf{2}$. Using Lemma 4.27, Corollary 4.34, and Lemma 4.36, show that if $U \in \mathrm{M}_{\mathbf{A}}(0, \beta)$ and B is the body of U then $C(\Theta(B^2), \beta; 0)$—i.e., the congruence generated by collapsing B centralizes β.

The next two lemmas reveal interesting and useful properties of non-Abelian prime quotients. In the first lemma we do not require that the algebra be finite.

LEMMA 5.12. *Let $\langle \alpha, \beta \rangle$ be a non-Abelian prime quotient of an algebra* $\mathbf{A}$. *There exists a (unique) congruence δ such that for all congruences μ of A, $\mu \wedge \beta = \alpha$ iff $\alpha \leq \mu \leq \delta$.*

PROOF. We can prove this using not much more than the definition of an Abelian quotient (Definitions 3.3 and 3.6). Suppose that the conclusion stated in this lemma fails. Then $\delta = \bigvee\{\mu : \mu \wedge \beta = \alpha\}$ satisfies $\delta \wedge \beta \neq \alpha$. Obviously $\delta \geq \alpha$, and $\delta \wedge \beta \in I[\alpha, \beta]$, and so $\delta \wedge \beta = \beta$ since $\alpha \prec \beta$. Thus we have that $\beta \leq \delta$. Now by Proposition 3.4 (4), we have $C(\mu, \beta; \alpha)$ holding whenever $\mu \wedge \beta = \alpha$. Thus, by 3.4 (2), we have $C(\delta, \beta; \alpha)$. Since $\beta \leq \delta$, it follows by 3.4 (1) that $C(\beta, \beta; \alpha)$, i.e., that $\langle \alpha, \beta \rangle$ is Abelian. □

Remark 5.13. The largest congruence δ such that $\delta \wedge \beta = \alpha$ is called the **pseudo-complement of β over α**. This is a purely lattice-theoretic concept. Such pseudo-complements need not exist, in general. It is easily seen that when $\langle \alpha, \beta \rangle$ is prime and non-Abelian, the pseudo-complement of β over α is identical to $\mathrm{ann}(\alpha \mid \beta)$, defined in Exercise 3.8 (2).

Remark 5.14. Let $\mathbf{A}$ be finite and $\langle \alpha, \beta \rangle$ be a non-Abelian prime quotient of $\mathbf{A}$. Let δ be the pseudo-complement of β over α. Choose U in $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and let $1 \in U$ be the isolated element of the $\langle \alpha|_U, \beta|_U \rangle$-trace, as defined by Lemma 4.15 or 4.17 (whichever applies). Thus $1/(\alpha|_U) = \{1\}$. Clearly, $\mathbf{A}|_U$ possesses a largest congruence λ such that $1/\lambda = \{1\}$; and we have $\alpha|_U \leq \lambda$. Since $|_U$ is a lattice homomorphism, $\mathbf{A}$ has a largest congruence λ' satisfying $\lambda'|_U = \lambda$. It can easily be shown, using the information in Lemma 4.15 or Lemma 4.17, that λ' is identical with δ, the pseudo-complement of β over α.

LEMMA 5.15. *Let $\langle \alpha, \beta \rangle$ be a non-Abelian prime quotient of a finite algebra* $\mathbf{A}$, *and let $\gamma \in \mathrm{Con}\,\mathbf{A}$.*

(1) *If $\alpha \vee \gamma = \beta$, then there exists a smallest congruence δ such that $\delta \geq \alpha \wedge \gamma$ and $\alpha \vee \delta = \beta$.*
(2) *If $\langle \alpha, \beta \rangle$ is of Boolean or lattice type, then there exists a smallest congruence δ such that $\alpha \vee \delta = \beta$.*

PROOF. Choose any $\langle \alpha, \beta \rangle$-trace N. According to Lemma 4.15 or Lemma 4.17, we have $N = I \cup O$ (disjoint union) where $I = \{1\}$ and $\alpha|_N = I^2 \cup O^2$. By Lemma 2.4, the map $|_N$ is a lattice homomorphism on $I[0, \beta]$. Hence, since $\alpha \prec \beta$, the condition $\alpha \vee \delta = \beta$ is equivalent to $\delta \leq \beta$ and $\delta \cap (I \times O) \neq \emptyset$. Now if the type of $\langle \alpha, \beta \rangle$ is **3** or **4**, then Lemma 4.17 tells us that $O = \{0\}$ (for some element 0) and thus $\alpha \vee \delta = \beta$ is equivalent to $\langle 0, 1 \rangle \in \delta \leq \beta$. Thus in this case, $\Theta(0, 1)$ is the smallest congruence that joins with α to give β. This proves (2).

To prove (1), assume that $\alpha \vee \gamma = \beta$. Choosing $\langle 1, u\rangle \in \gamma \cap (I \times O)$, we put $\delta = (\alpha \wedge \gamma) \vee \Theta(1, u)$. Now let $\lambda \geq \alpha \wedge \gamma$ and $\alpha \vee \lambda = \beta$. Notice that from our definition of δ we have $\alpha \wedge \gamma = \alpha \wedge \delta$, and so $\alpha \wedge \delta \leq \lambda$. Choose $\langle 1, v\rangle \in \lambda \cap (I \times O)$. Let p be the pseudo-meet operation on N supplied by Lemma 4.15 or 4.17. Since $p(u, 1) = u$ and $p(1, v) = v$, we have $u \overset{\lambda}{\equiv} p(u, v) \overset{\delta}{\equiv} v$. Since $p(u, v) \in O$, we actually have $p(u, v) \overset{\alpha\wedge\delta}{\equiv} v$. Since $\alpha \wedge \delta \leq \lambda$, then $\langle u, v\rangle \in \lambda \vee (\alpha \wedge \delta) = \lambda$ and $\langle u, 1\rangle \in \lambda$; and so $\lambda \geq (\alpha \wedge \gamma) \vee \Theta(u, 1) = \delta$. This finishes the proof of (1). □

Remark 5.16. The smallest congruence δ such that $\delta \vee \alpha = \beta$, when it exists, is called the **pseudo complement of α under β**.

Every finite simple algebra is tame, and its type is the same as that of its unique prime congruence quotient (see Definition 5.1 (3)). Here is our first result on finite simple algebras. We shall study them at length in Chapter 14.

COROLLARY 5.17. *Let $\mathbf{A}, \mathbf{B}_1, \ldots, \mathbf{B}_n$ be finite algebras such that $\mathbf{A}$ is simple and of Boolean or lattice type. If $\mathbf{A}$ belongs to the variety generated by $\{\mathbf{B}_1, \ldots, \mathbf{B}_n\}$, then $\mathbf{A}$ is a homomorphic image of a subalgebra of one of the $\mathbf{B}_i$.*

PROOF. Let $\mathbf{A}$ belong to the variety generated by $\mathbf{B}_1, \ldots, \mathbf{B}_n$. By Theorem 0.2, $\mathbf{A}$ must be a homomorphic image of a subalgebra of $(\mathbf{B}_1 \times \cdots \times \mathbf{B}_n)^k$ for a finite integer k. Therefore, for some m, we have an algebra $\mathbf{S} \subseteq \prod_{j=1}^{m} \mathbf{C}_j$ where $\{\mathbf{C}_1, \ldots, \mathbf{C}_m\} \subseteq \{\mathbf{B}_1, \ldots, \mathbf{B}_n\}$, and a congruence α of $\mathbf{S}$ with $\mathbf{S}/\alpha \cong \mathbf{A}$. Since $\mathbf{A}$ is simple, $\alpha \prec 1_S$ in $\mathbf{Con}\ \mathbf{S}$, and we must have $\mathrm{typ}(\alpha, 1_S) = \mathrm{typ}(0_A, 1_A) = \mathrm{typ}(\mathbf{A})$ (by Corollary 5.3). Let δ be the pseudo-complement of α under 1_S, which exists by Lemma 5.15. For $1 \leq j \leq m$, let η_j be the kernel of the projection of $\mathbf{S}$ into $\mathbf{C}_j$. Since $\delta \not\leq \alpha$, and $\bigwedge\{\eta_j : j = 1, \ldots, m\} = 0_S$, then for some j we have $\delta \not\leq \eta_j$. By the definition of δ, it follows that $\eta_j \vee \alpha \neq 1_S$, implying that $\eta_j \leq \alpha$ since $\alpha \prec 1_S$. Let i be such that $\mathbf{C}_j = \mathbf{B}_i$. Then $\mathbf{S}/\alpha$ ($\cong \mathbf{A}$) is a homomorphic image of $\mathbf{S}/\eta_j$, which is isomorphic to a subalgebra of $\mathbf{B}_i$. This concludes our proof. □

DEFINITION 5.18. A lattice $\mathbf{L}$ is said to be **meet semi-distributive**, or to satisfy SD($\wedge$), iff whenever elements x, y, z in $\mathbf{L}$ satisfy $x \wedge y = x \wedge z$, they also satisfy $x \wedge y = x \wedge (y \vee z)$. The property SD($\vee$), **join semi-distributivity**, is the dual of SD($\wedge$). The conjunction of these two properties, denoted SD, is called **semi-distributivity.**

LEMMA 5.19. *Let θ, ψ_0, ψ_1 be congruences of a finite algebra $\mathbf{A}$.*

(1) *If $\theta \wedge \psi_0 = \theta \wedge \psi_1 = \alpha$, and if β is a congruence such that $\alpha \prec \beta \leq \theta \wedge (\psi_0 \vee \psi_1)$, then $\mathrm{typ}(\alpha, \beta) \in \{\mathbf{1}, \mathbf{2}\}$.*

(2) *If $\theta \vee \psi_0 = \theta \vee \psi_1 = \beta$, and if α is a congruence such that $\theta \vee (\psi_0 \wedge \psi_1) \leq \alpha \prec \beta$, then $\mathrm{typ}(\alpha, \beta) \in \{\mathbf{1}, \mathbf{2}, \mathbf{5}\}$.*

PROOF. Under the hypotheses of statement (1), $\beta \wedge \psi_0 = \beta \wedge \psi_1 = \alpha$, and $\beta \leq \psi_0 \vee \psi_1$. Thus the pseudo-complement of β over α does not exist. By Lemma 5.12, it follows that $\langle \alpha, \beta \rangle$ is Abelian. This proves (1).

The proof of (2) is similar, using Lemma 5.15. □

COROLLARY 5.20. *Suppose that α and β are congruences of a finite algebra $\mathbf{A}$ such that $\alpha < \beta$ and $\mathrm{typ}\{\alpha, \beta\} \subseteq \{\mathbf{3}, \mathbf{4}, \mathbf{5}\}$. Then the interval lattice $I[\alpha, \beta]$ satisfies* SD($\wedge$). *If $\mathrm{typ}\{\alpha, \beta\} \subseteq \{\mathbf{3}, \mathbf{4}\}$, then $I[\alpha, \beta]$ satisfies* SD($\vee$).

PROOF. This is an immediate consequence of Lemma 5.19. □

Shortly, we shall prove that the presence of a prime quotient of semilattice type in the congruence lattice of an algebra $\mathbf{A}$ forces a failure of join semi-distributivity in the congruence lattice of a certain subalgebra of $\mathbf{A}^2$. Similar results concerning prime quotients of unary or affine type will be proved in Chapter 6. These results, in combination with Corollary 5.20, will show that when we consider in place of a finite algebra $\mathbf{A}$ the class of all subalgebras of finite direct powers of $\mathbf{A}$, then congruence meet semi-distributivity is equivalent to the absence of Abelian prime quotients in all algebras of the class, while congruence join semi-distributivity is equivalent to the absence of Abelian prime quotients as well as those of semilattice type.

Remark 5.21. The smallest lattices satisfying one, but not both, semi-distributivity conditions are pictured below.

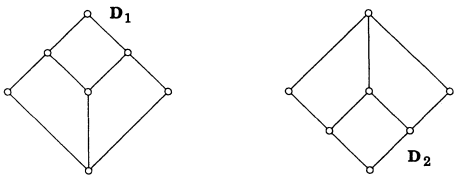


Figure 12

The lattice $\mathbf{D}_1$ fails SD($\wedge$), and $\mathbf{D}_2$, its dual, fails SD($\vee$). These lattices have an interesting role in our classification scheme for locally finite varieties (presented in Chapter 9), along with the smallest non-modular lattice, $\mathbf{N}_5$, and the smallest modular, non-distributive lattice, $\mathbf{M}_3$. We remark that $\mathbf{D}_2$ is isomorphic to the congruence lattice of $\mathbf{S}^2$, where $\mathbf{S}$ is a two-element semilattice. $\mathbf{D}_1$ is isomorphic to the lattice of convex subsets of a three-element linearly ordered set.

To conclude this chapter, we shall find characterizations of each of the three non-Abelian types of prime quotients, in language that does not involve tame congruence theory.

Recall from Chapter 0 that an *admissible n-ary relation* on an algebra $\mathbf{A}$ is a subset of A^n closed under the operations of $\mathbf{A}^n$. A *tolerance* of $\mathbf{A}$ is a binary relation over A that is admissible, reflexive and symmetric. Note that an admissible n-ary relation ρ on $\mathbf{A}$ is closed under all polynomial operations of $\mathbf{A}$ (acting coordinatewise in A^n) iff it contains the diagonal of $\mathbf{A}^n$, i.e., $\langle x, \dots, x\rangle \in \rho$ for all $x \in A$. (If ρ is binary, this means that ρ is reflexive.)

LEMMA 5.22. *If an algebra $\mathbf{A}$ has a Mal'cev polynomial, then every admissible binary relation of $\mathbf{A}$, reflexive over $\mathbf{A}$, is a congruence relation.*

PROOF. Let ρ be admissible and reflexive. Let $q(x, y, z)$ be a Mal'cev polynomial operation of $\mathbf{A}$ (Definition 4.5). Since ρ is reflexive, it is closed under q. Suppose that $\langle x, y\rangle$, $\langle y, z\rangle \in \rho$. Then $q(\langle x, x\rangle,\ \langle x, y\rangle,\ \langle y, y\rangle) = \langle q(x, x, y), q(x, y, y)\rangle = \langle y, x\rangle$ belongs to ρ. (In this calculation, we are using the operation on A^2 which is q acting at each coordinate.) Similarly, $q(\langle x, y\rangle, \langle y, y\rangle, \langle y, z\rangle) = \langle x, z\rangle$ belongs to ρ. Thus ρ is reflexive, symmetric, and transitive, which makes it a congruence relation. □

We recall some more definitions from Chapter 0. The converse of a binary relation ρ is the relation $\rho^{\cup} = \{\langle x, y\rangle : \langle y, x\rangle \in \rho\}$ (read "ρ converse"). The relation product of binary relations ρ and σ is the relation $\rho \circ \sigma = \{\langle x, z\rangle : \langle x, y\rangle \in \rho$ and $\langle y, z\rangle \in \sigma$ for some $y\}$. When σ is an equivalence relation, we say that ρ is **σ-closed** iff $\rho = \sigma \circ \rho \circ \sigma$; the **$\sigma$-closure** of ρ is the relation $\sigma \circ \rho \circ \sigma$.

DEFINITION 5.23. If $\langle \alpha, \beta\rangle$ is a prime quotient of a finite algebra $\mathbf{A}$, then by the **basic tolerance for** $\langle \alpha, \beta\rangle$ we mean the intersection of all α-closed tolerances τ of $\mathbf{A}$ satisfying $\alpha \neq \tau \subseteq \beta$.

LEMMA 5.24. *Let $\langle \alpha, \beta\rangle$ be a prime quotient of a finite algebra $\mathbf{A}$ with $\operatorname{typ}(\alpha, \beta) \neq \mathbf{1}$, and let ρ be the basic tolerance for $\langle \alpha, \beta\rangle$.*

(1) *If N is an $\langle \alpha, \beta\rangle$-trace and $\langle x, y\rangle \in N^2 - \alpha$, then ρ is the smallest α-closed tolerance containing $\langle x, y\rangle$. The transitive closure of ρ is β.*

(2) *If $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{2}, \mathbf{3}\}$, then ρ is the α-closure of $\alpha \cup \bigcup\{N^2 : N$ is an $\langle \alpha, \beta\rangle$-trace$\}$; and ρ is the smallest α-closed admissible reflexive relation τ satisfying $\alpha \neq \tau \subseteq \beta$.*

(3) *If $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{4}, \mathbf{5}\}$, then there are precisely two minimal α-closed, admissible, reflexive relations τ such that $\alpha \neq \tau \subseteq \beta$. These relations, ρ_0 and ρ_1, satisfy:*

   (i) *$\rho_0 = \rho_1^{\cup}$ and $\rho_0 \cap \rho_1 = \alpha$;*

   (ii) *$\rho_0 \cup \rho_1$ is the α-closure of $\alpha \cup \bigcup\{N^2 : N$ is an $\langle \alpha, \beta\rangle$-trace$\}$;*

   (iii) *ρ is the α-closure of the admissible relation generated by $\rho_0 \cup \rho_1$.*

PROOF. Our proof begins with a claim.

Claim 1. let τ be an α-closed admissible reflexive relation on $\mathbf{A}$ with $\alpha \neq \tau \subseteq \beta$, and let N be any $\langle \alpha, \beta \rangle$-trace. Then $N^2 \subseteq \tau \cup \tau^{\cup}$, and $\alpha \subseteq \tau$. If $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{2}, \mathbf{3}\}$, then $N^2 \subseteq \tau$.

To begin the proof of this claim, we note that every α-closed reflexive relation trivially contains α. Now choosing any $\langle a, b \rangle \in \tau - \alpha$, an easy application of Theorem 2.8 (4) and Corollary 5.2 (2) yields the existence of a unary polynomial $f(x)$ with $\langle f(a), f(b) \rangle \in N^2 - \alpha$; therefore $\tau|_N \not\subseteq \alpha|_N$. Since τ is reflexive, it is preserved by all of the polynomial operations of $\mathbf{A}$; and so $\tau|_N$ is an admissible, reflexive, $\alpha|_N$-closed relation of the algebra $\mathbf{A}|_N$.

If $\operatorname{typ}(\alpha, \beta) = \mathbf{2}$, then $\mathbf{A}|_N$ is Mal'cev (by Lemma 4.20); and if $\operatorname{typ}(\alpha, \beta) = \mathbf{3}$, then $\mathbf{A}|_N$ is polynomially equivalent to a two-element Boolean algebra (by Lemma 4.17), and again is Mal'cev. Hence if $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{2}, \mathbf{3}\}$ then it follows from Lemma 5.22 that $\tau|_N$ is a congruence of $\mathbf{A}|_N$. Now since $\alpha \prec \beta$ and $|_N$ is a homomorphism of $I[\alpha, \beta]$ onto $I[\alpha|_N, \beta|_N]$, we have $\alpha|_N \prec \beta|_N = 1_N$ in $\operatorname{Con} \mathbf{A}|_N$. Consequently, if $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{2}, \mathbf{3}\}$, then $\tau|_N$ can only be identical with 1_N; and so $\tau \supseteq N^2$ in this case. If $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{4}, \mathbf{5}\}$ then Lemma 4.15 or 4.17 implies that N is the union of $c/(\alpha|_N)$ and $d/(\alpha|_N)$, for any $\langle c, d \rangle \in 1_N - \alpha|_N$; so it is obvious in this case that $\tau \cup \tau^{\cup} \supseteq N^2$, since τ is α-closed and $\tau|_N \not\subseteq \alpha|_N$.

Claim 2. If $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{2}, \mathbf{3}\}$, then the α-closure of $\alpha \cup \bigcup \{N^2 : N \text{ is an } \langle \alpha, \beta \rangle\text{-trace}\}$ is a tolerance.

To prove this claim, let τ denote this relation which we wish to prove is a tolerance. Then τ is obviously symmetric and reflexive. To prove that it is admissible, let f be any n-ary polynomial of $\mathbf{A}$ and let $\langle u_i, v_i \rangle \in \tau$ for $0 \leq i < n$. In showing that $\langle f(\bar{u}), f(\bar{v}) \rangle \in \tau$, we can assume that for a certain $k \leq n$ we have $\langle u_i, v_i \rangle \in \alpha$ for $k \leq i < n$, and for each $i < k$ we have a trace N_i and elements $c_i, d_i \in N_i$ such that $\langle u_i, c_i \rangle \in \alpha$, $\langle v_i, d_i \rangle \in \alpha$, and $\langle c_i, d_i \rangle \notin \alpha$. Since τ is α-closed, it suffices to prove that $\langle f(c_0, \ldots, c_{k-1}, u_k, \ldots, u_{n-1}), f(d_0, \ldots, d_{k-1}, u_k, \ldots, u_{n-1}) \rangle$ belongs to τ. Thus, changing notation, we can assume that $k = n$ and that $\langle u_i, v_i \rangle \in N_i^2 - \alpha$ for $0 \leq i < n$.

Since we've assumed that $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{2}, \mathbf{3}\}$, by Corollary 5.2 (2) there exist unary polynomials $f_i(x)$ and elements $u_i', v_j' \in N_0$ such that $\langle u_i', v_i' \rangle \in N_0^2 - \alpha$ and $f_i(u_i') = u_i$, $f_i(v_i') = v_i$ for $0 \leq i < n$. Replacing f by the polynomial f' defined by $f'(x_0, \ldots, x_{n-1}) = f(f_0(x_0), \ldots, f_{n-1}(x_{n-1}))$ and writing N for N_0, and changing notation once again, we can now assume that $u_i, v_i \in N$ for all i. The argument breaks into two cases.

Case 1: Let $\operatorname{typ}(\alpha, \beta) = \mathbf{2}$. Thus $(\mathbf{A}|_N)/(\alpha|_N)$ is a vector space of dimension 1. (Since $\alpha \prec \beta$, as before we have $\alpha|_N \prec 1_N$, so the vector space is a simple

algebra.) Because u_0/α, v_0/α are unequal elements of this vector space, there exists, for all i, $1 \leq i < n$, a vector space polynomial h_i such that $h_i(u_0/\alpha) = u_i/\alpha$ and $h_i(v_0/\alpha) = v_i/\alpha$. Therefore there exist polynomials h_i' of $\mathbf{A}$ such that $h_i'(u_0) \equiv u_i \pmod{\alpha}$ and $h_i'(v_0) \equiv v_i \pmod{\alpha}$. We define $h(x) = f(x, h_1'(x), \ldots, h_{n-1}'(x))$, and observe that $f(\bar{u}) \equiv h(u_0) \pmod{\alpha}$ and $f(\bar{v}) \equiv h(v_0) \pmod{\alpha}$. Therefore, we are reduced to proving that $\langle h(u_0), h(v_0)\rangle \in \tau$. This follows from the result of Exercise 2.19 (6).

Case 2: Let $\operatorname{typ}(\alpha, \beta) = \mathbf{3}$. Thus, by Lemma 4.17, $N = \{u_0, v_0\}$, and $\mathbf{A}$ has a polynomial h' such that $h'(u_0) = v_0$ and $h'(v_0) = u_0$. The argument used for Case 1 works equally well in this case.

The proof of Claim 2 is finished. Assertions (1) and (2) of this lemma are easy consequences of Claim 1 and Claim 2. For (1), note that by Claim 1, every α-closed tolerance τ such that $\alpha \neq \tau \subseteq \beta$ must contain $\alpha \cup N^2$ for all traces N (since τ is symmetric). Thus ρ (the basic tolerance) must contain $\alpha \cup N^2$ for all traces N. Now if N is a trace and $\langle x, y\rangle \in N^2 - \alpha$, then taking τ to be the α-closure of the tolerance generated by $\langle x, y\rangle$, we have that $\tau \subseteq \rho$ by the last sentence, but also $\rho \subseteq \tau$ by the definition of ρ; consequently $\rho = \tau$. That β equals the transitive closure of ρ is a consequence of Lemma 2.17. This finishes the proof of (1). The proof of (2) is somewhat easier, and we omit it.

Claim 3. The admissible reflexive relation generated by a pair $\langle a, b\rangle \in A^2$ is

$$r(a, b) = \{\langle f(a), f(b)\rangle : \ f \in \operatorname{Pol}_1 \mathbf{A}\};$$

and the tolerance generated by $\langle a, b\rangle$ is

$$t(a, b) = \{\langle f(a, b), f(b, a)\rangle : \ f \in \operatorname{Pol}_2 \mathbf{A}\} .$$

The proof of this claim is a simple matter of showing that these relations are admissible; that $r(a, b)$ is reflexive and contains $\langle a, b\rangle$; that every admissible reflexive relation containing $\langle a, b\rangle$ contains $r(a, b)$ as a subset; and similar facts for $t(a, b)$. The proofs are left to the reader.

We now assume that $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{4}, \mathbf{5}\}$, in order to prove assertion (3) of this lemma. We choose a trace N, and choose $\langle a, b\rangle \in N^2 - \alpha$. We define ρ_0 and ρ_1 to be the α-closures of $r(a, b)$ and $r(b, a)$ respectively. By Claim 1, every α-closed, admissible, reflexive relation τ such that $\alpha \neq \tau \subseteq \beta$ contains either ρ_0 or ρ_1 (i.e., contains $\langle a, b\rangle$ or $\langle b, a\rangle$). Clearly $\alpha \neq \rho_i \subseteq \beta$ $(i = 0, 1)$. We now will show that $\rho_0 \cap \rho_1 = \alpha$, from which it should be clear that ρ_0 and ρ_1 are the unique minimal members of the family of relations under consideration. Suppose that there is a pair $\langle c, d\rangle \in \rho_0 \cap \rho_1$, $\langle c, d\rangle \notin \alpha$. By Exercise 5.11 (3), we can choose $h \in \operatorname{Pol}_1 \mathbf{A}$ with $\langle h(c), h(d)\rangle \in N^2 - \alpha$ and $h(c/\beta) = N$. By Claim 3, there are $f_0, f_1 \in \operatorname{Pol}_1 \mathbf{A}$ with

$f_0(a) \equiv c \equiv f_1(b) \pmod{\alpha}$ and $f_0(b) \equiv d \equiv f_1(a) \pmod{\alpha}$. Now N is the disjoint union of $a/(\alpha|_N)$ and $b/(\alpha|_N)$. If $h(c)$ is in the first class and $h(d)$ in the second, then $q = hf_1$ satisfies $q(a) \equiv b$, $q(b) \equiv a \pmod{\alpha}$. If the order of $h(c)$ and $h(d)$ is reversed, then $q = hf_0$ satisfies the same congruences. Choosing an $\langle \alpha, \beta \rangle$-minimal set U such that N is a trace in U, and an $e \in \mathrm{E}(\mathbf{A})$ with $e(A) = U$, it follows from $\langle q(a), q(b) \rangle \in N^2 - \alpha$ that N is closed under eq and $eq|_N$ is a permutation which exchanges the two $\alpha|_N$-classes. This contradicts the fact that $(\mathbf{A}|_N)/(\alpha|_N)$ is polynomially equivalent to a lattice or semilattice. The contradiction finishes our proof that $\rho_0 \cap \rho_1 = \alpha$. It follows easily from our definition of ρ_0 and ρ_1 that $(\rho_1)^\cup = \rho_0$.

To prove 3(ii), recall that by Claim 1, $\rho_0 \cup \rho_1$ $(= \rho_0 \cup \rho_0^\cup)$ contains $\alpha \cup \{N^2 : N \text{ a trace}\}$. On the other hand, by Claim 3 and Exercise 2.19 (6),

$$r(a,b) \cup r(b,a) \subseteq \alpha \cup \bigcup \{N^2 : N \text{ a trace}\} .$$

These facts easily yield 3(ii).

To prove 3(iii), notice that $\rho_0 \cup \rho_1$ is symmetric and reflexive. Therefore the α-closure of the admissible relation it generates is a tolerance. Thus, by definition of ρ, we have that this tolerance includes ρ. On the other hand, by (1), ρ is the α-closure of $t(a,b)$; and therefore ρ contains ρ_0 and ρ_1, by their definitions. □

DEFINITION 5.25. Let $\langle \alpha, \beta \rangle$ be any congruence quotient of an algebra $\mathbf{A}$. By an $\langle \alpha, \beta \rangle$-**pre-order** we mean an admissible binary relation τ of $\mathbf{A}$ such that τ is a pre-ordering of $\mathbf{A}$ (i.e., it is reflexive and transitive over $\mathbf{A}$), $\alpha = \tau \cap \tau^\cup$, and the transitive closure of $\tau \cup \tau^\cup$ is β. We say that $\langle \alpha, \beta \rangle$ is **orderable** iff there exists an $\langle \alpha, \beta \rangle$-pre-order.

THEOREM 5.26. *Let $\langle \alpha, \beta \rangle$ be a tame quotient of a finite algebra $\mathbf{A}$, with* $\mathrm{typ}(\alpha, \beta) \neq \mathbf{1}$.

(1) *$\langle \alpha, \beta \rangle$ is orderable iff* $\mathrm{typ}(\alpha, \beta) \in \{\mathbf{4}, \mathbf{5}\}$.

(2) *Assume that* $\mathrm{typ}(\alpha, \beta) \in \{\mathbf{4}, \mathbf{5}\}$. *There exist precisely two minimal $\langle \alpha, \beta \rangle$-pre-orders, ζ_0 and ζ_1, and two maximal $\langle \alpha, \beta \rangle$-pre-orders, ξ_0 and ξ_1, such that every $\langle \alpha, \beta \rangle$-pre-order τ satisfies $\zeta_0 \subseteq \tau \subseteq \xi_0$ or $\zeta_1 \subseteq \tau \subseteq \xi_1$. We have $\zeta_1 = \zeta_0^\cup$, $\xi_1 = \xi_0^\cup$, and ζ_0 and ζ_1 are the transitive closures of the relations ρ_0 and ρ_1 of Lemma 5.24 (3).*

PROOF. We begin by assuming that $\mathrm{typ}(\alpha, \beta) = \mathbf{2}$ or $\mathbf{3}$ and there exists an $\langle \alpha, \beta \rangle$-pre-order τ, and derive a contradiction from these assumptions. It is easily seen that $\tau \neq \alpha$. Since $\tau \circ \tau = \tau \supseteq \alpha$, τ is α-closed. By Lemma 5.24 (2), $\tau \supseteq N^2$ for every trace N. This contradicts the condition that $\tau \cap \tau^\cup = \alpha$.

We now assume that $\mathrm{typ}(\alpha, \beta) = \mathbf{4}$ or $\mathbf{5}$. Letting ρ_0 and ρ_1 be the two minimal, α-closed, admissible, reflexive relations (see Lemma 5.24 (3)), we define ζ_i to be the

transitive closure of ρ_i $(i = 0, 1)$. We choose an $\langle \alpha, \beta \rangle$-trace N and an element 1 in N. If $\mathrm{typ}(\alpha, \beta) = \mathbf{5}$, then we arrange that $\{1\} = 1/(\alpha|_N)$ is the neutral element of the semilattice $(\mathbf{A}|_N)/(\alpha|_N)$ (using Lemma 4.15). Thus $\{1\} = 1/(\alpha|_N)$ whether the type is **4** or **5**. We choose any $b \in N - \{1\}$. Thus we have $\langle 1, b \rangle \in N^2 - \alpha$, and $N = \{1\} \cup b/(\alpha|_N)$. By Lemma 5.24 (3), the pair $\langle b, 1 \rangle$ belongs to precisely one of ρ_0 and ρ_1; we shall assume that $\langle b, 1 \rangle \in \rho_0$.

Since $\rho_1 = \rho_0^{\cup}$, we have $\zeta_1 = \zeta_0^{\cup}$. The relations ζ_0 and ζ_1 are pre-orders, by their construction. It is easily seen that the transitive closure of any admissible reflexive relation is admissible. The relations ζ_0 and ζ_1 are therefore admissible pre-orders. Obviously, $\zeta_0 \cup \zeta_1 \subseteq \beta$.

We now define

$$\xi_0 = \{\langle x, y \rangle \in \beta : \text{ for all } f \in \mathrm{Pol}_1\mathbf{A} \text{ such that } f(x/\beta) \subseteq N \text{ and } f(x) = 1, \text{ we have } f(y) = 1\}$$

and we define $\xi_1 = \xi_0^{\cup}$. We proceed to prove several claims.

Claim 1. $\zeta_i \subseteq \xi_i \subseteq \beta$ and ξ_i is an admissible pre-order (for $i = 0, 1$).

It suffices to prove this claim for $i = 0$. Since it is obvious that ξ_0 is a pre-order, our first task will be to show that it is admissible. By Exercise 5.28 (2), this amounts to showing that ξ_0 is closed under the unary polynomials of $\mathbf{A}$. So let $h \in \mathrm{Pol}_1\mathbf{A}$ and $\langle u, v \rangle \in \xi_0$. To see that $\langle h(u), h(v) \rangle \in \xi_0$, let $f \in \mathrm{Pol}_1\mathbf{A}$ be such that $f(h(u)/\beta) \subseteq N$ and $f(h(u)) = 1$. Then $fh(u/\beta) \subseteq N$ and $fh(u) = 1$, so $fh(v) = 1$. We conclude that $\langle h(u), h(v) \rangle \in \xi_0$, and that ξ_0 is admissible.

Because ξ_0 is a pre-order, to show that $\zeta_0 \subseteq \xi_0$, we need only show that $\rho_0 \subseteq \xi_0$. To do this, let $\langle u, v \rangle \in \rho_0$ and $f \in \mathrm{Pol}_1\mathbf{A}$ with $f(u/\beta) \subseteq N$ and $f(u) = 1$. Thus $\langle 1, f(v) \rangle \in \rho_0 \cap N^2$. If $f(v) \neq 1$, then $f(v) \in b/(\alpha|_N)$, and since ρ_0 is α-closed, we have $\langle 1, b \rangle \in \rho_0$ as well as $\langle b, 1 \rangle \in \rho_0$; but this contradicts Lemma 5.24 (3(i)). Therefore $f(v) = 1$, and we conclude that $\langle u, v \rangle \in \xi_0$, and consequently that $\zeta_0 \subseteq \xi_0$. This finishes our proof of Claim 1.

Claim 2. $\xi_0 \cap \xi_1 = \alpha$ and the transitive closure of $\zeta_0 \cup \zeta_1$ is β. Therefore ζ_i, ξ_i are $\langle \alpha, \beta \rangle$-pre-orders $(i = 0, 1)$.

The second sentence in this claim follows from the first, from Claim 1, from the definition of $\langle \alpha, \beta \rangle$-pre-order, and from the facts that $\zeta_0 \cap \zeta_1 \supseteq \rho_0 \cap \rho_1 = \alpha$ and $\xi_0 \cup \xi_1 \subseteq \beta$. That the transitive closure of $\zeta_0 \cup \zeta_1$ equals β is a consequence of Lemma 5.24 (3(ii)) and Lemma 2.17.

Let us prove that $\xi_0 \cap \xi_1 = \alpha$. Suppose that $\langle u, v \rangle \in \xi_0 \cap \xi_1$. Then for every $f \in \mathrm{Pol}_1\mathbf{A}$ satisfying $f(u/\beta) \subseteq N$ we have $f(u) = 1 \leftrightarrow f(v) = 1$, and therefore $\langle f(u), f(v) \rangle \in \alpha$ since $(N - \{1\})^2 \subseteq \alpha$. Using Exercise 5.11 (3), we conclude that $\langle u, v \rangle \in \alpha$.

Claim 3. If τ is any $\langle\alpha,\beta\rangle$-pre-order, then $\zeta_0 \subseteq \tau \subseteq \xi_0$ or $\zeta_0 \subseteq \tau^{\cup} \subseteq \xi_0$.

Let τ be an $\langle\alpha,\beta\rangle$-pre-order. We recall from early in the proof that this implies $\alpha \neq \tau$, and that τ is α-closed. By Lemma 5.24 (3) we have $\rho_i \subseteq \tau$ for some $i \in \{0,1\}$, giving that $\rho_0 \subseteq \tau$ or $\rho_0 \subseteq \tau^{\cup}$. We may as well assume that $\rho_0 \subseteq \tau$. Thus, obviously, $\zeta_0 \subseteq \tau$. Finally, since τ is an α-closed subset of β, the assumption $\tau \not\subseteq \xi_0$ would imply directly that $\langle 1,b\rangle \in \tau$. (Use the definition of ξ_0.) This, in turn, would put $\langle 1,b\rangle \in (\tau \cap \tau^{\cup}) - \alpha$, contradicting that τ is an $\langle\alpha,\beta\rangle$-pre-order. Therefore $\tau \subseteq \xi_0$. This finishes the proof of Claim 3.

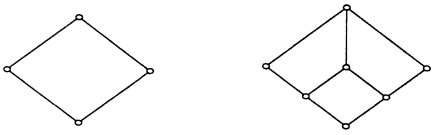
The minimality of ζ_i and maximality of ξ_i follows from Claim 3 and the obvious fact that any $\langle\alpha,\beta\rangle$-pre-order must be incomparable to its converse. □

We have characterized the unary type of tame quotient as strongly Abelian, the affine type as Abelian but not strongly Abelian, and the Boolean type (in Theorem 5.26) as non-Abelian and non-orderable. The next theorem exhibits a subtle difference between prime quotients of Boolean or lattice type, and those of semilattice type.

THEOREM 5.27. *Let $\langle\alpha,\beta\rangle$ be a non-Abelian prime quotient of a finite algebra $\mathbf{A}$. Let ρ be the basic tolerance for $\langle\alpha,\beta\rangle$, $\mathbf{R}$ be the subalgebra of $\mathbf{A}^2$ with universe $R = \rho$, and $\mathbf{L}$ be the interval sublattice $I[(\alpha \times \alpha)|_R\ ,\ (\beta \times \beta)|_R]$ in $\mathbf{Con}\ \mathbf{R}$.*

(1) *If* $\mathrm{typ}(\alpha,\beta) \in \{3,4\}$ *then* $\mathbf{L} \cong \mathbf{M}_2$.

(2) *If* $\mathrm{typ}(\alpha,\beta) = 5$ *then* $\mathbf{L} \cong \mathbf{D}_2$.



PROOF. Let $\pi : \mathbf{A}^2 \twoheadrightarrow (\mathbf{A}/\alpha)^2$ be the natural mapping. From the characterization of R $(= \rho)$ as the least α-closed tolerance τ such that $\alpha \neq \tau \subseteq \beta$, it is easy to prove that $\pi(R)$ is the basic tolerance for the quotient $\langle\alpha/\alpha,\beta/\alpha\rangle$ in $\mathbf{A}/\alpha$. The kernel of $\pi|_R$ is $(\alpha \times \alpha)|_R$; and we have $(\beta \times \beta)|_R = \pi^{-1}([(\beta/\alpha) \times (\beta/\alpha)]|_{\pi(R)})$. Therefore, the lattice $\mathbf{L}$ is isomorphic to the lattice derived in the same way from the quotient $\langle\alpha/\alpha,\beta/\alpha\rangle$ which, as we know, has the same type as $\langle\alpha,\beta\rangle$. These considerations show that it suffices to prove the theorem under the assumption $\alpha = 0_A$.

So let $\langle 0_A,\beta\rangle$ be a prime non-Abelian quotient of $\mathbf{A}$. Choose $U_0 \in \mathrm{M}_{\mathbf{A}}(0_A,\beta)$ and a binary polynomial $p(x,y)$ of $\mathbf{A}$ such that p is a pseudo-meet operation for $\mathbf{A}|_{U_0}$ relative to $\langle 0_{U_0},\beta|_{U_0}\rangle$. (See Definitions 4.16 and 4.18.) Let $N_0 = \{0,1\}$ be the unique trace in U_0, with 1 the neutral element for p.

Note that, by Lemma 5.24, R is the tolerance generated by $\langle 0,1\rangle$. By various parts of 5.24 (including "Claim 3" in its proof), we have

(5.27.1) $$N^2 \subseteq R \subseteq \beta \text{ for every } \langle 0_A, \beta\rangle\text{-trace } N; \text{ and}$$
$$R = \{\langle f(0,1), f(1,0)\rangle : \ f \in \mathrm{Pol}_2\mathbf{A}\} .$$

Since $R \supseteq 0_A$, it is easily checked that the polynomials of $\mathbf{R}$ are precisely all the operations of the form

$$f(\langle x_0, y_0\rangle, \ldots, \langle x_{n-1}, y_{n-1}\rangle) = \langle g(0,1,\bar{x}), g(1,0,\bar{y})\rangle$$

with $g \in \mathrm{Pol}_{n+2}\mathbf{A}$ if $f \in \mathrm{Pol}_n\mathbf{R}$. We have, in particular, that every polynomial of $\mathbf{A}$, acting coordinatewise on n-tuples of pairs in R, is a polynomial of $\mathbf{R}$.

Claim. If $\theta \in \mathrm{Con}\,\mathbf{R}$ and $\theta \leq \beta \times \beta$, then θ is generated by $\theta|_{N_0^2}$.

To prove this claim, we let θ be any congruence in the interval $I[0_R, (\beta \times \beta)|_R]$ of $\mathbf{Con}\,\mathbf{R}$, and we set θ_0 equal to the congruence of $\mathbf{R}$ generated by $\theta|_{N_0^2}$. Let $\langle\langle a,b\rangle, \langle c,d\rangle\rangle$ be any element of θ. We wish to show that $\langle\langle a,b\rangle, \langle c,d\rangle\rangle \in \theta_0$. We shall assume that $a \neq c$. (The proof in the case $b \neq d$ is similar, and if $a = c$ and $b = d$, then there is nothing to prove.)

Since $\langle a,c\rangle \in \beta - 0_A$, there is $f \in \mathrm{Pol}_1\mathbf{A}$ with $f(a/\beta) = N_0 = \{0,1\}$, and $f(a) \neq f(c)$. Note that $\{b,c,d\} \subseteq a/\beta$, and therefore

$$\langle\langle f(a), f(b)\rangle, \langle f(c), f(d)\rangle\rangle \in \theta|_{N_0^2} .$$

We form the "meets" of $\langle f(a), f(b)\rangle$ and $\langle f(c), f(d)\rangle$ with the element $\langle 1,0\rangle$ (using the operation p), and obtain that

$$\langle f(a), 0\rangle \equiv \langle f(c), 0\rangle \pmod{\theta} .$$

Since $\{f(a), f(c)\} = \{0,1\}$, we thus have $\langle 0,0\rangle \equiv \langle 1,0\rangle \pmod{\theta_0}$.

Now $\langle a,b\rangle = \langle f_0(0,1), f_0(1,0)\rangle$ and $\langle c,d\rangle = \langle f_1(0,1), f_1(1,0)\rangle$ for some binary polynomials f_0 and f_1 of $\mathbf{A}$; i.e.,

$$\langle a,b\rangle = f_0'(\langle 0,1\rangle, \langle 1,0\rangle) \text{ and } \langle c,d\rangle = f_1'(\langle 0,1\rangle, \langle 1,0\rangle)$$

where $f_0', f_1' \in \mathrm{Pol}_2\mathbf{R}$ are f_0, f_1 acting coordinatewise. Therefore, we have

(5.27.2)
$$\langle a,b\rangle \equiv f_0'(\langle 0,1\rangle, \langle 0,0\rangle) = \langle f_0(0,0), f_0(1,0)\rangle \pmod{\theta_0} ,$$
$$\langle c,d\rangle \equiv f_1'(\langle 0,1\rangle, \langle 0,0\rangle) = \langle f_1(0,0), f_1(1,0)\rangle \pmod{\theta_0} .$$

Case 1: If $b \neq d$, then by the same argument, $\langle 0,0\rangle \equiv \langle 0,1\rangle \pmod{\theta_0}$, and we find

$$\langle a,b\rangle \equiv \langle f_0(0,0), f_0(0,0)\rangle = \langle e_0, e_0\rangle \pmod{\theta_0} ,$$

$$\langle c,d\rangle \equiv \langle f_1(0,0), f_1(0,0)\rangle = \langle e_1, e_1\rangle \pmod{\theta_0}$$

for some e_0 and e_1. Since $0_A \prec \beta$, the restriction of θ to the diagonal subalgebra $0_A = \{\langle x,x\rangle : x \in A\}$ must be either the identity relation on this subset, or $(\beta\times\beta)|_{0_A}$. Thus if $e_0 \neq e_1$, then $\langle e_0, e_0\rangle \equiv \langle e_1, e_1\rangle \pmod{\theta}$ implies that $\langle\langle 0,0\rangle, \langle 1,1\rangle\rangle \in \theta|_{N_0^2} \subseteq \theta_0$. This gives that $\theta_0 \supseteq (\beta \times \beta)|_{0_A}$, and hence $\langle e_0, e_0\rangle \equiv \langle e_1, e_1\rangle \pmod{\theta_0}$. Thus, $e_0 \neq e_1$ implies $\langle a,b\rangle \equiv \langle c,d\rangle \pmod{\theta_0}$ in Case 1, and $e_0 = e_1$ obviously gives the same conclusion.

Case 2: Assume that $b = d$. If $\mathrm{typ}(0_A, \beta) = \mathbf{3}$ or $\mathbf{4}$, then there is also a pseudo-join operation for N_0. Then from $\langle 0,0\rangle \equiv \langle 1,0\rangle \pmod{\theta_0}$ follows $\langle 0,1\rangle \equiv \langle 1,1\rangle \pmod{\theta_0}$ (by taking the join with $\langle 0,1\rangle$). From this, and formulas (5.27.2), we obtain that

$$\langle a,b\rangle \equiv f_0'(\langle 1,1\rangle, \langle 0,0\rangle) = \langle f_0(1,0), f_0(1,0)\rangle \equiv \langle b,b\rangle \pmod{\theta_0}\,;$$

and likewise $\langle c,d\rangle \equiv \langle d,d\rangle \equiv \langle b,b\rangle \pmod{\theta_0}$. Therefore the proof of the claim is finished if $\mathrm{typ}(0_A,\beta) \neq \mathbf{5}$. So we assume now that $\mathrm{typ}(0_A,\beta) = \mathbf{5}$. We can also assume that $f_0(0,0) \neq f_1(0,0)$ (else we are done, by (5.27.2)).

To conclude the proof of the claim, we choose a $g \in \mathrm{Pol}_1\mathbf{A}$ such that $g(b/\beta) \subseteq N_0$ and $gf_0(0,0) \neq gf_1(0,0)$. Without losing generality, we assume that $gf_0(0,0) = 0$, $gf_1(0,0) = 1$. We must have

$$gf_1(1,0)\ (= g(d) = g(b)) = gf_1(0,0)\ (=1)\,,$$

else $gf_1(1;0) = 0$ and there is an obvious polynomial h satisfying $h(0) = 1$, $h(1) = 0$, contradicting that $\mathbf{A}|_{N_0}$ is a semilattice. From all the equalities collected in this paragraph (and $f_0(1,0) = b = f_1(1,0)$ as well), we have that g, acting coordinatewise, transforms the two ordered pairs on the far right of (5.27.2) onto $\langle 0,1\rangle$ and $\langle 1,1\rangle$, respectively. Thus $\langle 0,1\rangle \equiv \langle 1,1\rangle \pmod{\theta_0}$; and it follows that $\langle a,b\rangle \equiv \langle b,b\rangle \equiv \langle c,d\rangle \pmod{\theta_0}$ just as we saw for types **3** and **4** above. This finishes our proof of the claim.

To finish the proof of the theorem, we apply Lemma 2.4. Let $U_0' = U_0^2 \cap R$, and let $e = e^2 \in \mathrm{Pol}_1\mathbf{A}$ with $e(A) = U_0$, and define e' by $e'(\langle x,y\rangle) = \langle e(x), e(y)\rangle$. Thus $e' \in \mathrm{Pol}_1\mathbf{R}$, $(e')^2 = e'$, and $e'(R) = U_0'$. We have that N_0^2 is an equivalence class of $(\beta\times\beta)|_{U_0'} = ((\beta\times\beta)|_R)|_{U_0'}$. Applying Lemma 2.4, we have that

$$|_{N_0^2}\,:\ I[0_R, (\beta\times\beta)|_R] \twoheadrightarrow \mathbf{Con}\,\mathbf{R}|_{N_0^2}\,.$$

The claim proved above implies that this lattice homomorphism is one-to-one. Our lattice $\mathbf{L}$ is therefore isomorphic to $\mathbf{Con}\,\mathbf{R}|_{N_0^2}$.

It follows from our previous description of the polynomials of $\mathbf{R}$, and from the fact that $\mathbf{R}|_{N_0^2} = (\mathbf{R}|_{U_0'})|_{N_0^2}$ (because e' exists), and from our knowledge of U_0 and N_0, that $\mathbf{R}|_{N_0^2}$ is polynomially equivalent to $(\mathbf{A}|_{N_0})^2$. (The proof of this whopper is an exercise.) Assertions (1) and (2) of this theorem can now be validated by computing

the congruence lattices of the direct squares of a two-element Boolean algebra, lattice, and semilattice. □

Exercises 5.28

(1) Prove these additions to Lemma 5.24. If $\text{typ}(\alpha, \beta) = \mathbf{3}$, there exists a smallest admissible, reflexive τ satisfying $\tau \subseteq \beta$, $\tau \not\subseteq \alpha$; and this relation is a tolerance. If $\text{typ}(\alpha, \beta) = \mathbf{4}$, there exist precisely two minimal relations having these properties. (These assertions omit the requirement that τ be α-closed.)

(2) Prove that a pre-order on the universe of an algebra is admissible iff it is closed under unary polynomials.

(3) Prove the unproved assertion in the last paragraph of the proof of Theorem 5.27.

(4) Suppose that $\langle \alpha, \beta \rangle$ is a prime quotient of $\mathbf{A}$ of type $\mathbf{2}$, with basic tolerance R, and that $\mathbf{R} \subseteq \mathbf{A}^2$ is the algebra whose universe is R. Show that the interval $I[(\alpha \times \alpha)|_R\ ,\ (\beta \times \beta)|_R]$ contains a sublattice isomorphic to $\mathbf{M}_3$.

(5) Let α, β, R be as above, except that $\text{typ}(\alpha, \beta) = \mathbf{5}$. Let $\delta_0, \delta_1, \delta_2$ be the three co-atoms of $I[(\alpha \times \alpha)|_R\ ,\ (\beta \times \beta)|_R]$ as pictured in Theorem 5.27. Prove that $\text{typ}(\delta_i, (\beta \times \beta)|_R) = \mathbf{5}$ and that $\mathbf{R}/\delta_i \cong \mathbf{A}/\alpha$, for $i = 0, 1, 2$.

(6) Let $\mathbf{A}$ be an algebra such that $\mathbf{A}|_A$ is Mal'cev. Prove that for any $\alpha, \beta \in \text{Con } \mathbf{A}$, $\alpha \circ \beta = \beta \circ \alpha = \alpha \vee \beta$. ($\mathbf{A}$ has permuting congruences.) From this, derive that $\mathbf{Con\ A}$ is a modular lattice.

6. LABELED CONGRUENCE LATTICES

A finite lattice is completely described by its Hasse diagram, a directed graph whose vertices are the elements of the lattice, and whose edges are the prime quotients. When $\mathbf{L}$ is the congruence lattice of a finite algebra $\mathbf{A}$, the Hasse diagram of $\mathbf{L}$ has a natural labeling, namely, label every edge by its type as a prime congruence quotient of $\mathbf{A}$. This mapping from the set of edges to the set $\{\mathbf{1},\dots,\mathbf{5}\}$ is just the function typ, defined in Definition 5.1; we call it the **type labeling** of $\mathbf{L}$. The type labeling of $\mathbf{L} = \mathbf{Con}\ \mathbf{A}$ is determined by the polynomials of $\mathbf{A}$; in fact, it is determined by $\mathrm{Pol}_2\mathbf{A}$. Notice that if we replace $\mathbf{A}$ by $\langle A, \mathrm{Pol}_1\mathbf{A}\rangle$, then $\mathbf{L}$ remains unchanged and the sets of $\langle\alpha,\beta\rangle$-minimal sets and $\langle\alpha,\beta\rangle$-traces are unchanged, for every prime quotient $\langle\alpha,\beta\rangle$, but the type labeling of $\mathbf{L}$ changes to a trivial labeling using only the type label $\mathbf{1}$.

We recommend trying to visualize the labels as colors, rather than numbers (although officially we shall stick with the numbers). Use the color chart: $\mathbf{1}$ = orange, $\mathbf{2}$ = red, $\mathbf{3}$ = blue, $\mathbf{4}$ = green, $\mathbf{5}$ = yellow. The colored graphs thus obtained from finite algebras have many regularities, following from results proved in this chapter and the next one. Each graph is divided into disjoint regions (convex sublattices) within which only the colors red and orange appear. Edges joining separate regions are colored blue, green or yellow. Moreover, each red-orange region is divided into subregions colored entirely with orange, while edges between adjoining subregions are red. The regions and subregions constitute the blocks of two congruences on the congruence lattice which we shall study in the next chapter: the solvability congruence and the strong solvability congruence. Modulo the solvability congruence, the lattice is meet semi-distributive. Modulo strong solvability, the red-orange regions are modular lattices. An edge $\langle\alpha,\beta\rangle$ between separate red-orange regions must be painted yellow, unless α has a pseudo-complement under β. (This follows from Lemma 5.19.)

Our purpose in this chapter is to collect results relating the omission of type labels to the non-occurence of certain lattices as sublattices of congruence lattices. The results proved here will enable us to make smooth progress in subsequent chapters. This chapter is divided into two parts. In the first, we primarily study the labeled congruence lattice of one algebra, and in the second, we compare the variety generated by a finite algebra to the varieties generated by certain of its induced algebras. Our first result doesn't really belong to either part, but fits here as comfortably as anywhere.

LEMMA 6.1. *Let* $\mathbf{A}$ *be a finite algebra, and let* $\langle \alpha_1, \beta_1 \rangle, \ldots, \langle \alpha_n, \beta_n \rangle$ *be a list of prime quotients of* $\mathbf{A}$ *such that every congruence* Θ *on* $\mathbf{L} = \mathbf{Con}\,\mathbf{A}$, *except* $\Theta = 0_L$, *satisfies* $\langle \alpha_i, \beta_i \rangle \in \Theta$ *for some* $1 \leq i \leq n$. *Choose* $U_i \in \mathrm{M}_{\mathbf{A}}(\alpha_i, \beta_i)$ *for each* i. *The function defined on* $\mathbf{L}$ *by* $f(\delta) = \langle \delta|_{U_i} : 1 \leq i \leq n \rangle$ *is an isomorphism of* $\mathbf{L}$ *with a subdirect product of the* $\mathbf{Con}\,\mathbf{A}|_{U_i}$. *In symbols*

$$f : \mathbf{L} \underset{sd}{\hookrightarrow} \prod \{\mathbf{Con}\,\mathbf{A}|_{U_i} : 1 \leq i \leq n\} .$$

PROOF. By Lemma 2.3 and Theorem 2.8, $|_{U_i}$ is an onto lattice homomorphism for all i, and $\alpha_i|_{U_i} \neq \beta_i|_{U_i}$. Therefore f is a lattice homomorphism, and $(\ker f) \cap \{\langle \alpha_i, \beta_i \rangle : 1 \leq i \leq n\} = \emptyset$. Hence $\ker f = 0_L$, and f is one-to-one. □

LEMMA 6.2. *Let* $\langle \alpha_i, \beta_i \rangle$ $(i = 0, 1)$ *be prime quotients of a finite algebra* $\mathbf{A}$ *such that* $\beta_0 \wedge \alpha_1 = \alpha_0$ *and* $\beta_0 \vee \alpha_1 = \beta_1$. *Then* $\mathrm{M}_{\mathbf{A}}(\alpha_0, \beta_0) = \mathrm{M}_{\mathbf{A}}(\alpha_1, \beta_1)$ *and* $\mathrm{typ}(\alpha_0, \beta_0) = \mathrm{typ}(\alpha_1, \beta_1)$.

PROOF. That $\mathrm{M}_{\mathbf{A}}(\alpha_0, \beta_0) = \mathrm{M}_{\mathbf{A}}(\alpha_1, \beta_1)$ when $\langle \alpha_0, \beta_0 \rangle$ and $\langle \alpha_1, \beta_1 \rangle$ are projective quotients is the result of Exercise 2.19 (3).

To prove the equality of types, let U be an $\langle \alpha_0, \beta_0 \rangle$-minimal set. Suppose first that $\langle \alpha_1, \beta_1 \rangle$ is of non-Abelian type. Let N_1 be the unique $\langle \alpha_1, \beta_1 \rangle$-trace in U. (Note that U is also an $\langle \alpha_1, \beta_1 \rangle$-minimal set.) By Lemma 2.4, $\beta_0|_{N_1} \vee \alpha_1|_{N_1} = \beta_1|_{N_1}$ $(= 1_{N_1})$ and $\beta_0|_{N_1} \wedge \alpha_1|_{N_1} = \alpha_0|_{N_1}$. From these equations and the picture of N_1 supplied by Lemmas 4.15 and 4.17, it follows that N_1 contains precisely one $\langle \alpha_0, \beta_0 \rangle$-trace N_0 of U, and we have this picture of N_1 :

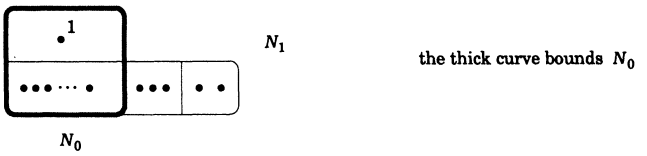


Figure 13

In the picture, $\alpha_0|_{N_0} = \alpha_1|_{N_0}$; $\{1\}$ and $N_1 - \{1\}$ are the two $\alpha_1|_{N_1}$-classes; $\{1\}$ and $N_0 - \{1\}$ are two of the $\alpha_0|_{N_1}$-classes; and $N_1 - N_0$ is partitioned in some way into $\alpha_0|_{N_1}$-classes.

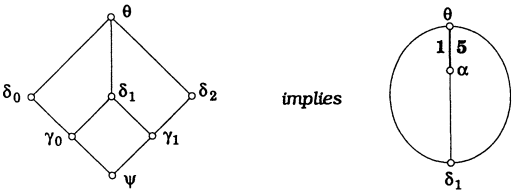
Now for any $a \in N_0 - \{1\}$, a pseudo-meet operation with respect to $\langle \alpha_1, \beta_1 \rangle$, restricted to $\{1, a\}$, is a semilattice operation, showing that $\langle \alpha_0, \beta_0 \rangle$ is non-Abelian. Thus Lemmas 4.15, 4.17 also apply to U with respect to $\langle \alpha_0, \beta_0 \rangle$, and N_0 is the unique $\langle \alpha_0, \beta_0 \rangle$-trace in U. If $\mathrm{typ}(\alpha_1, \beta_1) \neq \mathbf{5}$, then $N_1 = N_0$, a two-element set, and then $\mathrm{typ}(\alpha_0, \beta_0) = \mathrm{typ}(\alpha_1, \beta_1) = \mathrm{typ}(\mathbf{A}|_{N_1})$. If $\mathrm{typ}(\alpha_1, \beta_1) = \mathbf{5}$, then it is very easy

to see that $\mathbf{A}|_{N_0}$ cannot have a pseudo-join operation; hence $\text{typ}(\alpha_0, \beta_0) = \mathbf{5}$ also. This finishes our proof for equality of types in the case that $\langle \alpha_1, \beta_1 \rangle$ is not Abelian.

Let us suppose now that $\langle \alpha_1, \beta_1 \rangle$ is Abelian. By Proposition 3.7 (2), $\langle \alpha_0, \beta_0 \rangle$ is also Abelian. One can easily show, directly from the definition, that if $\langle \alpha_1, \beta_1 \rangle$ is strongly Abelian then $\langle \alpha_0, \beta_0 \rangle = \langle \beta_0 \wedge \alpha_1, \beta_0 \wedge \beta_1 \rangle$ is strongly Abelian. Therefore, the only thing remaining to be proved is that $\text{typ}(\alpha_1, \beta_1) = \mathbf{2}$ implies $\text{typ}(\alpha_0, \beta_0) \neq \mathbf{1}$. Assume that $\text{typ}(\alpha_1, \beta_1) = \mathbf{2}$, and let B_i be the $\langle \alpha_i, \beta_i \rangle$-body of U $(i = 0, 1)$. Let $d(x, y, z)$ be a pseudo-Mal'cev operation for U relative to $\langle \alpha_1, \beta_1 \rangle$ (Lemma 4.20). Then $d|_{B_1}$ is Mal'cev, and obviously $B_0 \subseteq B_1$. For any $\langle \alpha_0, \beta_0 \rangle$-trace $N_0 \subseteq B_0$, N_0 is closed under d since $d(x, x, x) = x$; therefore $(\mathbf{A}|_{N_0})/(\alpha|_{N_0})$ is Mal'cev, and cannot be a minimal algebra of type **1**. □

Exercises 6.23 (1–7) give examples showing that the type labeling need not be so well-behaved with regard to projective quotients of which one is prime and the other is not. It is not true, for instance, that if $\beta_0 \wedge \alpha_1 = \alpha_0$, $\beta_0 \vee \alpha_1 = \beta_1$, and $\alpha_0 \prec \beta_0$, then the equality $\text{typ}\{\alpha_1, \beta_1\} = \{\text{typ}(\alpha_0, \beta_0)\}$ need hold.

LEMMA 6.3. *Suppose that $\delta_0, \delta_1, \delta_2, \gamma_0, \gamma_1, \psi, \theta$ are congruences of a finite algebra $\mathbf{A}$ constituting a sublattice of* $\mathbf{Con}\ \mathbf{A}$ *isomorphic to $\mathbf{D}_2$, as pictured below. If $\delta_1 \leq \alpha \prec \theta$, then* $\text{typ}(\alpha, \theta) \in \{\mathbf{1}, \mathbf{5}\}$.

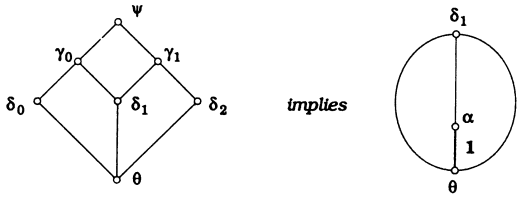


PROOF. Since $\delta_1 \vee \delta_0 = \delta_1 \vee \delta_2 = \theta$ and $\delta_1 \vee (\delta_0 \wedge \delta_2) = \delta_1$, it follows from Lemma 5.19 (2) that $\text{typ}(\alpha, \theta) \in \{\mathbf{1}, \mathbf{2}, \mathbf{5}\}$. Assume that $\text{typ}(\alpha, \theta) = \mathbf{2}$, in order to derive a contradiction. Let N be any $\langle \alpha, \theta \rangle$-trace. By Lemma 2.4, $|_N$ is a homomorphism of $I[0_A, \theta]$ onto $\mathbf{Con}\ \mathbf{A}|_N$; and by Lemma 4.20, $\mathbf{A}|_N$ is a Mal'cev algebra. According to Exercise 5.28 (6), $\mathbf{Con}\ \mathbf{A}|_N$ is a modular lattice. Therefore,

$$\begin{aligned} \delta_2|_N &= (\delta_2 \wedge (\gamma_1 \vee \delta_0))|_N = \delta_2|_N \wedge (\gamma_1|_N \vee \delta_0|_N) \\ &= \gamma_1|_N \vee (\delta_2|_N \wedge \delta_0|_N) = (\gamma_1 \vee (\delta_2 \wedge \delta_0))|_N = \gamma_1|_N \,. \end{aligned}$$

Consequently, $\theta|_N = (\delta_1 \vee \delta_2)|_N = \delta_1|_N \vee \delta_2|_N = \delta_1|_N \vee \gamma_1|_N = \delta_1|_N$. This gives $\alpha|_N = \theta|_N$, since $\delta_1 \leq \alpha \prec \theta$; but that is absurd since N is an $\langle \alpha, \theta \rangle$-trace. □

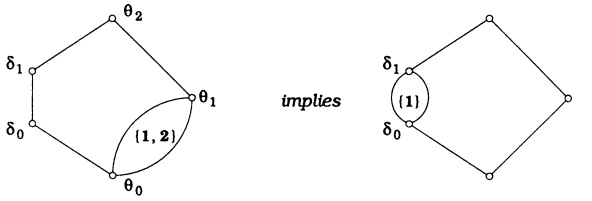
LEMMA 6.4. *Suppose that* $\delta_0, \delta_1, \delta_2, \gamma_0, \gamma_1, \psi, \theta$ *are congruences of a finite algebra* $\mathbf{A}$ *constituting a sublattice of* $\mathbf{Con}\,\mathbf{A}$ *isomorphic to* $\mathbf{D}_1$, *as pictured below. If* $\theta \prec \alpha \leq \delta_1$, *then* $\mathrm{typ}(\theta, \alpha) = \mathbf{1}$.



PROOF. Since $\delta_1 \wedge \delta_0 = \delta_1 \wedge \delta_2 = \theta$ and $\delta_1 \wedge (\delta_0 \vee \delta_2) = \delta_1$, it follows from Lemma 5.19 (1) that $\mathrm{typ}(\theta, \alpha) \in \{\mathbf{1}, \mathbf{2}\}$. Assume that $\mathrm{typ}(\theta, \alpha) = \mathbf{2}$, in order to derive a contradiction. Let U be any $\langle \theta, \alpha \rangle$-minimal set and let B be the body of U, and T be the tail. Since $\delta_i \wedge \delta_1 = \theta$ $(i = 0, 2)$, we have $\delta_i|_U = \delta_i|_U \vee \theta|_U \not\geq \alpha|_U$ $(i = 0, 2)$. So by Lemma 4.27 (4), $\delta_0|_U \cup \delta_2|_U \subseteq B^2 \cup T^2$. From this, and from the fact that $\delta_0|_U \vee \delta_2|_U = (\delta_0 \vee \delta_2)|_U$, it is obvious that $\delta_0|_B \vee \delta_2|_B = (\delta_0 \vee \delta_2)|_B$, a fact which will be needed below.

We repeat the calculation used in proving the last lemma, working with congruences over the Mal'cev algebra $\mathbf{A}|_B$. It is obvious that $|_B$ preserves lattice meets; and the one non-trivial join we need is preserved (see the last paragraph). We have $\delta_0|_B \wedge \gamma_1|_B = \theta|_B \leq \delta_2|_B$, and $\delta_0|_B \vee \delta_2|_B = \psi|_B \geq \gamma_1|_B$. Since $\mathbf{Con}\,\mathbf{A}|_B$ is modular, this implies that $\gamma_1|_B = \delta_2|_B$. Thus $\delta_1|_B = \delta_1|_B \wedge \gamma_1|_B = \delta_1|_B \wedge \delta_2|_B = \theta|_B$. Since $\theta \prec \alpha \leq \delta_1$, this contradicts the fact that $\theta|_B \neq \alpha|_B$. □

LEMMA 6.5. *Let* $\theta_0, \theta_1, \theta_2, \delta_1, \delta_0$ *be congruences of a finite algebra constituting a pentagon; i.e.,* $\theta_0 = \delta_1 \wedge \theta_1 < \delta_0 < \delta_1 < \delta_0 \vee \theta_1 = \theta_2$. *If* $\mathrm{typ}\{\theta_0, \theta_1\} \subseteq \{\mathbf{1}, \mathbf{2}\}$, *then* $\mathrm{typ}\{\delta_0, \delta_1\} = \{\mathbf{1}\}$.



PROOF. The truth of the lemma will follow if we can prove it under the assumption that $\delta_0 \prec \delta_1$. We make that assumption, and assume that $\mathrm{typ}\{\theta_0, \theta_1\} \subseteq \{\mathbf{1}, \mathbf{2}\}$, and $\mathrm{typ}(\delta_0, \delta_1) \neq \mathbf{1}$. We will derive a contradiction. Let U be a $\langle \delta_0, \delta_1 \rangle$-minimal set, and let B and T be its $\langle \delta_0, \delta_1 \rangle$-body and tail.

It is impossible to have $\delta_0|_B \vee \theta_1|_B \geq \delta_1|_B$. For we would then have a pentagon $\theta_0|_B, \theta_1|_B, \delta_0|_B \vee \theta_1|_B, \delta_1|_B, \delta_0|_B$ in $\mathbf{Con}\ \mathbf{A}|_B$, forcing $\operatorname{typ}(\delta_0, \delta_1) \neq \mathbf{2}$; but if $\operatorname{typ}(\delta_0, \delta_1) \in \{\mathbf{3}, \mathbf{4}, \mathbf{5}\}$ then $\delta_1|_B = B^2$, and there is no such pentagon. Therefore $\delta_0|_B \vee \theta_1|_B \not\geq \delta_1|_B$; but, of course, $\delta_0|_U \vee \theta_1|_U \geq \delta_1|_U$. From this, we draw the conclusion that $\theta_1 \cap (B \times T) \neq \emptyset$. (Recall that B is a union of $\delta_1|_U$-classes and δ_1 equals δ_0 on T.) Notice that $\theta_0 \cap (B \times T) = \emptyset$, since $\theta_0 \subseteq \delta_0$.

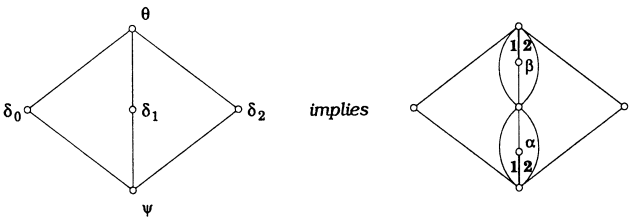
Clearly, there exists a prime quotient $\langle \gamma, \lambda \rangle$ in the interval $I[\theta_0, \theta_1]$ with

$$\gamma|_U \cap (B \times T) = \emptyset \neq \lambda|_U \cap (B \times T).$$

Now we assumed that $\operatorname{typ}\{\theta_0, \theta_1\} \subseteq \{\mathbf{1}, \mathbf{2}\}$; thus $\langle \gamma, \lambda \rangle$ and $\langle \gamma|_U, \lambda|_U \rangle$ are Abelian. It follows by an application of Lemma 4.27 (4ii), to the algebra $\mathbf{C} = \mathbf{A}|_U$ and its quotient $\langle \delta_0|_U, \delta_1|_U \rangle$, that $\operatorname{typ}(\delta_0, \delta_1) \neq \mathbf{2}$.

Thus we must have $\operatorname{typ}(\delta_0, \delta_1) \in \{\mathbf{3}, \mathbf{4}, \mathbf{5}\}$. Let $p(x, y)$ be a pseudo-meet operation of $\mathbf{A}|_U$ relative to $\langle \delta_0|_U, \delta_1|_U \rangle$. Choose $\langle b, u \rangle \in \lambda \cap (B \times T)$ and let $v = p(b, u)$. By Lemma 4.15 or Lemma 4.17, $p(b, v) = v = p(v, v)$, and $v \equiv p(b, b) = b \pmod{\lambda}$. Using that $\langle \gamma, \lambda \rangle$ is Abelian, we have $p(b, b) = b \equiv p(v, b) \pmod{\gamma}$. But $b \in B$ and $u, v, p(v, b) \in T$. This contradicts the fact that $\gamma \cap B \times T = \emptyset$; and so our proof is finished. (Incidentally, we have just worked the second half of Exercise 4.37 (5).) □

LEMMA 6.6. *Let $\delta_0, \delta_1, \delta_2, \psi, \theta$ be congruences of a finite algebra constituting a diamond; i.e., $\delta_i \vee \delta_j = \theta$ and $\delta_i \wedge \delta_j = \psi$ for $0 \leq i < j \leq 2$. If $\psi \prec \alpha \leq \delta_1$ and $\delta_1 \leq \beta \prec \theta$, then $\{\operatorname{typ}(\psi, \alpha), \operatorname{typ}(\beta, \theta)\} \subseteq \{\mathbf{1}, \mathbf{2}\}$.*



PROOF. By Exercise 3.8 (6), each quotient $\langle \psi, \delta_i \rangle$ is Abelian. Thus $\langle \psi, \alpha \rangle$ is Abelian and must have type **1** or **2**. By Lemma 5.19 (2), we have $\operatorname{typ}(\beta, \theta) \in \{\mathbf{1}, \mathbf{2}, \mathbf{5}\}$. If $\operatorname{typ}(\beta, \theta) = \mathbf{5}$ and N is a $\langle \beta, \theta \rangle$-trace, then $\delta_i|_N, \theta|_N, \psi|_N$ form a diamond with $\delta_1|_N \leq \beta|_N < \theta|_N$. We must have $\langle 1, u \rangle \in \delta_0|_N - \beta$ for some u, where 1 is the neutral element for the pseudo-meet operation $p(x, y)$ (since $\delta_0|_N \vee \beta|_N = 1_N$). But $\langle \{1, u\}, p \rangle$ is a semilattice, contradicting that $\langle \psi, \delta_0 \rangle$ is Abelian and $\langle 1, u \rangle \in \delta_0 - \psi$. □

Remark 6.7. With the aid of the theory of solvability presented in Chapter 7, it can be proved that when $\mathbf{D}_1$ occurs as a sublattice of $\mathbf{Con}\ \mathbf{A}$ ($\mathbf{A}$ finite) as in

Lemma 6.4, then $\text{typ}\{\theta, \delta_1\} \subseteq \{\mathbf{1}, \mathbf{2}\}$; and when $\mathbf{M}_3$ appears, as in Lemma 6.6, then $\text{typ}\{\psi, \theta\} \subseteq \{\mathbf{1}, \mathbf{2}\}$.

The preceding four lemmas give restrictions governing the type labels that can appear in certain positions relative to an occurence of $\mathbf{D}_2, \mathbf{D}_1, \mathbf{N}_5$ or $\mathbf{M}_3$ as a sublattice of **Con A**. As a corollary to these results, we can conclude that if the unary type does not occur in the type labeling of **Con A**, then $\mathbf{D}_1$ is not embedded in **Con A** (and analogous results for $\mathbf{D}_2$ and $\mathbf{M}_3$).

Our purpose in the second half of this chapter will be to produce an approximate converse to each of these corollaries. A result of the kind we will be proving is already to be found in Theorem 5.27: If $\mathbf{5} \in \text{typ}\{\mathbf{A}\}$, then the congruence lattice of a certain subalgebra of $\mathbf{A}^2$ has a copy of $\mathbf{D}_2$. Before beginning this task, we present two more lemmas, and this notable corollary of Lemma 6.5.

COROLLARY 6.8. *Suppose that α, β are congruences of a finite algebra $\mathbf{A}$ with $\alpha < \beta$ and $\text{typ}\{\alpha, \beta\} = \{\mathbf{2}\}$. Then $I[\alpha, \beta]$ is a modular lattice.*

LEMMA 6.9. *Let $\langle \alpha, \beta \rangle$ be a prime quotient in a finite algebra $\mathbf{A}$. Suppose that $\theta_0, \ldots, \theta_n \in I[\alpha, 1_A]$ satisfy $\beta \leq \bigvee\{\theta_i : i \leq n\}$. If $\text{typ}(\alpha, \beta) \neq \mathbf{1}$, then for some $i \leq n$, $\text{typ}(\alpha, \beta) \in \text{typ}\{\alpha, \theta_i\}$.*

PROOF. If $\langle \alpha, \beta \rangle$ is non-Abelian, then $\beta \leq \theta_i$ for some i (by Lemma 5.12), and the desired conclusion is trivial. Thus, we assume that $\text{typ}(\alpha, \beta) = \mathbf{2}$. Let U be an $\langle \alpha, \beta \rangle$-minimal set, let B be the body of U, and let T be the tail. By Lemma 4.27 (4i), if $\theta_i|_U \not\subseteq B^2 \cup T^2$ for some i, then $\theta_i|_U \geq \beta|_U$; but then $\theta_i \geq \beta$, and we are done. Thus, assume that B is a union of $\theta_i|_U$-classes, for all i. Then $\beta|_B \leq \bigvee\{\theta_i|_B : i \leq n\}$; and so we can pick an i_0 with $\theta_{i_0}|_B > \alpha|_B$. Let $\langle \tau, \lambda \rangle$ be a prime quotient in $I[\alpha, \theta_{i_0}]$ satisfying $\tau|_B = \alpha|_B$ and $\alpha|_B < \lambda|_B$.

We claim that $\text{typ}(\tau, \lambda) = \mathbf{2}$. To prove it, we choose any $\langle u, v \rangle \in \lambda|_B - \tau|_B$, and $e \in \text{E}(\mathbf{A})$ with $e(A) = U$. Since $\langle u, v \rangle \in \lambda$, there is a sequence $u = u_0, \ldots, u_m = v$ with

$$\langle u_i, u_{i+1} \rangle \in \tau \cup \bigcup\{N^2 : N \text{ a } \langle \tau, \lambda \rangle\text{-trace } \} \text{ for all } i < m\,.$$

Now for all $\langle \tau, \lambda \rangle$-traces N, either $(e(N))^2 \subseteq \tau$, or $e(N)$ is a $\langle \tau, \lambda \rangle$-trace. Since $\langle u, v \rangle \notin \tau$, there exists a $\langle \tau, \lambda \rangle$-trace $N \subseteq U$ such that $N \cap u/(\tau|_U) \neq \emptyset$. But $u/(\tau|_U) \subseteq B$, and $N^2 \subseteq \theta_{i_0}|_U \subseteq B^2 \cup T^2$; hence $N \subseteq B$.

The function e, restricted to a $\langle \tau, \lambda \rangle$-minimal set including N as trace, must be a polynomial isomorphism of this set onto a $\langle \tau, \lambda \rangle$-minimal set $V \subseteq U$. We can choose $e' \in \text{E}(\mathbf{A})$ with $e'(A) = V$; and then we have $e'|_U \in \text{E}(\mathbf{A}|_U)$ and $N \subseteq e'(U) \cap B$. Applying Lemma 4.30, we find that $e'|_U = \text{id}|_U$, and so $U = V$. Since $U = e(A)$, and B and N are congruence blocks in $U = V$ (see Lemma 4.27 (3)), we have that $\mathbf{A}|_N = (\mathbf{A}|_B)|_N$ and this algebra is Mal'cev and nilpotent. (By Theorem 4.31 and Lemma 4.36, $\mathbf{A}|_B$ is nilpotent, and its induced algebras must inherit this property.) Thus the minimal algebra $(\mathbf{A}|_N)/(\tau|_N)$ can only have type **2**. □

LEMMA 6.10. *Let $\langle \alpha, \beta \rangle$ be a prime quotient in a finite algebra* $\mathbf{A}$. *Suppose that $\theta_0, \ldots, \theta_n \in I[0_A, \beta]$ satisfy $\alpha \geq \bigwedge\{\theta_i : i \leq n\}$. If $\operatorname{typ}(\alpha, \beta) \notin \{\mathbf{1}, \mathbf{5}\}$, then for some $i \leq n$, $\operatorname{typ}(\alpha, \beta) \in \operatorname{typ}\{\theta_i, \beta\}$.*

PROOF. If $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{3}, \mathbf{4}\}$, then by Lemma 5.15, $\theta_i \leq \alpha$ for some i and we are done. Thus, let $\operatorname{typ}(\alpha, \beta) = \mathbf{2}$, and let U be an $\langle \alpha, \beta \rangle$-minimal set, and B and T be its body and tail. We assume that $\theta_i \vee \alpha = \beta$ for all i (else $\theta_i \leq \alpha$). We shall use several times the fact that $|_B$ is a homomorphism of $I[0_A, \beta]$ onto the modular lattice $I[0_B, \beta|_B] \subseteq \mathbf{Con}\,\mathbf{A}|_B$, which follows easily from Lemma 2.4 and Lemma 4.27 (3). (There exists a congruence θ of $\mathbf{A}$, with $\theta \geq \beta$, such that B is a $\theta|_U$-equivalence class.)

To begin, we have $\theta_i|_B \vee \alpha|_B = \beta|_B$ for all i, and $\bigwedge(\theta_i|_B) \leq \alpha|_B$. Also, $\alpha|_B \prec \beta|_B$, since $\alpha|_B < \beta|_B$ and $\alpha \prec \beta$ and $|_B$ is an onto homomorphism. Note also that when $\tau \leq \beta$ we have $\tau \leq \alpha \leftrightarrow \tau|_B \leq \alpha|_B$. We can obviously assume that $\bigwedge\{\theta_i : i \neq j\} \not\leq \alpha$ for each $j \leq n$, and in fact, that whenever $\theta_j < \tau \leq \beta$ then $\tau \wedge \bigwedge\{\theta_i : i \neq j\} \not\leq \alpha$. These facts then hold also for the $\theta_i|_B, \alpha|_B, \beta|_B$ in $\mathbf{Con}\,\mathbf{A}|_B$.

Let χ_0 denote $\theta_0|_B$, χ_0' be a cover of χ_0 in the interval $I[\chi_0, \beta|_B]$ (i.e., $\chi_0 \prec \chi_0' \leq \beta|_B$), $\chi_1' = \bigwedge\{\theta_i|_B : 1 \leq i \leq n\} \wedge \chi_0'$, and $\chi_1 = \chi_1' \wedge \alpha|_B$. Our assumptions imply that $\langle \alpha|_B, \beta|_B \rangle \searrow \langle \chi_1, \chi_1' \rangle$ and $\langle \chi_0 \wedge \chi_1', \chi_1' \rangle \nearrow \langle \chi_0, \chi_0' \rangle$, in the notation of Exercise 6.23 (13). The proof of this is an exercise for the reader. Now $\alpha|_B \prec \beta|_B$ and $\chi_0 \prec \chi_0'$; so by Exercise 6.23 (13), $\chi_1 \prec \chi_1'$ and $\chi_0 \wedge \chi_1' \prec \chi_1'$. Note that $\chi_0 \wedge \chi_1' \leq \alpha|_B$, so $\chi_0 \wedge \chi_1' \leq \chi_1' \wedge \alpha|_B = \chi_1$, and thus $\chi_0 \wedge \chi_1' = \chi_1$.

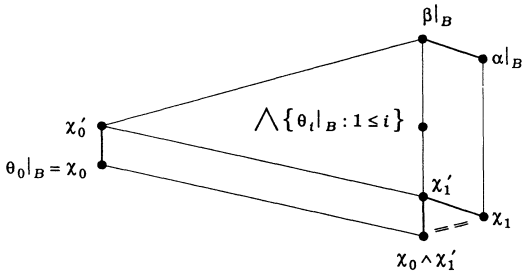


Figure 14

Now we define ψ_1 to be the largest congruence of $\mathbf{A}$ such that $\psi_1 \leq \beta$ and $\psi_1|_B = \chi_1$, and we let ψ_1' be the smallest congruence $\geq \psi_1$ such that $\psi_1'|_B = \chi_1'$. By previous remarks, $\psi_1 \leq \alpha$ and we have $\psi_1' \leq \beta$ and $\psi_1' \succ \psi_1$. It is easy to see that $I[\alpha, \beta] \searrow I[\psi_1, \psi_1']$. We put $\psi_0' = \psi_1' \vee \theta_0$, so that $\psi_0' \leq \beta$ and $\psi_0'|_B = \chi_0'$; and we choose ψ_0 so that $\theta_0 \vee \psi_1 \leq \psi_0 \prec \psi_0'$. Thus $\operatorname{typ}(\psi_0, \psi_0') \in \operatorname{typ}\{\theta_0, \beta\}$. Now it is easy to see that $I[\psi_1, \psi_1'] \nearrow I[\psi_0, \psi_0']$. By Lemma 6.2, $\operatorname{typ}(\psi_0, \psi_0') = \operatorname{typ}(\psi_1, \psi_1') = \operatorname{typ}(\alpha, \beta)$, and this concludes our proof. □

We now change our focus. Here begins a study of locally finite varieties, to which we devote the remainder of this book. Recall from Chapter 0 that a **variety** is a nonvoid class $\mathcal{V}$ of similar indexed algebras such that

$$\boldsymbol{H}\mathcal{V} = \boldsymbol{S}\mathcal{V} = \boldsymbol{P}\mathcal{V} = \mathcal{V},$$

meaning that $\mathcal{V}$ is closed under the formation of homomorphic images, subalgebras, and algebras isomorphic to Cartesian products of algebras in $\mathcal{V}$. A variety is **locally finite** iff all of its finitely generated algebras are finite. The variety generated by a class $\mathcal{K}$ of similar algebras is denoted $\boldsymbol{V}(\mathcal{K})$; thus $\boldsymbol{V}(\mathcal{K}) = \boldsymbol{HSP}\mathcal{K}$. If $\mathcal{K} = \{\mathbf{A}\}$, we write $\boldsymbol{V}(\mathbf{A})$ in place of $\boldsymbol{V}(\mathcal{K})$. A variety generated by a finite set of finite algebras is said to be **finitely generated.** Recall that finitely generated varieties are locally finite.

DEFINITION 6.11. Let $\mathcal{K}$ be any class of algebras. By CON $\mathcal{K}$ we denote the class of all congruence lattices of algebras in $\mathcal{K}$. By $\mathcal{K}_{fin}$ we denote the class of all finite members of $\mathcal{K}$. We denote the set $\bigcup\{\text{typ}\{\mathbf{A}\} : \mathbf{A} \in \mathcal{K}_{fin}\}$ by typ$\{\mathcal{K}\}$, and call it the **type set** of $\mathcal{K}$.

The type set of a locally finite variety determines a surprising collection of varietal properties, as we shall see in Chapter 9. We remark that

$$\begin{aligned}
\text{typ}\{\ \mathbf{G}\text{-}\mathit{Sets}\ \} &= \{\ \text{unary type}\ \},\quad \mathbf{G} \text{ a finite non-trivial group;}\\
\text{typ}\{\ \mathbf{F}\text{-}\mathit{Vector\ Spaces}\ \} &= \{\ \text{affine type}\ \},\quad \mathbf{F} \text{ a finite field;}\\
\text{typ}\{\ \mathit{Boolean\ Algebras}\ \} &= \{\ \text{Boolean type}\ \};\\
\text{typ}\{\ \mathit{Distributive\ Lattices}\ \} &= \{\ \text{lattice type}\ \};\\
\text{typ}\{\ \mathit{Semilattices}\ \} &= \{\ \text{semilattice type}\ \}.
\end{aligned}$$

The underlying theme of this second half of Chapter 6 will be that when $\mathbf{A}$ is a finite algebra and N is a trace set for one of the prime congruence quotients of $\mathbf{A}$, then $\mathbf{A}|_N$ (after conversion to an indexed algebra) generates a variety which is interpretable in a very well-behaved fashion into the variety generated by $\mathbf{A}$. Through these interpretations, we will find that every lattice in CON $\boldsymbol{V}(\mathbf{A}|_N)$ is a complete homomorphic image of an interval in some member of CON $\boldsymbol{V}(\mathbf{A})$. Every locally finite variety $\mathcal{V}$ "contains", in the sense of our interpretations, one of the varieties in the above list corresponding to each type-label appearing in typ$\{\mathcal{V}\}$.

DEFINITION 6.12. Let $\mathbf{A}$ be any algebra and let U be any nonvoid subset of the universe of $\mathbf{A}$. By $\mathbf{AI}_U$ we mean the indexed algebra $\langle U, f\ (\ f \in (\mathrm{Pol}\ \mathbf{A})|_U\ )\rangle$. This indexed algebra $\mathbf{AI}_U$ is polynomially equivalent to $\mathbf{A}|_U$, and will be called $\mathbf{A}|_U$ **with the normal indexing**.

DEFINITION 6.13. Let $\mathbf{A}$ be any indexed algebra and T be any set. By a **diagonal subalgebra** of $\mathbf{A}^T$ we mean any subalgebra of $\mathbf{A}^T$ containing the diagonal Δ, the set of all constant functions from T into A. For every nonvoid subset S of A^T, we denote by $\mathbf{A}(S)$ the subalgebra of $\mathbf{A}^T$ generated by $S \cup \Delta$. This algebra will be called the **extension of A by** S. For any operation f on A, we write $f^{(T)}$ for the operation on A^T which is f acting coordinatewise. For any equivalence relation β on A, we write $\beta^{(T)}$ for the equivalence relation defined by $\langle x, y\rangle \in \beta^{(T)}$ iff for all $t \in T$, $\langle x(t), y(t)\rangle \in \beta$.

Notice that $\mathbf{A}(\emptyset) \cong \mathbf{A}$, and that $\mathbf{A}(S)$ *is*, up to isomorphism, an extension of $\mathbf{A}$. We are interested in this construction mainly in the case where $S \subseteq N^T$ for some trace N of $\mathbf{A}$, but we shall prove our basic results in a more general setting.

LEMMA 6.14. *Suppose that* $\mathbf{A}$ *is an algebra; that* $e \in \mathrm{E}(\mathbf{A})$, $U = e(A)$ *and* $\beta \in \mathrm{Con}\ \mathbf{A}$; *and that* S *is a* $\beta|_U$*-equivalence class. Let* T *be any set and let* $\mathbf{S}' = \langle S', \dots\rangle$ *be a subalgebra of* $(\mathbf{AI}_S)^T$. *Then define* $\mathbf{A}' = \mathbf{A}(S')$; $e' = e^{(T)}|_{A'}$; $U' = e'(A')$; *and* $\beta' = \beta^{(T)}|_{A'}$.

(1) *The universe of* $\mathbf{A}'$ *is closed under* $f^{(T)}$ *for all* $f \in \mathrm{Pol}\ \mathbf{A}$. *We have that* $\mathrm{Pol}\ \mathbf{A}' \supseteq \{f^{(T)}|_{A'} :\ f \in \mathrm{Pol}\ \mathbf{A}\}$, *and*

$$A' = \{f^{(T)}(s_0, \dots, s_{n-1}) :\ f \in \mathrm{Pol}_n\mathbf{A} \quad \text{for some} \quad n \quad \text{and} \quad \{s_0, \dots, s_{n-1}\} \subseteq S'\}\ .$$

(2) *We have that* $e' \in \mathrm{E}(\mathbf{A}')$; $U' = e'(A') = A' \cap U^T$; $\beta' \in \mathrm{Con}\ \mathbf{A}'$; S' *is a* $\beta'|_{U'}$*-equivalence class; and* $S' = A' \cap S^T$.

(3) $\mathbf{A}'|_{S'} = \mathbf{S}'|_{S'}$.

PROOF. Statement (1) depends on nothing more than the fact that $\mathbf{A}'$ is the diagonal subalgebra of $\mathbf{A}^T$ generated by S'. To prove it, let $f \in \mathrm{Pol}\ \mathbf{A}$. For some m and n, we have an $m+n$-ary term operation $g \in \mathrm{Clo}_{m+n}\mathbf{A}$ and elements $a_0, \dots, a_{m-1}$ in A such that $f(x_0, \dots, x_{n-1}) = g(a_0, \dots, a_{m-1}, x_0, \dots, x_{n-1})$. We write $\langle a_i\rangle$ for the member of $\Delta \subseteq A^T$ whose constant value is a_i. Now $g^{(T)}$ is a term operation of $\mathbf{A}^T$, and $f^{(T)}(x_0, \dots, x_{n-1}) = g^{(T)}(\langle a_0\rangle, \dots, \langle a_{m-1}\rangle, x_0, \dots, x_{n-1})$. Obviously, A' is closed under $f^{(T)}$, since it is closed under $g^{(T)}$ and $\langle a_0\rangle, \dots, \langle a_{m-1}\rangle \in A'$; and since $g^{(T)}|_{A'}$ is a term operation of $\mathbf{A}'$, it follows that $f^{(T)}|_{A'}$ is a polynomial operation of $\mathbf{A}'$. The description of A' follows easily from these considerations.

To prove (2), we note that $e' \in \mathrm{Pol}_1 \mathbf{A}'$ by (1), and clearly $e'e' = e'$; so $e' \in \mathrm{E}(\mathbf{A}')$. For $x \in A'$, we have $x \in e'(A')$ iff $e'(x) = x$ iff $e(x(t)) = x(t)$ for all $t \in T$ iff $x \in U^T$. Obviously, $\beta' \in \mathrm{Con}\ \mathbf{A}'$, and it is easy to see that $A' \cap S^T$ is a $\beta'|_{U'}$-equivalence class which includes S'. To prove that $A' \cap S^T \subseteq S'$, let $a \in A' \cap S^T$. By (1), we can write $a = f^{(T)}(s_0, \ldots, s_{n-1})$, $f \in \mathrm{Pol}_n \mathbf{A}$, $s_0, \ldots, s_{n-1} \in S'$. We can assume that $f = ef$, since $e^{(T)}(a) = a$. For any $t \in T$, $f(s_0(t), \ldots, s_{n-1}(t)) = a(t) \in S$, implying that $f(S^n) \subseteq S$. This holds because $f(U^n) \subseteq U$, S is a $\beta|_U$-equivalence class, and $a(t), s_0(t), \ldots, s_{n-1}(t) \in S$. (Note that if $T = \emptyset$ then our lemma holds trivially; $\mathbf{A}^T$ is then a one-element algebra.) Therefore $f|_S$ is an operation of $\mathbf{AI}_S$. It follows that $a \in S'$, as claimed, since $a = f^{(T)}(s_0, \ldots, s_{n-1}) = (f|_S)^{(T)}(s_0, \ldots, s_{n-1})$ and S' is a subuniverse of $(\mathbf{AI}_S)^T$. This finishes the proof of (2).

In order to prove (3), we need these characterizations of Pol $\mathbf{S}'$ and Pol $\mathbf{A}'$.

$$\mathrm{Pol}_n \mathbf{S}' = \{ f^{(T)}|_{S'}(s_0, \ldots, s_{m-1}, x_0, \ldots, x_{n-1}) : \ f \in \mathrm{Pol}_{m+n} \mathbf{A} \text{ for some } m,\ f(S^{m+n}) \subseteq S, \text{ and } s_0, \ldots, s_{m-1} \in S' \} . \tag{6.14.1}$$

$$\mathrm{Pol}_n \mathbf{A}' = \{ f^{(T)}|_{A'}(s_0, \ldots, s_{m-1}, x_0, \ldots, x_{n-1}) : \ f \in \mathrm{Pol}_{m+n} \mathbf{A} \text{ for some } m, \text{ and } s_0, \ldots, s_{m-1} \in S' \} . \tag{6.14.2}$$

To prove (6.14.1), notice that the term operations of $\mathbf{AI}_S$ are precisely the $f|_S$ such that $f \in \mathrm{Pol}_k \mathbf{A}$ and $f(S^k) \subseteq S$ for some k. Consequently, those of $\mathbf{S}'$ are precisely the $(f|_S)^{(T)}|_{S'} = f^{(T)}|_{S'}$ such that $f \in \mathrm{Pol}_k \mathbf{A}$ and $f(S^k) \subseteq S$ for some k. The characterization of $\mathrm{Pol}_n \mathbf{S}'$ follows immediately from this.

To prove (6.14.2), recall that by (1), $f^{(T)}|_{A'}$ is a polynomial of $\mathbf{A}'$, for all $f \in \mathrm{Pol}\ \mathbf{A}$. Replacing some variables by "constants" (i.e., by $s_0, \ldots, s_{m-1}$) in a polynomial creates a new polynomial. Therefore we have $\supseteq$ in (6.14.2). To get the reverse inclusion, let $g^{(T)}|_{A'}$ ($g \in \mathrm{Clo}\ \mathbf{A}$) be any $k+n$-ary term operation of $\mathbf{A}'$, and let $w_0, \ldots, w_{k-1} \in A'$. It must be shown that where

$$h(x_0, \ldots, x_{n-1}) = g^{(T)}|_{A'}(w_0, \ldots, w_{k-1}, x_0, \ldots, x_{n-1}),$$

$h(x_0, \ldots, x_{n-1})$ can be expressed in the form claimed in (6.14.2). By an obvious extension of (1), there exist (for some m), $s_0, \ldots, s_{m-1} \in S'$ and $g_0, \ldots, g_{k-1} \in \mathrm{Pol}_m \mathbf{A}$ with $w_i = g_i^{(T)}(s_0, \ldots, s_{m-1})$ for $0 \leq i < k$. We define

$$f(y_0, \ldots, y_{m-1}, x_0, \ldots, x_{n-1}) = g(g_0(\bar{y}), \ldots, g_{k-1}(\bar{y}), x_0, \ldots, x_{n-1}) .$$

Then $f \in \mathrm{Pol}_{m+n} \mathbf{A}$, and it is easy to check that

$$f^{(T)}|_{A'}(s_0, \ldots, s_{m-1}, x_0, \ldots, x_{n-1}) = h(x_0, \ldots, x_{n-1}) .$$

This finishes our proof of (6.14.2).

The proof of (3) is immediate from (6.14.1) and (6.14.2), using the trick of composing a polynomial with e, that was employed in the proof of (2). □

LEMMA 6.15. *Assume that* $\mathbf{A}$ *is an algebra; that* $e \in \mathrm{E}(\mathbf{A})$, $U = e(A)$, $\beta \in \mathrm{Con}\,\mathbf{A}$; *and that* S *is a* $\beta|_U$*-equivalence class. Let* θ *be any congruence of* $\mathbf{A}$ *satisfying* $\theta \leq \beta$. *Define* $\mathbf{A}' = \mathbf{A}/\theta$; $e' = e_\theta$; $U' = e'(A')$; $\beta' = \beta/\theta$; *and* $S' = S/\theta$. *Then* $e' \in \mathrm{E}(\mathbf{A}')$; $\beta' \in \mathrm{Con}\,\mathbf{A}'$; S' *is a* $\beta'|_{U'}$*-equivalence class; and* $\mathbf{A}'|_{S'} \cong (\mathbf{A}|_S)/(\theta|_S)$.

PROOF. This lemma looks formidable, but is actually quite trivial to prove. The proof is left up to the reader. □

LEMMA 6.16. *Suppose that* $\mathbf{A}$ *is a finite algebra; that* $e \in \mathrm{E}(\mathbf{A})$, $U = e(A)$, $\beta \in \mathrm{Con}\,\mathbf{A}$; *and that* S *is a* $\beta|_U$*-equivalence class. Then* $\mathrm{typ}\{\mathbf{A}|_S\} \subseteq \mathrm{typ}\{0_A, \beta\}$.

PROOF. Let $\langle \delta, \theta \rangle$ be any prime quotient of $\mathbf{A}|_S$. By Lemma 2.4, restriction is a homomorphism of $I[0_A, \beta]$ onto $\mathrm{Con}\,\mathbf{A}|_S$. We can choose $\overline{\delta}$, $\overline{\theta} \in \mathrm{Con}\,\mathbf{A}$ such that $\overline{\delta} \prec \overline{\theta} \leq \beta$ and $\overline{\delta}|_S = \delta$, $\overline{\theta}|_S = \theta$. We then choose $\langle c, d \rangle \in S \cap (\overline{\theta} - \overline{\delta})$. Notice that $e(c/\overline{\theta}) \subseteq c/\overline{\theta}$ and $e(c/\overline{\theta}) \not\subseteq c/\overline{\delta}$. Thus by Exercise 5.11 (3) (the version of Theorem 2.8 (6) adapted to traces) there is a $\langle \overline{\delta}, \overline{\theta} \rangle$-trace $N \subseteq c/\overline{\theta}$ such that $e(N) = N_1$ is a $\langle \overline{\delta}, \overline{\theta} \rangle$-trace. Now $N_1 \subseteq U \cap c/\beta = S$.

We can assume that $c, d \in N_1$ (or choose new elements). There is $e_1 \in \mathrm{E}(\mathbf{A})$ with $e_1(A) \subseteq e(A) = U$, $e_1(A) \in \mathrm{M}_A(\overline{\delta}, \overline{\theta})$, and N_1 a $\langle \overline{\delta}, \overline{\theta} \rangle$-trace in $e_1(A)$. Clearly $e_1(N_1) = N_1$ and $e_1(S) \subseteq S$. Since $e_1(\theta) \not\subseteq \delta$, the range of the polynomial $e_1|_S$ contains a $\langle \delta, \theta \rangle$-minimal set V. We have $V = e'(S)$ for some $e' \in \mathrm{E}(\mathbf{A}|_S)$; and of course there exists $e_2 \in \mathrm{E}(\mathbf{A})$ such that $e_2|_S = e'$. We may assume that $e_1 e_2 = e_2$. Clearly $e_2(\overline{\theta}) \not\subseteq \overline{\delta}$, and $e_2(A) \subseteq e_1(A)$, hence $e_2(A) = e_1(A)$. It follows from this that all elements of N_1 are fixed by e_2, and thus $N_1 \subseteq e_2(S) = V$. Now $c/\theta \cap V = M$ is a $\langle \delta, \theta \rangle$-trace in V, and $N_1 \subseteq M$. But since $V \subseteq e_1(A)$, we have $M \subseteq c/\overline{\theta} \cap e_1(A) = N_1$. So the set $M = N_1$ is both a $\langle \overline{\delta}, \overline{\theta} \rangle$-trace and a $\langle \delta, \theta \rangle$-trace. It is easy to prove that $\mathbf{A}|_M = (\mathbf{A}|_S)|_M$; and clearly $\delta|_M = \overline{\delta}|_M$. Hence $\mathrm{typ}(\overline{\delta}, \overline{\theta}) = \mathrm{typ}((\mathbf{A}|_M)/(\overline{\delta}|_M)) = \mathrm{typ}(\delta, \theta)$. □

THEOREM 6.17. *Suppose that* $\mathbf{A}$ *is an algebra; that* $e \in \mathrm{E}(\mathbf{A})$, $U = e(A)$, $\beta \in \mathrm{Con}\,\mathbf{A}$; *and that* S *is a* $\beta|_U$*-equivalence class.*

(1) *For every algebra* $\mathbf{C} \in \boldsymbol{V}(\mathbf{AI}_S)$, *there exist* $\mathbf{A}' \in \boldsymbol{V}(\mathbf{A})$, $e' \in \mathrm{E}(\mathbf{A}')$, $U' = e'(A')$, $\beta' \in \mathrm{Con}\,\mathbf{A}'$, *and a* $\beta'|_{U'}$*-equivalence class* S' *satisfying:*
   (i) $\mathbf{A}'|_{S'} \cong \mathbf{C}|_C$.
   (ii) *There exists a complete lattice homomorphism of* $I[0_{A'}, \beta']$ *onto* $\mathbf{Con}\,\mathbf{C}$.
   (iii) *If* $\mathbf{A}$ *and* $\mathbf{C}$ *are finite, then* $\mathbf{A}'$ *is finite.*

(2) *If* $\mathbf{A}$ *is finite, then* $\mathrm{typ}\{\boldsymbol{V}(\mathbf{AI}_S)\} \subseteq \mathrm{typ}\{\boldsymbol{V}(\mathbf{A})\}$.

PROOF. When (1i) holds, then (1ii) follows, by Lemma 2.4 and Exercise 2.5 (1). To prove (1), let $\mathbf{C} \in \boldsymbol{V}(\mathbf{AI}_S)$. There exists $\mathbf{S}'' \subseteq (\mathbf{AI}_S)^T$ for some set T, and a congruence $\bar{\theta}$ on $\mathbf{S}''$ with $\mathbf{C} \cong \mathbf{S}''/\bar{\theta}$. If $\mathbf{A}$ and $\mathbf{C}$ are finite, then we can take a finite T, by Theorem 0.2. Applying Lemma 6.14, we obtain $\mathbf{A}'' \subseteq \mathbf{A}^T$, $e'' \in \mathrm{E}(\mathbf{A}'')$, etc. By Lemma 2.4, there exists $\theta'' \in I[0_{A''}, \beta'']$ with $\theta''|_{S''} = \bar{\theta}$. Applying Lemma 6.15 to the system $\langle \mathbf{A}'', e'', U'', \beta'', S'', \theta'' \rangle$, we obtain a system $\langle \mathbf{A}', e', U', \beta', S' \rangle$. We have

$$\mathbf{A}'|_{S'} \cong (\mathbf{A}''|_{S''})/(\theta''|_{S''}) = (\mathbf{S}''|_{S''})/\bar{\theta} \cong \mathbf{C}|_C \ .$$

This proves (1). Statement (2) follows from (1), by Lemma 6.16. □

Theorem 6.17 has some interesting corollaries. In order to introduce them, we need one more lemma.

LEMMA 6.18. *Let* $\mathbf{M}$ *be a finite minimal algebra of unary type. The variety* $\boldsymbol{V}(\mathbf{MI}_M)$ *generated by* $\mathbf{M}$ *with the normal indexing contains, for every nonvoid set* S, *an algebra* $\mathbf{S} = \langle S, \dots \rangle$ *such that* $\mathbf{S}$ *has only trivial polynomials, i.e.,* $\mathbf{S}|_S = \langle S \rangle|_S$.

PROOF. Let $\Lambda = (\mathrm{Sym}\ M) \cap (\mathrm{Pol}_1\mathbf{M})$. Every polynomial $f(x_0, \dots, x_{n-1})$ of $\mathbf{M}$ is constant, or of the form $f(x_0, \dots, x_{n-1}) = \sigma(x_i)$ for some $i < n$ and for some $\sigma \in \Lambda$. The set Λ is a subuniverse of the group $\mathrm{Sym}\ M$.

Let S be any set of at least two elements. Choosing elements $u \neq v$ in M, let D be the subset of M^S consisting of the constant functions and all the functions $p(\sigma, s)$ ($\sigma \in \Lambda$, $s \in S$) defined by

$$p(\sigma, s)(s') = \begin{cases} \sigma(u) & \text{if} \quad s' \in S - \{s\} \\ \sigma(v) & \text{if} \quad s' = s \end{cases}$$

It is easy to check that D is a subuniverse of $(\mathbf{MI}_M)^S$. The algebra $\mathbf{D} \subseteq (\mathbf{MI}_M)^S$ whose universe is D has a congruence θ defined by

$$\langle x, y \rangle \in \theta \leftrightarrow (\exists \sigma \in \Lambda)(\sigma(x(s)) = y(s) \text{ for all } s \in S) \ .$$

The algebra $\mathbf{E} = \mathbf{D}/\theta$ has at least $|S|$ elements, and every term operation of $\mathbf{E}$ is either constant or a projection. This lemma follows from these considerations. □

The variety of **bounded distributive lattices** is the variety generated by the algebra $\langle \{0,1\}, \vee, \wedge, 0, 1 \rangle$. The variety of **bounded semilattices** is the variety generated by the algebra $\langle \{0,1\}, \wedge, 0, 1 \rangle$. Recall that $\boldsymbol{\Pi}_\kappa$ denotes the lattice of all equivalence relations on the cardinal κ (and that κ is a set of ordinal numbers). We define

$\mathcal{L}_1 = \{\ \mathbf{\Pi}_\kappa :\ \kappa$ is any cardinal $\}$;

$\mathcal{L}_{\mathbf{F}} = \{\ \mathbf{Con\ V} :\ \mathbf{V}$ is an $\mathbf{F}$-vector space $\}$, $\mathbf{F}$ is a field;

$\mathcal{L}_3 = \{\ \mathbf{Con\ B} :\ \mathbf{B}$ is a Boolean algebra $\}$;

$\mathcal{L}_4 = \{\ \mathbf{Con\ L} :\ \mathbf{L}$ is a bounded distributive lattice $\}$;

$\mathcal{L}_5 = \{\ \mathbf{Con\ S} :\ \mathbf{S}$ is a bounded semilattice $\}$.

THEOREM 6.19. *Let* $\mathbf{A}$ *be any finite indexed algebra.*

(1) *If* $\mathbf{1} \in \mathrm{typ}\{\mathbf{A}\}$, *then for every* $\mathbf{L} \in \mathcal{L}_1$ *there exists* $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$, *and* $\theta \in \mathrm{Con}\,\mathbf{B}$, *and a complete* $0,1$*-separating homomorphism of* $I[0_B, \theta]$ *onto* $\mathbf{L}$. *If* $\mathbf{L} = \mathbf{\Pi}_n$ *for an integer* $n \geq 4$, *then* $\mathbf{B}$ *can be chosen to be finite and* $\langle 0_B, \theta\rangle$ *to be tame of unary type.*

(2) *If* $\langle \alpha, \beta\rangle$ *is tame in* $\mathbf{A}$ *of affine type with associated field* $\mathbf{F}$, *then for every* $\mathbf{L} \in \mathcal{L}_{\mathbf{F}}$ *there exists* $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$, *and* $\theta \in \mathrm{Con}\,\mathbf{B}$, *and a complete* $0,1$*-separating homomorphism of* $I[0_B, \theta]$ *onto* $\mathbf{L}$. *If* $\mathbf{L} = \mathbf{Con\ V}$ *for a finite vector space* $\mathbf{V}$ *of dimension* > 1, *then* $\mathbf{B}$ *can be chosen to be finite, and* θ *can be chosen so that* $\langle 0_B, \theta\rangle$ *is tame of affine type, and the associated minimal algebras* $\mathbf{B}|_{N'}$ *satisfy* $\mathbf{B}|_{N'} \cong \mathbf{V}|_V$.

(3) *If* $\mathbf{3}$, $\mathbf{4}$ *or* $\mathbf{5}$ *belong to* $\mathrm{typ}\{\mathbf{A}\}$, *then for every* $\mathbf{L} \in \mathcal{L}_i$ *(*$i = 3$, 4 *or* 5, *respectively), there exists* $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$, *finite if* $\mathbf{L}$ *is finite, and* $\theta \in \mathrm{Con}\,\mathbf{B}$, *and a complete* $0,1$*-separating homomorphism of* $I[0_B, \theta]$ *onto* $\mathbf{L}$.

PROOF. We begin with (1). Suppose that $\mathbf{1} \in \mathrm{typ}\{\mathbf{A}\}$. Replacing $\mathbf{A}$ by a homomorphic image, we can assume that $0_A \prec \beta$ in $\mathbf{Con\ A}$, $\mathrm{typ}(0_A, \beta) = \mathbf{1}$, $U \in \mathrm{M}_{\mathbf{A}}(0_A, \beta)$, $e \in \mathrm{E}(\mathbf{A})$, $e(A) = U$, and N is a $\langle 0_A, \beta\rangle$-trace in U. The algebra $\mathbf{N} = \mathbf{A}\mathrm{I}_N = \mathbf{N}\mathrm{I}_N$ is minimal of unary type.

Let $\mathbf{L} = \mathbf{\Pi}_\kappa$, the lattice of all equivalence relations over the cardinal number κ. By Lemma 6.18, there exists $\mathbf{C} \in \boldsymbol{V}(\mathbf{N})$ with $\mathbf{Con\ C} \cong \mathbf{L}$, and $\mathbf{C}$ is finite if κ is finite. By Theorem 6.17, there exists $\mathbf{A}'$ in $\boldsymbol{V}(\mathbf{A})$ (with $\mathbf{A}'$ finite if $\mathbf{C}$ is finite), and $\beta' \in \mathrm{Con}\,\mathbf{A}'$, and a complete lattice homomorphism $\pi' : I[0_{A'}, \beta'] \twoheadrightarrow \mathbf{L}$. For any such homomorphism, there exists a smallest $\theta' \leq \beta'$ such that $\pi'(\theta') = \pi'(\beta')$, and a largest $\delta' \leq \theta'$ such that $\pi'(\delta') = \pi'(0_{A'})$. Replacing $\mathbf{A}'$ by $\mathbf{B} = \mathbf{A}'/\delta'$, and using that $I[\delta', \theta'] \cong I[0_B, \theta]$, where $\theta = \theta'/\delta'$, we have a complete $0,1$-separating homomorphism $\pi : I[0_B, \theta] \twoheadrightarrow \mathbf{L}$.

Now if $\mathbf{L} = \mathbf{\Pi}_n$, $n \geq 4$, then $\mathbf{B}$ is finite by construction. The interval $I[0_B, \theta]$ is a tight lattice, by Lemma 1.10 and Example 1.12. By Theorem 2.11, $\langle 0_B, \theta\rangle$ is tame. Now $\mathbf{\Pi}_n$ is simple and nonmodular. Hence by Lemma 1.10, $I[0_B, \theta]$ cannot

admit a 0, 1-separating homomorphism onto the congruence lattice of a vector space. Therefore by Theorem 5.7, $\langle 0_B, \theta \rangle$ is of unary type (strongly Abelian). This concludes the proof of (1).

The proof of (2) is similar. We can assume to start with that $\langle 0_A, \beta \rangle$ is a prime quotient of affine type, and that $\mathbf{N} = \mathbf{AI}_N = \mathbf{W}|_W$ where $\mathbf{W}$ is a vector space over $\mathbf{F}$ of dimension 1. The steps followed before lead to $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$, $\theta \in \operatorname{Con} \mathbf{B}$, and $S \subseteq B$ such that $\pi = |_S : I[0_B, \theta] \twoheadrightarrow \operatorname{Con} \mathbf{B}|_S$ is complete and 0, 1-separating, $\mathbf{B}|_S \cong \mathbf{V}|_V$, and $\mathbf{L} \cong \mathbf{Con}\, \mathbf{V}$. Assuming that $\mathbf{L}$ is finite and $\dim \mathbf{V} > 1$, then $\mathbf{B}$ is finite; and as before (by Example 1.13), $I[0_B, \theta]$ is tight and $\mathbf{L}$ is its simple homomorphic image, unique up to isomorphism. By Theorem 5.7, the type of $\langle 0_B, \theta \rangle$ can only be **1** or **2**. It is not **1**, because $\mathbf{B}|_S$ is Mal'cev and S is contained in a θ-class. Thus $\langle 0_B, \theta \rangle$ is of type **2**. Letting N' be any $\langle 0_B, \theta \rangle$-trace, we have that $\mathbf{L}' = \mathbf{Con}\, \mathbf{B}|_{N'}$ is a 0, 1-separating simple homomorphic image of $I[0_B, \theta]$; and so $\mathbf{L} \cong \mathbf{L}'$. Now, via coordinatization in projective geometry, the field of scalars and the dimension of a vector space can be recovered from its congruence lattice (or, as is more usual, from the lattice of subspaces). Therefore, we can conclude that $\mathbf{B}|_{N'} \cong \mathbf{V}|_V$.

The proof of (3) follows the same pattern, and is easier. Note that if $\mathbf{L} = \mathbf{Con}\, \mathbf{Q}$ where $\mathbf{Q}$ is a Boolean algebra, bounded distributive lattice, or bounded semilattice, and if $\mathbf{L}$ is finite, then $\mathbf{Q}$ is finite. □

We shall draw further corollaries from Theorem 6.17 after the next definition and lemma.

DEFINITION 6.20. A lattice $\mathbf{L}$ will be called **finitely projective** iff $\mathbf{L}$ is finite and for each onto lattice homomorphism $\varphi : \mathbf{L}' \twoheadrightarrow \mathbf{L}$ with $\mathbf{L}'$ finite, there exists a homomorphism $\sigma : \mathbf{L} \to \mathbf{L}'$ satisfying $\varphi\sigma = \mathrm{id}_L$.

Note that if $\mathbf{L}$ is finitely projective, and if $\varphi : \mathbf{L}' \twoheadrightarrow \mathbf{L}$ with $\mathbf{L}'$ finite, then $\mathbf{L}'$ has a sublattice isomorphic to $\mathbf{L}$. Finitely projective lattices are characterized in Exercise 6.23 (14).

LEMMA 6.21. *Each of the lattices* $\mathbf{N}_5, \mathbf{D}_1, \mathbf{D}_2$ *and* $\mathbf{M}_n$ $(n \geq 1)$ *is finitely projective.*

PROOF. We prove this fact for $\mathbf{D}_1$, and leave the remaining proofs to the reader. $\mathbf{D}_1$ is pictured in Figure 12. (See Remark 5.21.) Suppose that $\varphi : \mathbf{L}' \twoheadrightarrow \mathbf{D}_1$ and $\mathbf{L}'$ is finite. Let 0 and 1 denote the least and the largest elements of $\mathbf{D}_1$ respectively. Let $a = \bigvee \varphi^{-1}\{0\}$, and $b = \bigwedge \varphi^{-1}\{1\}$. Let $\mathbf{L}''$ be the interval $I[a, a \vee b]$ in $\mathbf{L}'$ and put $\varphi'' = \varphi|_{L''}$. If $x \in L'$, then $x'' = (a \vee x) \wedge (a \vee b)$ belongs to L'' and $\varphi''(x'') = \varphi(x)$. Therefore φ'' maps $\mathbf{L}''$ onto $\mathbf{L}$. Moreover, $\varphi'' : \mathbf{L}'' \twoheadrightarrow \mathbf{L}$ is 0, 1-separating.

Now let u, v, w be the three atoms of $\mathbf{D}_1$, satisfying $u \vee w = 1$, $(u \vee v) \wedge (v \vee w) = v$. (See Figure 12.) Choose any $u'', v'', w'' \in L''$ with

$$\varphi''(u'') = u, \varphi''(v'') = v, \varphi''(w'') = w\,.$$

Replacing v'' by $(u'' \vee v'') \wedge (v'' \vee w'')$, we can be sure that

$$(u'' \vee v'') \wedge (v'' \vee w'') = v'' .$$

Since $\varphi''(u'' \vee w'') = 1$, we have $u'' \vee w'' = a \vee b$. Similarly,

$$u'' \wedge v'' = u'' \wedge w'' = v'' \wedge w'' = a .$$

The relations

$$(u'' \vee v'') \wedge w'' = a = u'' \wedge (v'' \vee w'')$$

can be demonstrated in the same manner. One can now check that $\{a, u'', v'', w'', u'' \vee v'', v'' \vee w'', a \vee b\}$ is a sublattice of $\mathbf{L}'$ isomorphic to $\mathbf{D}_1$, and that the isomorphism provides the required map $\sigma : \mathbf{L} \to \mathbf{L}'$. □

By a **finite subdirect power** of an algebra $\mathbf{A}$ is meant an algebra $\mathbf{B}$ such that for some integer $n \geq 1$, $\mathbf{B} \subseteq \mathbf{A}^n$ and the image of $\mathbf{B}$ under each of the coordinate projections from $\mathbf{A}^n$ is $\mathbf{A}$.

THEOREM 6.22. *Let $\mathbf{A}$ be a finite indexed algebra, let $\mathcal{K}$ be the class of all finite subdirect powers of $\mathbf{A}$, and let $\boldsymbol{S}(\mathrm{CON}\ \mathcal{K})$ be the class of all lattices isomorphic to a sublattice of $\mathbf{Con}\ \mathbf{B}$ for some $\mathbf{B} \in \mathcal{K}$.*

(1) *These statements are equivalent:*
   (i) $\mathbf{1} \in \mathrm{typ}\{\mathcal{K}\}$;
   (ii) $\mathbf{D}_1 \in \boldsymbol{S}(\mathrm{CON}\ \mathcal{K})$;
   (iii) *Every finitely projective lattice belongs to* $\boldsymbol{S}(\mathrm{CON}\ \mathcal{K})$.

(2) $\mathbf{D}_2 \in \boldsymbol{S}(\mathrm{CON}\ \mathcal{K})$ *iff* $\mathrm{typ}\{\mathcal{K}\} \cap \{\mathbf{1}, \mathbf{5}\} \neq \emptyset$.

(3) $\mathbf{M}_3 \in \boldsymbol{S}(\mathrm{CON}\ \mathcal{K})$ *iff* $\mathrm{typ}\{\mathcal{K}\} \cap \{\mathbf{1}, \mathbf{2}\} \neq \emptyset$.

PROOF. That (1iii) implies (1ii) follows from the last lemma. That (1ii) implies (1i) follows from Lemma 6.4. Now suppose that (1i) holds; let $\mathbf{L}$ be any finitely projective lattice. It was proved by P. Pudlák and J. Tuma in [30] that every finite lattice is isomorphic to a sublattice of $\mathbf{\Pi}_n$ for some finite n. We can thus assume that $\mathbf{L} \subseteq \mathbf{\Pi}_n$ and $n \geq 4$. By Theorem 6.19(1), there is $\mathbf{B} \in \mathcal{K}$, and an interval $I[\alpha, \beta]$ in $\mathbf{Con}\ \mathbf{B}$, and a homomorphism $\varphi : I[\alpha, \beta] \twoheadrightarrow \mathbf{\Pi}_n$. [Theorem 6.19 only gives a finite $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$, but the proof, via Lemmas 6.14 and 6.15, actually produces an algebra which is a homomorphic image of a diagonal subalgebra of $\mathbf{A}^k$ for a finite k. Thus, if we don't require $\alpha = 0_B$, we can have $\mathbf{B} \in \mathcal{K}$.] Letting $\mathbf{L}' = \varphi^{-1}(\mathbf{L})$, since $\varphi|_{L'} : \mathbf{L}' \twoheadrightarrow \mathbf{L}$ and $\mathbf{L}$ is finitely projective, there exists $\mathbf{L}'' \cong \mathbf{L}$ with $\mathbf{L}'' \subseteq \mathbf{L}' \subseteq \mathbf{Con}\ \mathbf{B}$. This finishes the proof that $\mathbf{L} \in \boldsymbol{S}(\mathrm{CON}\ \mathcal{K})$, and the proof that (1i) implies (1iii).

That $\mathrm{typ}\{\mathcal{K}\} \cap \{\mathbf{1}, \mathbf{5}\} \neq \emptyset$ if $\mathbf{D}_2 \in \boldsymbol{S}(\mathrm{CON}\ \mathcal{K})$ follows directly from Lemma 6.3. For the other implication in statement (2), Theorem 5.27(2) implies that $\mathbf{D}_2 \in$

$\boldsymbol{S}(\mathrm{CON}\ \mathcal{K})$ if $\mathbf{5} \in \mathrm{typ}\{\mathcal{K}\}$; and (1), just proved (combined with Lemma 6.21) implies that $\mathbf{D}_2 \in \boldsymbol{S}(\mathrm{CON}\ \mathcal{K})$ if $\mathbf{1} \in \mathrm{typ}\{\mathcal{K}\}$.

Statement (3) follows from Lemma 6.6 if $\mathbf{M}_3 \in \boldsymbol{S}(\mathrm{CON}\ \mathcal{K})$, and follows from (1) and Lemma 6.21 if $\mathbf{1} \in \mathrm{typ}\{\mathcal{K}\}$. So assume that $\mathbf{2} \in \mathrm{typ}\{\mathcal{K}\}$. Just as in the proof of (1), Theorem 6.19 (2) gives the existence of $\mathbf{B} \in \mathcal{K}$ and an interval $I[\alpha, \beta]$ in $\mathbf{Con}\ \mathbf{B}$ which has $\mathbf{M}_n$ for some $n \geq 3$ (has, actually, the congruence lattice of a two-dimensional vector space over some finite field) as a homomorphic image. Since $\mathbf{M}_3 \subseteq \mathbf{M}_n$ and $\mathbf{M}_3$ is finitely projective, we have that $\mathbf{M}_3 \in \boldsymbol{S}(\mathbf{Con}\ \mathbf{B})$. □

A class of finite, similar, indexed algebras closed under the formation of subalgebras, homomorphic images, and products of two algebras at a time, is called a **pseudo-variety.** Statements (1), (2), and (3) of Theorem 6.22 are obviously valid for any pseudo-variety. (This follows from Theorem 6.22.) The subsequent chapters are focused mainly on locally finite varieties, not pseudo-varieties, but most of the results obtained will be valid for pseudo-varieties. Theorem 6.22 is a precursor of the full-scale type-omission theorems for locally finite varieties proved in Chapter 9.

Exercises 6.23. We construct a collection of examples which illustrate our theorems and destroy some plausible conjectures. We begin with several four-element algebras having the universe $A = \{0, 1, 0', 1'\}$ and the congruences and congruence lattice pictured in Figure 15.

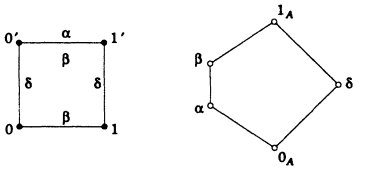


Figure 15

The following operations will be used.

s_1	0	1	0′	1′
0	0	1	0′	1′
1	1	0	1′	0′
0′	0′	1′	0′	1′
1′	1′	0′	1′	0′

s_2	0	1	0′	1′
0	0′	0′	0′	0′
1	0′	1′	0′	1′
0′	0′	0′	0′	0′
1′	0′	1′	0′	1′

s_3	0	1	0′	1′
0	0	0	0	0
1	0	0	0	0
0′	0	0	0′	0′
1′	0	0	0′	0′

x	$u_1(x)$
0	0′
1	0′
0′	0
1′	0

x	$u_2(x)$
0	1′
1	1′
0′	1
1′	1

Figure 16

(1) Assume that $\mathbf{A} = \langle \{0, 1, 0', 1'\}, \dots \rangle$ (operations unknown) and that $\operatorname{Con} \mathbf{A} = \{0_A, 1_A, \alpha, \beta, \delta\}$ (as displayed in Figure 15). Prove:
   (i) $\mathbf{A}$ is $\langle \alpha, \beta \rangle$-minimal and $\{0, 1\}$ is the only $\langle \alpha, \beta \rangle$-trace.
   (ii) Let $t(x) = s_1(x, 0')$. Either $\mathrm{E}(\mathbf{A}) = \{\text{constants}\} \cup \{\mathrm{id}, t\}$ or $\mathrm{E}(\mathbf{A}) = \{\text{constants}\} \cup \{\mathrm{id}, t, u_1^2, u_2^2\}$.
   (iii) $\mathrm{M}_{\mathbf{A}}(0, \alpha) = \{\{0', 1'\}\}$; and $\{0, 0'\}$, $\{1, 1'\}$ are the $\langle 0, \delta \rangle$-traces.
   (iv) Since $A/\delta = 0/\delta \cup 1/\delta$, Pol $\mathbf{A}/\delta$ is at least as rich as $(\text{Pol } \mathbf{A})|_{\{0,1\}}$; hence $\operatorname{typ}(\alpha, \beta) \leq \operatorname{typ}(\delta, 1)$ in the ordering of types pictured in Figure 10 (preceeding Theorem 5.5).
   (v) If $\operatorname{typ}(\alpha, \beta) = \mathbf{2}$ and $d(x, y, z)$ is pseudo-Mal'cev for $\langle \alpha, \beta \rangle$, then we must have $s_1(x, y) = d(x, 0, y)$.

(2) Show that each of the operations s_1, s_2, s_3, u_1, u_2 preserves α, β and δ. Show that $\operatorname{Con} \langle A, s_1 \rangle = \{0_A, 1_A, \alpha, \beta, \delta\}$.

(3) Let $\mathbf{A}_1 = \langle A, s_1 \rangle$, $\mathbf{A}_2 = \langle A, s_1, s_3 \rangle$, $\mathbf{A}_3 = \langle A, s_1, u_1, u_2 \rangle$, and let $\mathbf{A}_{i+3}$ $(i = 1, 2, 3)$ be $\mathbf{A}_i$ with the operation s_2 adjoined. By the last exercise, each of $\mathbf{A}_1, \dots, \mathbf{A}_6$ has the pentagon of Figure 15 as congruence lattice. Prove that the type labelings for these algebras are:

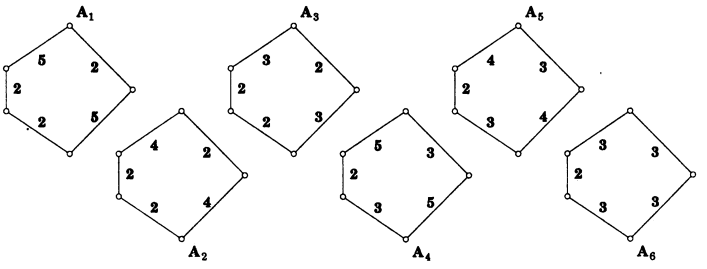


Figure 17

[Note: Using Lemma 6.2, all the type labels except $\operatorname{typ}(\alpha, \beta)$ can be determined by computing the two-element algebras $\mathbf{A}/\beta$ and $\mathbf{A}/\delta$, and determining their types. In each of the algebras $\mathbf{A} = \mathbf{A}_i$, the $\langle \alpha, \beta \rangle$-trace algebra $\mathbf{A}|_{\{0,1\}}$ has at least the operation of a group; thus $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{2}, \mathbf{3}\}$. The work is finished by proving that in the richest of these algebras, $\mathbf{A}_6$, $\langle \alpha, \beta \rangle$ is Abelian. Define $\rho \subseteq A^3$ as $\{0', 1'\}^3 \cup \{\langle x, y, z \rangle \in \{0, 1\}^3 : s_1(x, y) = z\}$. Show that ρ is admissible for $\mathbf{A}_6$. From this, derive that $\mathbf{A}_6|_{\{0,1\}}$ is Abelian.]

(4) For any pair of non-unary types $\mathbf{u}$ and $\mathbf{v}$, construct an algebra with universe $\{0, 1, 0', 1'\}$ whose congruences are the equivalence relations depicted in Figure

15, and in which

$$\text{typ}(\alpha, \beta) = \mathbf{1},\ \text{typ}(\beta, 1) = \mathbf{u},\ \text{typ}(\delta, 1) = \mathbf{v}.$$

We construct several algebras on the base set $B = \{0, 1, 0', 1', \bar{1}\}$, having the congruences and congruence lattice pictured in Figure 18.

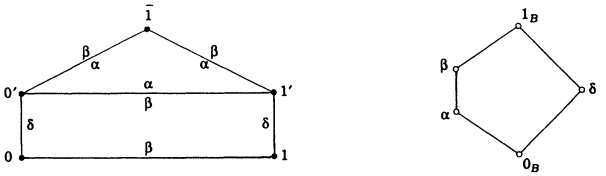


Figure 18

The following operations will be used.

p_1	0	1	0′	1′	$\bar{1}$
0	0	1	0′	1′	$\bar{1}$
1	1	0	1′	0′	$\bar{1}$
0′	0′	1′	0′	1′	$\bar{1}$
1′	1′	0′	1′	0′	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$

p_2	0	1	0′	1′	$\bar{1}$
0	0	0	0	0	0
1	0	0	0	0	0
0′	0	0	0′	0′	0′
1′	0	0	0′	0′	0′
$\bar{1}$	0	0	0′	0′	0′

p_3	0	1	0′	1′	$\bar{1}$
0	0′	0′	0′	0′	0′
1	0′	0′	0′	0′	0′
0′	0′	0′	0′	0′	0′
1′	0′	0′	0′	0′	0′
$\bar{1}$	0′	0′	0′	0′	$\bar{1}$

q_1	0	1	0′	1′	$\bar{1}$
0	0	1	0′	1′	$\bar{1}$
1	1	1	1′	1′	$\bar{1}$
0′	0′	1′	0′	1′	$\bar{1}$
1′	1′	1′	1′	1′	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$

q_2	0	1	0′	1′	$\bar{1}$
0	0	0	0′	0′	$\bar{1}$
1	0	1	0′	1′	$\bar{1}$
0′	0′	0′	0′	0′	$\bar{1}$
1′	0′	1′	0′	1′	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$

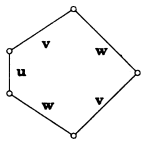
q_3	0	1	0′	1′	$\bar{1}$
0	0′	$\bar{1}$	0′	$\bar{1}$	$\bar{1}$
1	$\bar{1}$	1′	$\bar{1}$	1′	$\bar{1}$
0′	0′	$\bar{1}$	0′	$\bar{1}$	$\bar{1}$
1′	$\bar{1}$	1′	$\bar{1}$	1′	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$

x	$\pi(x)$	$\nu_1(x)$	$\nu_2(x)$	$\nu_3(x)$	$\nu_4(x)$	$\sigma(x)$	$\tau(x)$
0	1	0′	$\bar{1}$	0	1	0′	$\bar{1}$
1	0	$\bar{1}$	1′	0	1	0′	0′
0′	1′	0′	$\bar{1}$	0′	1′	0	$\bar{1}$
1′	0′	$\bar{1}$	1′	0′	1′	0	0′
$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	0	0′

Figure 19

(5) Show that each operation $p_1, \ldots, \sigma, \tau$ preserves the equivalence relations α, β, δ of Figure 18.

(6) For every $\{\mathbf{u},\mathbf{v},\mathbf{w}\} \subseteq \{\mathbf{2},\mathbf{3},\mathbf{4},\mathbf{5}\}$, such that $\{\mathbf{v},\mathbf{w}\} \subseteq \{\mathbf{3},\mathbf{4},\mathbf{5}\}$, construct an algebra $\mathbf{B} = \langle B, \ldots \rangle$, using a subset of the above defined set of operations, such that $\text{Con}\,\mathbf{B} = \{0_B, 1_B, \alpha, \beta, \delta\}$ and the type labeling of **Con B** is:



(7) Let $\mathbf{A} = \langle \{0,1\}, f_0, f_1, f_2 \rangle$, $\mathbf{B} = \langle \{0,1\}, g_0, g_1, g_2 \rangle$, where

$$f_0(x,y) = g_0(x,y) = x \vee y\,,$$
$$f_1(x,y) = g_2(x,y) = x \wedge y\,,$$
$$f_2(x,y) = g_1(x,y) = 1\,.$$

Let η_0 and η_1 be the kernels of the two coordinate projections from $\mathbf{A} \times \mathbf{B}$, and let α be the equivalence relation on $A \times B$ with blocks $A \times B - \{\langle 0,0 \rangle\}$ and $\{\langle 0,0 \rangle\}$. Show that the labeled congruence lattice of $\mathbf{A} \times \mathbf{B}$ is

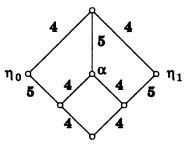


Figure 20

Prove that if we replace f_1, f_2, g_1, g_2 by $f_1'(x) = 1 - x = g_2'(x)$ and $f_2'(x) = 1 = g_1'(x)$, then the congruence lattice of $\mathbf{A} \times \mathbf{B}$ is unchanged, and the type labels **5** remain unchanged, but the **4**'s become **3**'s.

The above exercises make it obvious that types of prime quotients not present in $\mathbf{A}$ or in $\mathbf{B}$ can appear in $\mathbf{A} \times \mathbf{B}$, or in subdirect products of $\mathbf{A}$ and $\mathbf{B}$. The same situation prevails with regard to the formation of subalgebras. It seems that the only valid type-conservation theorems involve homomorphic images, and the type set $\{\mathbf{1}, \mathbf{2}\}$. [We have that $\text{typ}\{\mathbf{A}/\alpha\} \subseteq \text{typ}\{\mathbf{A}\}$ if $\mathbf{A}$ is finite. Subalgebras and finite products of finite solvable algebras are solvable, as will be proved in Chapter 7.]

(8) Let $\mathbf{S}$ be a finite simple algebra of at least three elements whose minimal sets are two-element sets, and such that $\text{typ}(\mathbf{S}) \neq \mathbf{1}$. (Such an $\mathbf{S}$ exists having any prescribed type.) Define $\mathbf{A} = \langle S, F \rangle$, where F consists of all $f \in \text{Pol } \mathbf{S}$ such that f is essentially unary or its range is a two-element set. Then $\mathbf{A}$ is simple, $\text{typ}(\mathbf{A}) = \text{typ}(\mathbf{S})$, and $\mathbf{A}$ has no proper subalgebras. Let $n = |A|$, and define an equivalence relation θ on A^n by: $\langle x, y \rangle \in \theta \leftrightarrow x = y$ or range $(x) \neq A \neq$

range (y). Show that $\theta \in \operatorname{Con} \mathbf{A}^n$ and $\mathbf{A}^n/\theta$ is a minimal algebra of unary type.

(9) Let $\mathbf{B} = \langle \{0,1\}, \dots \rangle$ be any algebra with base set $\{0,1\}$. Let F be the set of all operations f on $A = \{0,1,2\}$ such that $\{0,1\}$ is closed under f and $f|_{\{0,1\}} \in \operatorname{Pol} \mathbf{B}$. Defining $\mathbf{A} = \langle A, f(f \in F) \rangle$, show that $\mathbf{A}$ is a simple algebra of type **3**, and that $\langle \{0,1\}, f|_{\{0,1\}} (f \in F) \rangle$ is a subalgebra of $\mathbf{A}$ whose type equals the type of $\mathbf{B}$.

(10) Prove the claims in the paragraph following Definition 6.11 that concern the type set of a variety generated by a minimal algebra.

(11) Prove that if $\mathbf{A}$ is a finite group or ring, or any finite Mal'cev algebra, then $\operatorname{typ}\{\mathbf{A}\} \subseteq \{\mathbf{2}, \mathbf{3}\}$.

(12) Let $\mathbf{A}$ be an indexed algebra. Show that (1) $\Rightarrow$ (2) $\Rightarrow$ (3):

(1) For every subalgebra $\mathbf{B}$ of $\mathbf{A}^2$, $\mathbf{Con}\ \mathbf{B}$ satisfies SD($\vee$).

(2) For all $\theta, \lambda \in \operatorname{Con} \mathbf{A}$, $[\theta, \lambda] = \theta \wedge \lambda$.

(3) $\mathbf{Con}\ \mathbf{A}$ satisfies SD($\wedge$).

{The semi-distributive laws SD($\vee$) and SD($\wedge$) are defined in Definition 5.18. The commutator $[\theta, \lambda]$ is defined in Exercise 3.8 (3). The proof of (1) $\Rightarrow$ (2) involves looking at an algebra $\mathbf{B} = \mathbf{A}(\beta) \subseteq \mathbf{A}^2$ whose universe is β, and three congruences, $\eta_0 = \{\langle x, y \rangle \in B^2 : x(0) = y(0)\}$, $\eta_1 = \{\langle x, y \rangle \in B^2 : x(1) = y(1)\}$, and δ, the congruence generated by $\{\langle \langle a, a \rangle, \langle b, b \rangle \rangle : \langle a, b \rangle \in \beta\}$. Here, β is any congruence of $\mathbf{A}$ such that $[\beta, \beta] < \beta$.}

(13) For two quotients $\langle x_i, y_i \rangle$ ($i = 0, 1$) of a lattice $\mathbf{L}$, we write $\langle x_0, y_0 \rangle \nearrow \langle x_1, y_1 \rangle$ (or $\langle x_1, y_1 \rangle \searrow \langle x_0, y_0 \rangle$) iff $y_0 \wedge x_1 = x_0$ and $y_0 \vee x_1 = y_1$. When this holds, we say that $\langle x_1, y_1 \rangle$ **is projective to** $\langle x_0, y_0 \rangle$ **in one step**. Prove that if $\mathbf{L}$ is modular and $\langle x_0, y_0 \rangle \nearrow \langle x_1, y_1 \rangle$, then the maps $x \mapsto x \vee x_1$ and $y \mapsto y \wedge y_0$ are mutually inverse isomorphisms between the interval sublattices $I[x_0, y_0]$ and $I[x_1, y_1]$.

(14) It is known that a finite lattice $\mathbf{L}$ is finitely projective (Definition 6.20) iff $\mathbf{L}$ satisfies this condition (W): for all $x, y, u, v, a, b \in L$, if $x \wedge y = a \leq b = u \vee v$ then $\{x, y, u, v\} \cap I[a, b] \neq \emptyset$. Try to prove this result of B.A. Davey and B. Sands [8]. (It is also known that a finite lattice is projective in the class of all lattices iff it satisfies (W) and is semi-distributive. This deep result is due to J. B. Nation [24].)

7. SOLVABILITY AND SEMI-DISTRIBUTIVITY

The notions of solvable and of strongly solvable congruence quotients were defined in Chapter 3, and their most basic properties were developed there. In this chapter, we delve deeper, and show that each of these notions supplies an interesting congruence *on* the congruence lattice of a locally finite algebra. We require a new definition.

DEFINITION 7.1. Let $\mathbf{A}$ be any algebra.

(1) A 1-**snag** of $\mathbf{A}$ is any pair $\langle a, b\rangle$ of distinct elements of $\mathbf{A}$ such that for some $f \in \mathrm{Pol}_2\mathbf{A}$, $f(a,b) = f(b,a) = a$ and $f(b,b) = b$. $\mathrm{Sn}_1(\mathbf{A})$ denotes the set of all 1-snags of $\mathbf{A}$.

(2) A 2-**snag** of $\mathbf{A}$ is any pair $\langle a, b\rangle$ of distinct elements of $\mathbf{A}$ such that for some $f \in \mathrm{Pol}_2\mathbf{A}$, $f(a,b) = f(b,a) = f(a,a) = a$ and $f(b,b) = b$. $\mathrm{Sn}_2(\mathbf{A})$ denotes the set of all 2-snags of $\mathbf{A}$.

According to Exercises 5.11 (1–2), a prime quotient $\langle \alpha, \beta\rangle$ in a finite algebra $\mathbf{A}$ is strongly Abelian iff $(\beta - \alpha) \cap \mathrm{Sn}_1(\mathbf{A}) = \emptyset$, and is Abelian iff $(\beta - \alpha) \cap \mathrm{Sn}_2(\mathbf{A}) = \emptyset$. These facts allow us to prove the next theorem.

THEOREM 7.2. *Let $\mathbf{A}$ be finite and let $\delta \leq \gamma$ be congruences of $\mathbf{A}$. The following are equivalent*

(1) $\langle \delta, \gamma\rangle$ *is solvable (or strongly solvable).*

(2) $\mathrm{Sn}_2(\mathbf{A}) \cap (\gamma - \delta) = \emptyset$ *(or* $\mathrm{Sn}_1(\mathbf{A}) \cap (\gamma - \delta) = \emptyset$*).*

(3) *For all $\delta \leq \alpha \prec \beta \leq \gamma$, the quotient $\langle \alpha, \beta\rangle$ is Abelian (or strongly Abelian).*

(4) $\mathrm{typ}\{\delta, \gamma\} \subseteq \{\mathbf{1},\mathbf{2}\}$ *(or* $\mathrm{typ}\{\delta, \gamma\} \subseteq \{\mathbf{1}\}$*).*

PROOF. The proof that the statements in parentheses are equivalent is analogous to the proof for the unparenthesized statements, and will be omitted.

The equivalence of (3) and (4) is by Theorem 5.7 (3). Now suppose that (1) holds. So we have a chain of congruences $\delta = \alpha_0 \leq \alpha_1 \leq \cdots \leq \alpha_n = \gamma$ such that $\langle \alpha_i, \alpha_{i+1}\rangle$ is Abelian for $i = 0, \ldots, n-1$. Then, directly from the definitions, it follows that $\mathrm{Sn}_2(\mathbf{A}) \cap (\alpha_{i+1} - \alpha_i)$ is empty for $i = 0, \ldots, n-1$, from which we conclude directly that (2) holds. Thus (1) implies (2).

Exercise 5.11 (1) yields that (2) implies (3). That (3) implies (1) is made clear by considering any maximal chain $\delta = \alpha_0 \prec \alpha_1 \cdots \prec \alpha_k = \gamma$ in the interval $I[\delta, \gamma]$. □

DEFINITION 7.3. Letting $\mathbf{A}$ be any algebra, we define an equivalence relation $\overset{s}{\sim}$ on Con $\mathbf{A}$ by setting $\gamma_0 \overset{s}{\sim} \gamma_1$ iff $\gamma_0 \cap \mathrm{Sn}_2(\mathbf{A}) = \gamma_1 \cap \mathrm{Sn}_2(\mathbf{A})$. We define a second equivalence relation $\overset{ss}{\sim}$ by $\gamma_0 \overset{ss}{\sim} \gamma_1$ iff $\gamma_0 \cap \mathrm{Sn}_1(\mathbf{A}) = \gamma_1 \cap \mathrm{Sn}_1(\mathbf{A})$.

LEMMA 7.4. *Let $\mathbf{A}$ be a locally finite algebra. Then $\overset{s}{\sim}$ and $\overset{ss}{\sim}$ are congruences on* **Con A**.

PROOF. We first prove the lemma under the assumption that $\mathbf{A}$ is finite; and we tackle $\overset{s}{\sim}$ first. Let $\alpha, \gamma_0, \gamma_1 \in$ Con $\mathbf{A}$ be such that $\gamma_0 \overset{s}{\sim} \gamma_1$. It suffices to show that $\alpha \wedge \gamma_0 \overset{s}{\sim} \alpha \wedge \gamma_1$ and $\alpha \vee \gamma_0 \overset{s}{\sim} \alpha \vee \gamma_1$. The former is clear, and to see the latter, assume not, say $\langle a, b\rangle \in \mathrm{Sn}_2(\mathbf{A})$ and $\langle a, b\rangle \in (\alpha \vee \gamma_0) - (\alpha \vee \gamma_1)$. By Theorem 7.2, there exist μ, ν for which

$$\alpha \vee (\gamma_0 \wedge \gamma_1) \leq \mu \prec \nu \leq \alpha \vee \gamma_0$$

with $\mathrm{typ}(\mu, \nu) \in \{\mathbf{3,4,5}\}$. We choose a set $U \in \mathrm{M}_{\mathbf{A}}(\mu, \nu)$, with trace N and a pseudo-meet operation $p(x, y)$ which has a neutral element $1 \in N$. (See Definitions 4.16 and 4.18.) Now $\alpha|_U \leq \mu|_U$, so

$$\nu|_U \leq \alpha|_U \vee \gamma_0|_U \leq \mu|_U \vee \gamma_0|_U;$$

and $\{1\}$ is a $\mu|_U$-equivalence class, from which we conclude that for some $u \in U - \{1\}$, $\langle u, 1\rangle \in \gamma_0 - \mu$. By Lemma 4.15 or Lemma 4.17, the pair $\langle u, 1\rangle$ is a 2-snag, implying that $\langle u, 1\rangle \in \gamma_0 \wedge \gamma_1$, since $\gamma_0 \overset{s}{\sim} \gamma_1$. But $\gamma_0 \wedge \gamma_1 \leq \mu$, giving $\langle u, 1\rangle \in \mu$, a contradiction. Thus $\overset{s}{\sim}$ is a congruence on the lattice **Con A**.

The proof that $\overset{ss}{\sim}$ is a congruence is very similar. Suppose that $\gamma_0 \overset{ss}{\sim} \gamma_1$ and $\alpha \vee (\gamma_0 \wedge \gamma_1) \leq \mu \prec \nu \leq \alpha \vee \gamma_0$ where $\mathrm{typ}(\mu, \nu) \neq \mathbf{1}$, and $U \in \mathrm{M}_{\mathbf{A}}(\mu, \nu)$. If $\mathrm{typ}(\mu, \nu) \notin \{\mathbf{1,2}\}$, the previous proof yields a contradiction. (Observe that $\mathrm{Sn}_2(\mathbf{A}) \subseteq \mathrm{Sn}_1(\mathbf{A})$). If $\mathrm{typ}(\mu, \nu) = \mathbf{2}$, let $d(x, y, z)$ be a pseudo-Mal'cev operation for U with respect to $\langle \mu, \nu\rangle$. There must exist $\langle u, b\rangle \in \gamma_0 - \mu$ with $u \in U$ and b in the body of U, since $\mu \vee \gamma_0 \geq \nu$. The equations true for $d(x, y, z)$ (see Lemma 4.20) show that $f(x, y) = d(x, b, y)$ makes $\langle u, b\rangle$ a 1-snag. Thus $\langle u, b\rangle \in \gamma_0 \wedge \gamma_1 \leq \mu$, a contradiction.

In case $\mathbf{A}$ is locally finite but not finite, we argue as follows. Let $\gamma_0, \gamma_1, \alpha \in$ Con $\mathbf{A}$ with $\gamma_0 \overset{s}{\sim} \gamma_1$. Of course $\alpha \wedge \gamma_0 \overset{s}{\sim} \alpha \wedge \gamma_1$; to see that $\alpha \vee \gamma_0 \overset{s}{\sim} \alpha \vee \gamma_1$, let $\langle a, b\rangle \in \mathrm{Sn}_2(\mathbf{A}) \cap (\alpha \vee \gamma_0)$. There is a finite algebra $\mathbf{F} \subseteq \mathbf{A}$ with $\langle a, b\rangle \in \mathrm{Sn}_2(\mathbf{F}) \cap (\alpha|_F \vee \gamma_0|_F)$. Obviously, $\gamma_0|_F \overset{s}{\sim} \gamma_1|_F$, and so we can conclude that $\langle a, b\rangle \in \alpha|_F \vee \gamma_1|_F$ as above. Thus $\langle a, b\rangle \in \alpha \vee \gamma_1$ as desired. The proof for $\overset{ss}{\sim}$ is the same. □

COROLLARY 7.5. *Let $\mathbf{A}$ be locally finite and $\alpha, \beta \in$ Con $\mathbf{A}$. Then $\alpha \overset{s}{\sim} \beta$ (or $\alpha \overset{ss}{\sim} \beta$) iff for every finite subalgebra $\mathbf{F}$ of $\mathbf{A}$, $(\alpha \vee \beta)|_F$ is solvable (or strongly solvable) over $(\alpha \wedge \beta)|_F$. If $\mathbf{A}$ is finite then $\alpha \overset{s}{\sim} \beta$ iff $\langle \alpha \wedge \beta, \alpha \vee \beta\rangle$ is a solvable quotient; and $\alpha \overset{ss}{\sim} \beta$ iff $\langle \alpha \wedge \beta, \alpha \vee \beta\rangle$ is a strongly solvable quotient.* □

Motivated by the theorem and corollary, congruences satisfying $\alpha \overset{s}{\sim} \beta$ will be called **locally solvable equivalent**, and algebras satisfying $0_A \overset{s}{\sim} 1_A$ will be called **locally**

solvable. In finite algebras, we drop the adjective "locally". Similar terminology will be used for $\overset{ss}{\sim}$.

COROLLARY 7.6. *Let $\mathcal{V}$ be a locally finite variety. The class of locally solvable algebras in $\mathcal{V}$ is a variety, as is the class of locally strongly solvable algebras in $\mathcal{V}$.*

PROOF. We will prove the two assertions simultaneously. It is obvious that the class of locally (strongly) solvable algebras in $\mathcal{V}$ is closed under the formation of products and subalgebras.

So let $\mathbf{A} \in \mathcal{V}$ contain no 2-snags (1-snags), and let $\mathbf{B} = \mathbf{A}/\theta$. We want to show that $\mathrm{Sn}_2(\mathbf{B}) = \emptyset$ ($\mathrm{Sn}_1(\mathbf{B}) = \emptyset$), as well. If $\mathrm{Sn}_2(\mathbf{B})$ ($\mathrm{Sn}_1(\mathbf{B})$) is non-empty, then there is a finite $\mathbf{F} \subseteq \mathbf{B}$ with $\mathrm{Sn}_2(\mathbf{F})$ ($\mathrm{Sn}_1(\mathbf{F})$) non-empty. There is a finite $\mathbf{F}' \subseteq \mathbf{A}$ with $\mathbf{F}'/(\theta|F') \cong \mathbf{F}$. By Theorem 7.2, $\mathbf{F}$ is not (strongly) solvable; so $\langle \theta|_{\mathbf{F}'}, 1|_{\mathbf{F}'} \rangle$ is not (strongly) solvable, by Proposition 3.7(3) (Proposition 3.11(3)). Thus $\mathbf{F}'$, and hence $\mathbf{A}$, contains a 2-snag (1-snag). This contradiction shows that the class of locally (strongly) solvable algebras in $\mathcal{V}$ is closed under the formation of homomorphic images; and since it is also closed under the formation of products and subalgebras, it is a variety. □

Before stating our main theorem about the solvability congruences, we recall that SD(∧) and SD(∨), the properties of meet and join semi-distributivity, are defined in Definition 5.18. Algebraic lattices are defined in §0.2.

THEOREM 7.7. *Let $\mathbf{A}$ be any locally finite algebra and let $\mathbf{L} = \mathbf{Con}\,\mathbf{A}$.*

(1) *The lattices $\mathbf{L}/\overset{s}{\sim}$ and $\mathbf{L}/\overset{ss}{\sim}$ are algebraic, and the quotient homomorphisms from $\mathbf{L}$ onto these lattices are complete (preserve all joins and meets).*
(2) *$\mathbf{L}/\overset{s}{\sim}$ satisfies* SD(∧).
(3) *If $\mathbf{A}$ is finite and $\mathbf{5} \notin \mathrm{typ}\{\mathbf{A}\}$ then $\mathbf{L}/\overset{s}{\sim}$ satisfies* SD(∨) *and* SD(∧).
(4) *$\overset{ss}{\sim}$ is contained in $\overset{s}{\sim}$, and every equivalence class of the congruence $\overset{s}{\sim}/\overset{ss}{\sim}$ is a modular sublattice of $\mathbf{L}/\overset{ss}{\sim}$.*

PROOF. We only prove the part of (1) that refers to $\overset{s}{\sim}$. First we prove that every equivalence class of $\overset{s}{\sim}$ has a least and a largest element. From this it follows easily that $\mathbf{L}/\overset{s}{\sim}$ is complete and that $\mathbf{L} \to \mathbf{L}/\overset{s}{\sim}$ is a complete homomorphism.

Let $\alpha \in L$ and put $\alpha^+ = \bigvee\{\beta : \beta \overset{s}{\sim} \alpha\}$ and $\alpha^- = \bigwedge\{\beta : \beta \overset{s}{\sim} \alpha\}$. Clearly, $\alpha \cap \mathrm{Sn}_2(\mathbf{A}) = \alpha^- \cap \mathrm{Sn}_2(\mathbf{A})$, hence $\alpha \overset{s}{\sim} \alpha^-$. To see that $\alpha \overset{s}{\sim} \alpha^+$, let $\langle a, b \rangle \in \mathrm{Sn}_2(\mathbf{A}) \cap \alpha^+$. Then for some finite nonvoid set of congruences $T \subseteq \alpha/\overset{s}{\sim}$, we have $\langle a, b \rangle \in \bigvee T$. Since $\bigvee T \overset{s}{\sim} \alpha$, then $\langle a, b \rangle \in \alpha$. Thus $\alpha^+ \overset{s}{\sim} \alpha \overset{s}{\sim} \alpha^-$ and $\alpha/\overset{s}{\sim}$ does indeed have least and largest elements.

Now we prove that the complete lattice $\mathbf{L}/\overset{s}{\sim}$ is algebraic. Let $\bar{\alpha} = \alpha/\overset{s}{\sim}$ be some element in $L/\overset{s}{\sim}$, and put

$$C = \{\Theta(a, b)/\overset{s}{\sim} : \langle a, b \rangle \in \mathrm{Sn}_2(\mathbf{A}) \cap \alpha\}.$$

(Here, $\Theta(a,b)$ is the congruence of $\mathbf{A}$ generated by $\langle a,b\rangle$.) Now $\bigvee C = \tau/\overset{s}{\sim}$ where $\tau = \bigvee\{\Theta(a,b) : \langle a,b\rangle \in \mathrm{Sn}_2(\mathbf{A}) \cap \alpha\}$ by the part already proved. Clearly, $\tau \leq \alpha$ and $\alpha \cap \mathrm{Sn}_2(\mathbf{A}) \subseteq \tau$; thus $\tau \overset{s}{\sim} \alpha$. We conclude then that $\bigvee C = \bar{\alpha}$. We can easily see that every member of C is compact in $L/\overset{s}{\sim}$. Indeed, let $\langle a,b\rangle \in \mathrm{Sn}_2(\mathbf{A})$ and $\delta = \Theta(a,b)$, $\bar{\delta} = \delta/\overset{s}{\sim}$. Suppose that

$$\bar{\delta} \leq \bigvee\{\gamma/\overset{s}{\sim} :\ \gamma \in S\} = (\bigvee S)/\overset{s}{\sim}$$

where $S \subseteq L$. This means that $\delta \cap \mathrm{Sn}_2(\mathbf{A}) \subseteq \bigvee S$. Hence $\langle a,b\rangle \in \gamma_0 \vee \cdots \vee \gamma_m$ for some $\{\gamma_0,\ldots,\gamma_m\} \subseteq S$. We conclude that $\bar{\delta}$ is contained in the join of a finite subset of the $\gamma/\overset{s}{\sim}$ $(\gamma \in S)$. This shows that $\bar{\delta}$ is compact.

We have shown that $\mathbf{L}/\overset{s}{\sim}$ is complete and that each of its elements is a join of compact elements; i.e., that it is an algebraic lattice. The analogous facts for $\mathbf{L}/\overset{ss}{\sim}$ are proved in the same manner.

To prove (2), we suppose that $\mathrm{SD}(\wedge)$ fails in the lattice $\mathbf{L}/\overset{s}{\sim}$, in order to derive a contradiction. Then let $\bar{\alpha},\bar{\beta},\bar{\gamma} \in L/\overset{s}{\sim}$ (where $\bar{\alpha} = \alpha/\overset{s}{\sim}$, etc) be such that

$$\bar{\alpha} \wedge \bar{\beta} = \bar{\alpha} \wedge \bar{\gamma} < \bar{\alpha} \wedge (\bar{\beta} \vee \bar{\gamma}).$$

We can assume that α, β and γ are the largest elements in their respective equivalence classes. Then $\alpha \wedge \beta$ and $\alpha \wedge \gamma$ are largest in their classes, so $\alpha \wedge \beta = \alpha \wedge \gamma$. The failure of meet semi-distributivity means that there exists

$$\langle a,b\rangle \in \mathrm{Sn}_2(\mathbf{A}) \cap \alpha \cap [(\beta \vee \gamma) - \beta].$$

We can find a finite algebra $\mathbf{F} \subseteq \mathbf{A}$ with

$$\langle a,b\rangle \in \mathrm{Sn}_2(\mathbf{F}) \cap \alpha|_F \cap [(\beta|_F \vee \gamma|_F) - \beta|_F].$$

Then clearly,

$$\alpha|_F \wedge \beta|_F = \alpha|_F \wedge \gamma|_F \ \not\equiv\ \alpha|_F \wedge (\beta|_F \vee \gamma|_F) \pmod{\overset{s}{\sim}}.$$

Now let α',β',γ' be the largest elements of $\mathrm{Con}\,\mathbf{F}$ congruent modulo $\overset{s}{\sim}$ (in $\mathrm{Con}\,\mathbf{F}$) to $\alpha|_F$, $\beta|_F$, $\gamma|_F$ respectively. Again we have

$$\alpha' \wedge \beta' = \alpha' \wedge \gamma' \ \not\equiv\ \alpha' \wedge (\beta' \vee \gamma') \pmod{\overset{s}{\sim}}.$$

Choose any congruence $\delta \in \mathrm{Con}\,\mathbf{F}$ with $\alpha' \wedge \beta' \prec \delta \leq \alpha' \wedge (\beta' \vee \gamma')$. By Lemma 5.19 (1), the quotient $\langle \alpha' \wedge \beta', \delta\rangle$ is Abelian. Thus $\delta \overset{s}{\sim} \alpha' \wedge \beta'$, contradicting that $\alpha' \wedge \beta'$ is the largest element in its $\overset{s}{\sim}$-class. This finishes the proof of (2).

To prove (3), we argue as above from a failure of $\mathrm{SD}(\vee)$ in $\mathbf{L}/\overset{s}{\sim}$. This leads to $\alpha,\beta,\gamma,\delta \in \mathrm{Con}\,\mathbf{A}$ with $\alpha \vee (\beta \wedge \gamma) \leq \delta \prec \alpha \vee \beta = \alpha \vee \gamma$ and $\langle \delta, \alpha \vee \beta\rangle$ non-Abelian. But

according to Lemma 5.19 (2), $\text{typ}(\delta, \alpha \vee \beta) \in \{\mathbf{1}, \mathbf{2}, \mathbf{5}\}$, implying that $\text{typ}(\delta, \alpha \vee \beta) = \mathbf{5}$. This concludes the proof of (3).

To prove (4), we suppose that $\alpha \in L$, $M = \alpha/\overset{s}{\sim}$, and $M/\overset{ss}{\sim}$ is a non-modular sublattice of $\mathbf{L}/\overset{ss}{\sim}$. (It is obvious that $\overset{ss}{\sim} \subseteq \overset{s}{\sim}$.) Thus we have congruences $\delta_0, \delta_1, \theta \in M$ with $\delta_0 \leq \delta_1$ and $\delta_1 \wedge (\delta_0 \vee \theta) \not\equiv \delta_0 \vee (\delta_1 \wedge \theta) \pmod{\overset{ss}{\sim}}$. There is a finite $\mathbf{F} \subseteq \mathbf{A}$ with $\delta_1' \wedge (\delta_0' \vee \theta') \not\equiv \delta_0' \vee (\delta_1' \wedge \theta') \pmod{\overset{ss}{\sim}}$ where $\delta_i' = \delta_i|_F$, $\theta' = \theta|_F$. But, clearly, $\delta_0' \overset{s}{\sim} \delta_1' \overset{s}{\sim} \theta'$; so we have in Con $\mathbf{F}$ this pentagon.

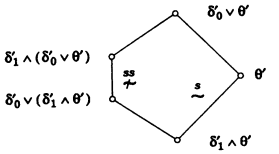


Figure 17

According to Lemma 6.5, this is impossible. □

Theorem 7.7 leads directly to our first characterizations of locally finite varieties which omit the type **1**, or the types **1** and **5**. For any classes $\mathcal{K}_0$ and $\mathcal{K}_1$ of lattices, we denote by $\mathcal{K}_1/\mathcal{K}_0$ the class of lattices $\mathbf{L}$ having a congruence θ such that $\mathbf{L}/\theta \in \mathcal{K}_1$ and every equivalence class of θ (as a sublattice of $\mathbf{L}$) belongs to $\mathcal{K}_0$. We shall prove that a locally finite variety $\mathcal{V}$ has $\mathbf{1} \notin \text{typ}\{\mathcal{V}\}$ iff $\text{CON } \mathcal{V} \subseteq \text{SD}(\wedge)/\mathit{Modular}$. We require a lattice-theoretic lemma.

LEMMA 7.8. *Let $\theta, \psi \in \text{Con } \mathbf{L}$ where $\mathbf{L}$ is a lattice, and suppose that every θ-equivalence class is a modular lattice. The lattice $\mathbf{L}' = \mathbf{L}/\psi$ has a congruence θ' such that $\mathbf{L}'/\theta'$ is a homomorphic image of $\mathbf{L}/\theta$ and every θ'-equivalence class is a modular lattice.*

PROOF. We take $\theta' = (\theta \vee \psi)/\psi$. Since

$$\mathbf{L}'/\theta' \cong \mathbf{L}/(\theta \vee \psi) \cong (\mathbf{L}/\theta)/[(\theta \vee \psi)/\theta],$$

we need only show that every equivalence class of θ' is modular. We can assume that $\theta \wedge \psi = 0_L$, since neither the hypothesis nor the desired conclusion is altered by factoring out the congruence $\theta \wedge \psi$. If the theorem is false, there must exist a pentagon $\langle a, b, c, d, e \rangle$ in $\mathbf{L}$ (as pictured below) with $a \equiv c \pmod{\theta \vee \psi}$ and $\langle e, d \rangle \notin \psi$.

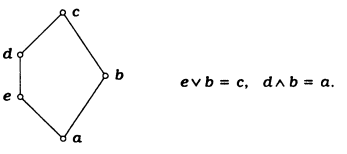


Figure 18

Since $\langle e, d\rangle \in (\theta \vee \psi) - \psi$, there must exist $e \leq e' < d' \leq d$ with $\langle e', d'\rangle \in \theta$. Thus there exists such a pentagon with $\langle e, d\rangle \in \theta$.

For any $\langle x, y\rangle \in \theta \vee \psi$, we define $\rho(x, y)$ to be the least n such that there exist $x = u_0, u_1, \ldots, u_n = y$ with $\langle u_i, u_{i+1}\rangle \in \theta \cup \psi$ for all $i < n$. In Figure 18, $\langle e, c\rangle$ and $\langle a, b\rangle$ are projective quotients, as are $\langle a, b\rangle$ and $\langle d, c\rangle$. Thus $\rho(e, c) = \rho(a, b) = \rho(d, c)$. Similarly, $\rho(a, d) = \rho(b, c) = \rho(a, e)$. Now we choose a pentagon $\langle a, b, c, d, e\rangle$ with $a \equiv c \pmod{\theta \vee \psi}$ and $\langle e, d\rangle \in \theta - \psi$, and such that $\rho(a, e) + \rho(d, c)$ is minimal for all pentagons having these properties. We shall show that $\langle d, c\rangle \in \theta$.

Clearly, there exists u with $d \leq u < c$ such that $\rho(d, c) = \rho(d, u) + 1$ and $\langle u, c\rangle \in \theta \cup \psi$.

Case 1. $\langle u, c\rangle \in \psi$. Let $z = u \wedge b$, $e' = z \vee e$, $d' = z \vee d$. Then $e' \overset{\psi}{\equiv} (c \wedge b) \vee e = c$ and $e' \overset{\theta}{\equiv} d'$. Since $e' \leq d' \leq c$, then $d' \equiv e' \pmod{\psi}$; and we have $\langle e', d'\rangle \in \theta \wedge \psi$, so $e' = d'$. Therefore $\langle a, z, e', d, e\rangle$ is a pentagon. (See Figure 19.)

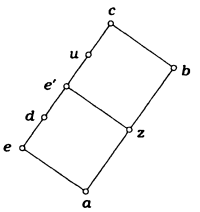


Figure 19

But $\rho(d, e') \leq \rho(d, u) = \rho(d, c) - 1$, contradicting the minimality of $\rho(a, e) + \rho(d, c)$. Thus Case 1 cannot occur.

Case 2. $\langle u, c\rangle \in \theta$. Define z, d', e' just as before. If $d' = e'$ then we have the same contradiction as before. Hence $e' < d'$. We have the pentagon $\langle z, b, c, d', e'\rangle$, pictured in Figure 20.

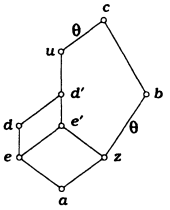


Figure 20

In this picture, $\langle a, e\rangle$ and $\langle z, e'\rangle$ are projective quotients; hence $\rho(z, e') = \rho(a, e)$. Likewise, $\langle z, b\rangle$ and $\langle d', c\rangle$ are projective and so $\langle d', c\rangle \in \theta$ and $\rho(d', c) = 1$. Now in the pentagon $\langle z, b, c, d', e'\rangle$, $\rho(z, e') + \rho(d', c) = \rho(a, e) + 1$. This implies that $\rho(d, c) = 1$, since $\rho(a, e) + \rho(d, c)$ is minimal. It follows that $\rho(d, u) = \rho(d, c) - 1 = 0$ and $d = u$. Thus, $\langle d, c\rangle \in \theta$, as was claimed.

By a dual argument, $\langle a, e\rangle \in \theta$. Thus the pentagon $\langle a, \ldots, e\rangle$ lies entirely inside the class a/θ. This contradicts our assumption that a/θ is a modular sublattice of L; and finishes our proof of the lemma. □

THEOREM 7.9. *For any locally finite variety $\mathcal{V}$, the following are equivalent:*

(1) $\mathbf{1} \notin \mathrm{typ}\{\mathcal{V}\}$.

(2) $\mathbf{D}_1 \notin \boldsymbol{S}(\mathrm{CON}\ \mathcal{V})$.

(3) $\mathrm{CON}\ \mathcal{V} \subseteq \mathrm{SD}(\wedge)/\mathit{Modular}$.

PROOF. That (2) implies (1) is implied by Theorem 6.22 (1).

To prove that (1) implies (2), suppose that $\mathbf{D}_1 \in \boldsymbol{S}(\mathrm{CON}\ \mathcal{V})$. Thus we have congruences of an algebra $\mathbf{A} \in \mathcal{V}$ forming a sublattice of $\mathbf{Con}\ \mathbf{A}$ as pictured in Figure 21.

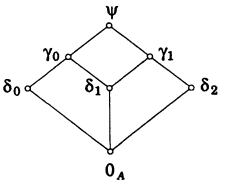


Figure 21

(We can certainly assume that the least element of the copy of $\mathbf{D}_1$ is the least congruence of $\mathbf{A}$.) Let $\langle a, b\rangle \in \delta_1$, $a \neq b$, and choose a finite algebra $\mathbf{B} \subseteq \mathbf{A}$ such that $\{a, b\} \subseteq B$ and $\langle a, b\rangle \in \delta_0|_B \vee \delta_2|_B$. The congruences 0_B, $\delta_0' = \delta_0|_B$, $\delta_2' = \delta_2|_B$, $\gamma_0' = \delta_0' \vee \Theta_{\mathbf{B}}(a, b)$, $\gamma_1' = \delta_2' \vee \Theta_{\mathbf{B}}(a, b)$, $\delta_1' = \gamma_0' \wedge \gamma_1'$, $\psi' = \delta_0' \vee \delta_2'$ constitute a sublattice of $\mathbf{Con}\ \mathbf{B}$ isomorphic to $\mathbf{D}_1$, as can readily be verified. Thus by Lemma 6.4, we have that $\mathbf{1} \in \mathrm{typ}\{\mathbf{B}\}$; whence $\mathbf{1} \in \mathrm{typ}\{\mathcal{V}\}$.

To see that (1) implies (3), assume that $\mathbf{1} \notin \mathrm{typ}\{\mathcal{V}\}$. By Theorem 7.2, and Definition 7.3, we have that $\overset{ss}{\sim}$ is the identity relation on $\mathbf{Con}\ \mathbf{A}$ whenever $\mathbf{A}$ is a finite algebra in $\mathcal{V}$. By Corollary 7.5, this holds also when $\mathbf{A}$ is infinite. Thus by Theorem 7.7, $\mathbf{Con}\ \mathbf{A} \in \mathrm{SD}(\wedge)/\mathit{Modular}$ for all $\mathbf{A} \in \mathcal{V}$.

Finally, we show that if (1) fails then (3) fails. Suppose that $\mathbf{1} \in \mathrm{typ}\{\mathcal{V}\}$. By Theorem 6.19 (1), there exists a finite algebra $\mathbf{B} \in \mathcal{V}$ and $\theta \in \mathrm{Con}\ \mathbf{B}$ and a homomorphism of $I[0_B, \theta]$ onto $\mathbf{\Pi}_4$ (the lattice of all equivalence relations on a four-element set). The lattice $\mathbf{\Pi}_4$ is simple and non-modular, and does not belong to $\mathrm{SD}(\wedge)$.

Hence $\mathbf{\Pi}_4 \notin \mathrm{SD}(\wedge)/\mathcal{M}odular$. Since the class of finite lattices in $\mathrm{SD}(\wedge)$ is closed under homomorphisms, it follows from Lemma 7.8 that $I[0_B, \theta]$ does not belong to $\mathrm{SD}(\wedge)/\mathcal{M}odular$. Thus $\mathbf{Con\ B} \notin \mathrm{SD}(\wedge)/\mathcal{M}odular$. □

THEOREM 7.10. *For any locally finite variety $\mathcal{V}$ the following are equivalent.*

(1) $\mathrm{typ}\{\mathcal{V}\} \cap \{\mathbf{1,5}\} = \emptyset$.
(2) $\mathbf{D}_2 \notin \boldsymbol{S}(\mathrm{CON}\ \mathcal{V}_{fin})$.
(3) $\mathrm{CON}\ \mathcal{V}_{fin} \subseteq \mathrm{SD}(\vee)/\mathcal{M}odular$.

PROOF. The equivalence of (1) and (2) is by Theorem 6.22 (2). That (1) implies (3) is by Theorem 7.7. If (1) fails, then by Theorem 6.19, either $\mathbf{\Pi}_4$, or the congruence lattice $\mathbf{L}$ of the semilattice $\mathbf{S}_3 \times \mathbf{S}_3$ (where $\mathbf{S}_3 = \langle\{0,1,2\}, \wedge\rangle$), is in $\boldsymbol{HS}(\mathbf{Con\ A})$ for some finite $\mathbf{A} \in \mathcal{V}$. It can be shown, with some effort, that neither $\mathbf{L}$ nor $\mathbf{\Pi}_4$ is in $\mathrm{SD}(\vee)/\mathcal{M}odular$. Thus it follows, as in the proof of Theorem 7.9, that (3) fails if (1) does. □

The properties "$\mathrm{CON}\ \mathcal{V} \subseteq \mathrm{SD}(\wedge)$," "$\mathrm{CON}\ \mathcal{V}_{fin} \subseteq \mathrm{SD}(\vee)$," of a variety $\mathcal{V}$ can be characterized in an analogous fashion, using Theorem 6.22 and Theorem 7.7. These results are contained in Exercises 7.13 (3–4), and will be incorporated into the theorems in Chapter 9. There is another characterization of the family of locally finite varieties omitting type **1**, which is quite interesting in its own right and will become a useful tool in Chapter 9. This is Theorem 7.12, the proof of which requires a result contained in the next theorem.

THEOREM 7.11. *Let $\mathcal{V}$ be any locally finite variety.*

(1) $\mathrm{typ}\{\mathcal{V}\} \subseteq \{\mathbf{1}\}$ *iff every algebra in $\mathcal{V}$ is locally strongly solvable.*
(2) $\mathrm{typ}\{\mathcal{V}\} \subseteq \{\mathbf{1,2}\}$ *iff every algebra in $\mathcal{V}$ is locally solvable.*
(3) $\mathrm{typ}\{\mathcal{V}\} \subseteq \{\mathbf{2}\}$ *iff $\mathcal{V}$ has permuting congruences and every algebra in $\mathcal{V}$ is locally solvable.*

PROOF. Statements (1) and (2) follow from Theorem 7.2, Definition 7.3, and Corollary 7.5.

To prove (3), suppose first that $\mathcal{V}$ has permuting congruences and its algebras are locally solvable. Then $\mathrm{CON}\ \mathcal{V} \subseteq \mathcal{M}odular \subseteq \mathrm{SD}(\wedge)/\mathcal{M}odular$, implying that $\mathbf{1} \notin \mathrm{typ}\{\mathcal{V}\}$ by Theorem 7.9. Then by 7.11 (2), we have that $\mathrm{typ}\{\mathcal{V}\} \subseteq \{\mathbf{2}\}$. Now suppose, conversely, that $\mathrm{typ}\{\mathcal{V}\} \subseteq \{\mathbf{2}\}$. For every $\mathbf{A} \in \mathcal{V}$, $\overset{ss}{\sim}$ is the identity relation on $\mathrm{Con}\ \mathbf{A}$ and $\overset{s}{\sim}$ is the universal relation. Therefore $\mathcal{V}$ is congruence modular, by Theorem 7.7. In H. P. Gumm [16], it is proved that every solvable algebra in a congruence modular variety has permuting congruences. The finite algebra $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z)$, the free algebra in $\mathcal{V}$ on three generators, is solvable. Hence $\mathbf{F}$, and therefore every algebra in $\mathcal{V}$, has permuting congruences. (See the proof of Theorem 0.3 (3).) □

THEOREM 7.12. *For any locally finite variety $\mathcal{V}$, the following are equivalent.*

(1) $\mathbf{1} \notin \text{typ}\{\mathcal{V}\}$.

(2) *There exists a term $p(x,y,z)$ in the language of $\mathcal{V}$ such that the equation $p(x,x,x) \approx x$ holds in $\mathcal{V}$ and for every $\mathbf{A} \in \mathcal{V}$ and $\theta \in \text{Con } \mathbf{A}$: if $\theta \overset{s}{\sim} 0_A$ and $\langle a,b \rangle \in \theta$ then $p(a,b,b) = a$ and $p(a,a,b) = b$.*

(3) *For every $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta \in \text{Con } \mathbf{A}$, if $\alpha \overset{s}{\sim} \beta$ then $\alpha \circ \beta = \beta \circ \alpha$.*

PROOF. Suppose that (3) holds. Then for $\mathbf{A} \in \mathcal{V}$, we have that every equivalence class of $\overset{s}{\sim}$ on Con $\mathbf{A}$ consists of commuting equivalence relations. Consequently, these equivalence classes are modular lattices. Then $\mathbf{Con}\ \mathbf{A} \in \text{SD}(\wedge)/\mathcal{M}odular$, by Theorem 7.7. Hence $\mathbf{1} \notin \text{typ}\{\mathcal{V}\}$, by Theorem 7.9; and we conclude that (3) implies (1).

Now to show that (2) implies (3), let $\mathbf{A} \in \mathcal{V}$, let $\alpha, \beta \in \text{Con } \mathbf{A}$, and assume that $\alpha \overset{s}{\sim} \beta$. Then $\nu \overset{s}{\sim} \mu$ where $\nu = \alpha \wedge \beta$, $\mu = \alpha \vee \beta$. By the result of Exercise 7.13 (2), we have $\mu/\nu \overset{s}{\sim} 0$ in Con $(\mathbf{A}/\nu)$. Now suppose that $\langle a,b \rangle \in \alpha$ and $\langle b,c \rangle \in \beta$. Let $p(x,y,z)$ be the term supplied by statement (2), and let $u = p(a,b,c)$. In $\mathbf{A}/\nu$ We have

$$p(a/\nu, a/\nu, c/\nu) = c/\nu \text{ and}$$
$$p(a/\nu, c/\nu, c/\nu) = a/\nu$$

since $\langle a/\nu, c/\nu \rangle \in \mu/\nu$. This means that $p(a,a,c) \equiv c \pmod{\nu}$ and $p(a,c,c) \equiv a \pmod{\nu}$. Thus

$$u \overset{\alpha}{\equiv} p(a,a,c) \overset{\nu}{\equiv} c,$$

implying that $\langle u,c \rangle \in \alpha$; and in a similar fashion we obtain that $\langle a,u \rangle \in \beta$. These considerations imply that $\alpha \circ \beta \subseteq \beta \circ \alpha$, and from this it follows that $\alpha \circ \beta = \beta \circ \alpha$.

The proof that (1) implies (2) uses several nontrivial results already proved. Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x,y)$, let $\mu = \Theta(x,y)$ in $\mathbf{F}$, let ν be the smallest congruence in the equivalence class $\mu/\overset{s}{\sim}$ (see Theorem 7.7), and let $\mathbf{A} = \mathbf{F}/\nu$. We assume that $\mathbf{1} \notin \text{typ}\{\mathcal{V}\}$. Let $e = \text{id}_A \in \text{E}(\mathbf{A})$, $U = A = e(A)$, $\beta = \mu/\nu \in \text{Con } \mathbf{A}$, $\bar{x} = x/\nu$, $\bar{y} = y/\nu$, and $S = \bar{x}/\beta$. By Theorem 6.17, we have that $\text{typ}\{\, \boldsymbol{V}(\mathbf{AI}_S)\, \} \subseteq \text{typ}\{\mathcal{V}\}$, so that $\mathbf{1} \notin \text{typ}\{\, \boldsymbol{V}(\mathbf{AI}_S)\, \}$. Also, the algebra $\mathbf{AI}_S$ is solvable. In fact, β is solvable, from its definition, which yields the existence of a chain of congruences

$$0 = \beta_0 \leq \beta_1 \leq \cdots \leq \beta_n = \beta$$

such that each quotient $\langle \beta_i, \beta_{i+1} \rangle$ is Abelian. It is easy to see that the chain

$$0 = \beta_0|_S \leq \cdots \leq \beta_n|_S = 1_S$$

of congruences of $\mathbf{AI}_S$ also has each of its quotients $\langle \beta_i|_S, \beta_{i+1}|_S \rangle$ Abelian. Now since $\mathbf{AI}_S$ is solvable, the variety $\boldsymbol{V}(\mathbf{AI}_S)$ consists of locally solvable algebras (see Corollary

7.6); and since this variety omits the type **1**, then it follows by Theorem 7.11 that it is a variety in which congruences permute. Hence there exists a Mal'cev operation $f \in \mathrm{Clo}_3(\mathbf{A}\mathrm{I}_S)$. (See Theorem 0.3(3).) This operation f is the restriction of a polynomial operation of $\mathbf{A}$, which in turn is induced by some polynomial operation h of $\mathbf{F}$, where h can be expressed in the form

$$h(r,s,t) = q(x,y,r,s,t) \quad \text{for all} \quad r,\ s,\ t \in F$$

for a certain 5-ary term q in the language of $\mathcal{V}$ and where x, y are the free generators of $\mathbf{F}$.

We know that $(h_\nu)|_S$ is Mal'cev. Since $\bar{x}, \bar{y} \in S$, it follows that

$$\begin{aligned} x &\equiv q(x,y,x,y,y) \pmod{\nu} \\ y &\equiv q(x,y,x,x,y) \pmod{\nu}\,. \end{aligned} \tag{7.12.1}$$

We now define $p(u,v,w) = q(u,w,u,v,w)$. It remains to prove that the term p has the desired properties. Observe that the congruences (7.12.1) can be written as

$$\begin{aligned} x &\equiv p(x,y,y) \pmod{\nu} \\ y &\equiv p(x,x,y) \pmod{\nu}\,. \end{aligned} \tag{7.12.2}$$

Let $\mathbf{B} \in \mathcal{V}$ and let $\theta \in \mathrm{Con}\,\mathbf{B}$ with $\theta \overset{s}{\sim} 0_B$ and let $\langle a,b\rangle \in \theta$. Then define $\varphi : \mathbf{F} \to \mathbf{B}$ to be the homomorphism satisfying $\varphi(x) = a$, $\varphi(y) = b$. It follows directly from the definition of $\overset{s}{\sim}$, and from the equivalence $\theta \overset{s}{\sim} 0_B$, that $\varphi^{-1}(0_B) \overset{s}{\sim} \varphi^{-1}(\theta)$. We have $\langle x,y\rangle \in \varphi^{-1}(\theta)$, hence $\mu \le \varphi^{-1}(\theta)$, and so

$$\mu = \mu \wedge \varphi^{-1}(\theta) \overset{s}{\sim} \mu \wedge \varphi^{-1}(0_B).$$

From the definition of ν, it follows that $\nu \le \mu \wedge \varphi^{-1}(0_B)$; equivalently, $\nu \subseteq \ker\varphi$. The congruence formulas (7.12.2) then imply the desired equations in $\mathbf{B}$, namely $p(a,b,b) = a$ and $p(a,a,b) = b$. Taking $\theta = 0_B$ and $a = b$, we obtain also that $p(b,b,b) = b$ for all $b \in \mathbf{B}$. □

In [16] on page 54, a proof is presented showing that in a congruence modular variety, every solvable congruence permutes with any congruence. We have an analogue of that result.

COROLLARY 7.13. *Let $\mathcal{V}$ be a locally finite variety with $\mathbf{1} \notin \mathrm{typ}\{\mathcal{V}\}$. Let $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$. If $\alpha \overset{s}{\sim} 1$ or $\beta \overset{s}{\sim} 0$ (or, more generally, if $\beta \overset{s}{\sim} \alpha \wedge \beta$) then $\alpha \vee \beta = \alpha \circ \beta \circ \alpha$.*

PROOF. By factoring the algebra modulo $\alpha \wedge \beta$, we reduce our task to deriving the desired conclusion under the assumption that $\beta \overset{s}{\sim} 0_A$. Then, letting $p(x,y,z)$ be a

term as in Theorem 7.12 (2), we proceed to prove that $\beta \circ \alpha \circ \beta \subseteq \alpha \circ \beta \circ \alpha$. Suppose that

$$a \overset{\beta}{\equiv} b \overset{\alpha}{\equiv} c \overset{\beta}{\equiv} d.$$

Then $a = p(a, b, b)$ and $p(c, c, d) = d$, by Theorem 7.12 (2), since $\beta \overset{s}{\sim} 0_A$. Thus

$$a = p(a, b, b) \overset{\alpha}{\equiv} p(a, b, c) \overset{\beta}{\equiv} p(b, b, d) \overset{\alpha}{\equiv} p(c, c, d) = d.$$

Now from $\beta \circ \alpha \circ \beta \subseteq \alpha \circ \beta \circ \alpha$, it is easy to prove inductively that $(\alpha \circ \beta)^n \subseteq \alpha \circ \beta \circ \alpha$ for all n; and this implies that $\alpha \vee \beta = \alpha \circ \beta \circ \alpha$. □

Exercises 7.14

(1) Let $\mathbf{A}$ be a locally finite algebra and α be its largest locally solvable congruence. Prove that $\mathbf{A}/\alpha$ is isomorphic to a subdirect product of subdirectly irreducible algebras whose monoliths are non-Abelian. (The *monolith* of a subdirectly irreducible algebra is its smallest non-zero congruence.)

(2) Let $\mathbf{A}$ be locally finite, $\delta \leq \theta$ in Con $\mathbf{A}$. Show that $\delta \overset{s}{\sim} \theta$ iff $0 \overset{s}{\sim} \theta/\delta$ in Con $(\mathbf{A}/\delta)$.

(3) For a locally finite variety $\mathcal{V}$, show that $\text{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{2}\} = \emptyset$ iff CON $\mathcal{V} \subseteq$ SD($\wedge$) iff $\mathbf{M}_3 \notin \boldsymbol{S}(\text{CON } \mathcal{V})$. (See Theorem 6.22.)

(4) For a locally finite variety $\mathcal{V}$, show that $\text{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{2}, \mathbf{5}\} = \emptyset$ iff CON $\mathcal{V}_{fin} \subseteq$ SD($\vee$).

(5) Show that the variety of semilattices has meet semi-distributive congruence lattices. (Use Exercise 3.)

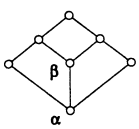
(6) Show that if $\mathcal{V}$ is any variety of lattices, then $\mathcal{V}/\mathcal{M}odular$ is a variety. (Use Lemma 7.8.)

(7) Show that Lemma 7.8 remains true when the word "modular" is replaced everywhere by the word "distributive". Conclude that $\mathcal{V}/\mathcal{D}istributive$ is a variety whenever $\mathcal{V}$ is a variety of lattices.

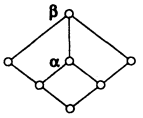
(8) Show that each of the classes SD($\wedge$)/$\mathcal{M}odular$ and SD($\vee$)/$\mathcal{M}odular$ is closed under the formation of products, sublattices, and homomorphic images of finite lattices.

(9) Let $\mathbf{A}$ be a finite algebra. Prove:

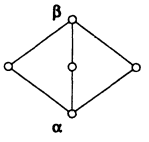
(i) If the sublattice pictured below occurs in **Con A** then $\text{typ}\{\alpha, \beta\} \subseteq \{\mathbf{1}, \mathbf{2}\}$, and $\langle \alpha, \beta \rangle$ is Abelian. (Note that $\langle \alpha, \beta \rangle$ is Abelian even if $\mathbf{A}$ is infinite.)



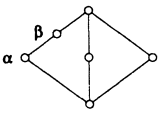
(ii) If the sublattice pictured below occurs in **Con A** and $\langle \alpha, \beta \rangle$ is not solvable then $\mathbf{5} \in \text{typ}\{\alpha, \beta\}$. (Use the congruence $\overset{s}{\sim}$ and Lemma 5.19.)



(iii) If this sublattice occurs in **Con A** then $\text{typ}\{\alpha, \beta\} \subseteq \{\mathbf{1}, \mathbf{2}\}$.



(iv) If this sublattice occurs in **Con A** then $\text{typ}\{\alpha, \beta\} = \{\mathbf{1}\}$. (Use the last statement and Lemma 6.5.)



(10) Let $\mathcal{V}$ be any variety (possibly not locally finite). Prove that (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii).
   (i) CON $\mathcal{V} \subseteq$ SD($\vee$)
   (ii) Algebras in $\mathcal{V}$ have no non-zero Abelian congruences.
   (iii) CON $\mathcal{V} \subseteq$ SD($\wedge$). (See Exercise 6.23 (12).)

(11) Theorem 7.7 (2) implies that there are lattices such that any locally finite algebra that has its congruence lattice isomorphic to one of them must be locally solvable.
   (i) Show that if **A** is a locally finite algebra where **Con A** satisfies

$$1 = \bigvee \{x : \bigvee \{y : x \wedge y = 0\} = 1\},$$

   then **A** is locally solvable.
   (ii) Show that if **A** is a locally finite algebra and **Con A** is simple and does not satisfy SD($\wedge$), then **A** is locally solvable.

8. CONGRUENCE MODULAR VARIETIES

The two broad families of congruence-modular varieties and congruence-distributive varieties are rather familiar to universal algebraists and fairly well understood. The tame congruence theory becomes somewhat simpler in these varieties, and it can be used to obtain results that seem inaccessible to conventional methods. We first recall the most recent characterization of congruence-modular varieties, and the classical characterization of congruence-distributive varieties.

THEOREM 8.1. *(Gumm [16]) A variety $\mathcal{V}$ is congruence-modular iff for some $n \geq 0$ there are terms $d_0(x,y,z), \ldots, d_n(x,y,z)$, $p(x,y,z)$ in its language such that these equations hold in $\mathcal{V}$.*

(1) $d_0(x,y,z) \approx x$, $d_i(x,y,x) \approx x$ *for* $1 \leq i \leq n$.
(2) $d_i(x,y,y) \approx d_{i+1}(x,y,y)$ *for even* $i < n$.
(3) $d_i(x,x,y) \approx d_{i+1}(x,x,y)$ *for odd* $i < n$.
(4) $d_n(x,y,y) \approx p(x,y,y)$, $p(x,x,y) \approx y$.

THEOREM 8.2. *(Jónsson [19]) A variety $\mathcal{V}$ is congruence-distributive iff for some $n \geq 0$ there are terms $d_0(x,y,z), \ldots, d_n(x,y,z)$ in its language satisfying the equations 8.1 (1–3) and $d_n(x,y,z) \approx z$.*

It is a reasonable exercise to prove the theorem of Jónsson. The theorem of Gumm is not so easily proved. These two theorems make it appear that for varieties, congruence-modularity is an amalgam of congruence-distributivity and congruence-permutability.

The next lemma introduces an idea that will be frequently used in Chapter 9. See Definition 6.12 for the notation $\mathbf{AI}_S$.

LEMMA 8.3. *Let $\mathbf{A}$ be an algebra, $e \in \mathrm{E}(\mathbf{A})$, $U = e(A)$, $\beta \in \mathrm{Con}\,\mathbf{A}$, and $S = a/\beta \cap U$ for some $a \in U$. If $\boldsymbol{V}(\mathbf{A})$ is congruence-modular, congruence-distributive, or has permuting congruences, then $\boldsymbol{V}(\mathbf{AI}_S)$ has the same respective property.*

PROOF. If $\boldsymbol{V}(\mathbf{A})$ is congruence-permutable, then there is a Mal'cev operation $p \in \mathrm{Clo}_3\mathbf{A}$, by Theorem 0.3 (3). The operation $p'(x,y,z) = e(p(x,y,z))$, restricted to S, is Mal'cev and belongs to $\mathrm{Clo}_3(\mathbf{AI}_S)$. To see this, let $x,y,z \in S$. Then $p'(x,y,z) \in U$, obviously, and

$$p'(x,y,z) \equiv p'(a,a,a) = e(a) = a (\mathrm{mod}\ \beta),$$

so $p'(x,y,z) \in S$. Moreover,

$$p'(x,y,y) = e(p(x,y,y)) = e(x) = x,$$

and likewise $p'(x,x,y) = y$. Thus $\boldsymbol{V}(\mathbf{AI}_S)$ is congruence-permutable.

If $\boldsymbol{V}(\mathbf{A})$ is congruence-distributive, then we have $d_0, \dots, d_n \in \mathrm{Clo}_3\mathbf{A}$ satisfying Jónsson's equations of Theorem 8.2. These equations imply $d_i(x,x,x) \approx x$ for $i = 0, \dots, n$. Thus we see that the operations $d_i'(x,y,z) = e(d_i(x,y,z))$, restricted to S, belong to $\mathrm{Clo}_3(\mathbf{AI}_S)$. Since the Jónsson equations are linear (having no superposition of one operation applied to the results of operations), we can easily check that these equations are satisfied by $d_0', \dots, d_n'$. Thus $\boldsymbol{V}(\mathbf{AI}_S)$ is congruence-distributive.

The argument for modularity is very similar. All these arguments require the idempotence of the operations in the characteristic equations, and the linearity of these equations. □

COROLLARY 8.4. *Let $\mathcal{V}$ be a locally finite variety and $\mathbf{k} \in \{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4},\mathbf{5}\}$. If $\mathbf{k} \in \mathrm{typ}\{\mathcal{V}\}$ and $\mathcal{V}$ is congruence-modular, distributive, or permutable, then there is a minimal algebra $\mathbf{M}$ of type $\mathbf{k}$ such that $\boldsymbol{V}(\mathbf{M})$ has the same respective congruence property.*

PROOF. Suppose, for example, that $\mathcal{V}$ is congruence-distributive and $\mathbf{k} \in \mathrm{typ}\{\mathcal{V}\}$. There is a finite $\mathbf{A} \in \mathcal{V}$ and $\alpha \prec \beta$ in $\mathrm{Con}\,\mathbf{A}$ with $\mathrm{typ}(\alpha,\beta) = \mathbf{k}$. We choose $U \in \mathrm{M}_{\mathbf{A}}(\alpha,\beta)$ and a trace $N = U \cap a/\beta$ with $a \in U$. By Lemma 8.3, $\boldsymbol{V}(\mathbf{AI}_N)$ is congruence-distributive. The algebra $\mathbf{M} = (\mathbf{AI}_N)/(\alpha|_N)$ is a minimal algebra of type $\mathbf{k}$ in this variety. □

THEOREM 8.5. *A locally finite variety $\mathcal{V}$ is congruence-modular iff $\mathrm{typ}\{\mathcal{V}\} \cap \{\mathbf{1},\mathbf{5}\} = \emptyset$ and for all finite $\mathbf{A} \in \mathcal{V}$, $\alpha \prec \beta$ in $\mathrm{Con}\,\mathbf{A}$, and $U \in \mathrm{M}_{\mathbf{A}}(\alpha,\beta)$, the $\langle\alpha,\beta\rangle$-tail of U is empty.*

PROOF. Let $\mathcal{V}$ be a locally finite congruence-modular variety. Let $\mathbf{A}$ be any finite algebra in $\mathcal{V}$ with $0 \prec \beta$ in $\mathrm{Con}\,\mathbf{A}$. (By Lemma 2.18 and Corollary 5.3, it will suffice to consider only this case.) Choose any $U \in \mathrm{M}_{\mathbf{A}}(0,\beta)$, and let N be a $\langle 0,\beta\rangle$-trace in U and B be the body of U. By the proof of Lemma 8.3, there are

$$d_0(x,y,z), \dots, d_n(x,y,z), p(x,y,z) \in \mathrm{Pol}_3\mathbf{A}$$

such that U and N are closed under these operations and, restricted to U, they satisfy the equations 8.1 (1–4). The algebra $\mathbf{A}|_N$ cannot be unary or equivalent to a semilattice, since in either case it could not have polynomial operations satisfying those equations. Thus $\mathrm{typ}(0,\beta) \notin \{\mathbf{1},\mathbf{5}\}$.

In proving that $B = U$, we can assume that $U = A$. We suppose now that $B \neq A$, say $t \in A - B$, and we proceed to a contradiction. Let a and c be any elements of N.

For all i, $0 \leq i \leq n$, the function $f_i(x) = d_i(a, x, c)$ satisfies

$$f_i(t) \overset{\beta}{\equiv} d_i(a, t, a) = a.$$

Therefore $f_i(t) \in B$, $f_i \notin \text{Sym } A$ (else $f_i^{-1}(B) = B$), and f_i must be constant on N. (Since $A = U$ is $\langle 0, \beta \rangle$-minimal.) Now we can prove inductively that $d_i(a, b, c) = a$ for all $i \leq n$ and $a, b, c \in N$. This is true for $i = 0$, and if it holds for $i = j < n$, then

$$d_{j+1}(a, b, c) = d_{j+1}(a, c, c) = d_j(a, c, c) = a$$

if j is even, and

$$d_{j+1}(a, b, c) = d_{j+1}(a, a, c) = d_j(a, a, c) = a$$

if j is odd. Now we have $p(a, b, b) = d_n(a, b, b) = a$ for all $a, b \in N$; and $p(u, u, v) = v$ for all $u, v \in A$.

Proceeding as in the proof of Lemma 4.20, we now construct another polynomial operation of $\mathbf{A}$. Let $h(x, y) = p(x, y, y)$, and choose $k > 1$ such that $h^k_{(0)}(x, y) = h(\ldots(h(x, y), y), \ldots, y)$ satisfies $h^k_{(0)}(h^k_{(0)}(x, y), y) = h^k_{(0)}(x, y)$. Since $h_b(x) = h(x, b)$ is a permutation for $b \in N$ (in fact $h_b(a) = a$ for $a, b \in N$), it follows that $h^k_{(0)}(x, b) = x$ for all $x \in A$ and $b \in N$. We set $p'(x, y, z) = h^{k-1}_{(0)}(p(x, y, z), z)$; and observe that $p'(x, b, b) = h^k_{(0)}(x, b) = x$ when $x \in A$ and $b \in N$, and that $p'(x, x, y) = y$ for all $x, y \in A$.

Now we choose $a \in N$, let $t \in A - B$ as before, and define, for all $x \in A$,

$$g(x) = p'(x, p'(t, p'(t, x, a), a), a).$$

For any $b \in N$,

$$p'(t, b, a) \overset{\beta}{\equiv} p'(t, a, a) = t,$$

implying that $p'(t, b, a) = t$ since $t \notin B$. Thus $g(b) = b$, for $b \in N$, and we have that $g \in \text{Sym } A$. On the other hand, $g(t) = a$ can be calculated, using the equations from the end of the last paragraph. This contradicts that g must leave $A - B$ fixed, and the contradiction ends our proof that $U = B$.

To finish the proof of the theorem, we now assume that $\mathcal{V}$ is locally finite and not congruence-modular. There is a finite algebra $\mathbf{A} \in \mathcal{V}$ with $\mathbf{Con}\ \mathbf{A} = \mathbf{L}$ a non-modular lattice; for example, we can take $\mathbf{A} = \mathbf{F}_{\mathcal{V}}(4)$. By Lemma 6.1, there must exist a prime quotient $\langle \alpha, \beta \rangle$ in $\mathbf{L}$ and $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ such that for $\mathbf{U} = \mathbf{A}|_U$, we have $\mathbf{Con}\ \mathbf{U}$ non-modular. This implies that either the $\langle \alpha, \beta \rangle$-tail of U is non-empty, or else $\text{typ}(\alpha, \beta) \in \{\mathbf{1}, \mathbf{5}\}$. Otherwise, by Lemma 4.17 and Lemma 4.20, either $|U| = 2$ or $\mathbf{U}$ is a Mal'cev algebra; but in either case, $\mathbf{Con}\ \mathbf{U}$ would be a modular lattice. □

THEOREM 8.6. *A locally finite variety $\mathcal{V}$ is congruence-distributive iff* $\text{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{2}, \mathbf{5}\} = \emptyset$ *and for all finite $\mathbf{A} \in \mathcal{V}$, $\alpha \prec \beta$ in* Con $\mathbf{A}$, *and $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, we have $|U| = 2$.*

PROOF. Let $\mathcal{V}$ be a locally finite congruence-distributive variety. By Corollary 8.4, $\text{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{2}, \mathbf{5}\} = \emptyset$. Since $\mathcal{V}$ is congruence-modular, the previous theorem implies that in $\mathcal{V}$ every $\langle \alpha, \beta \rangle$-minimal set U is equal to its body, and since $\text{typ}(\alpha, \beta)$ must be **3** or **4**, Lemma 4.17 implies that $|U| = 2$.

Conversely, if $\mathcal{V}$ is locally finite and the $\langle \alpha, \beta \rangle$-minimal sets in $\mathcal{V}$ are 2-element sets, then Lemma 6.1 provides a subdirect representation of $\mathbf{Con}\ \mathbf{A}$ (for $\mathbf{A}$ finite in $\mathcal{V}$) in a product of two-element lattices, and from this it follows that $\mathcal{V}$ is congruence-distributive. □

The combination of Theorem 8.5 and Lemma 6.1 yields an interesting representation of the congruence lattices of finite algebras belonging to congruence-modular varieties, which is the content of the next theorem. Let $\mathbf{A}$ be a finite algebra in a congruence-modular variety. For any prime quotient $\langle \alpha, \beta \rangle$ in $\mathbf{A}$ and $\langle \alpha, \beta \rangle$-minimal set U, the algebra $\mathbf{A}|_U$ is either equivalent to a two-element bounded lattice or Boolean algebra, or it is a nilpotent Mal'cev algebra. (See Theorem 8.5, Lemmas 4.17, 4.20 and 4.36, and Theorem 4.31.) These algebras $\mathbf{A}|_U$ are E-minimal; and a complete description of all E-minimal Mal'cev algebras will be supplied in Theorem 13.9.

Quasigroups are defined right before Lemma 4.6. A **loop** is a quasigroup $\langle A, \cdot \rangle$ having an element 1 such that $1 \cdot x = x \cdot 1 = x$ for all elements x. A **loop with operators** is an algebra, one of whose basic operations is the operation of a loop.

THEOREM 8.7. *Let* $\mathbf{A}$ *be a finite algebra such that* $\boldsymbol{V}(\mathbf{A})$ *is congruence-modular. There exist finite algebras* $\mathbf{B}, \mathbf{B}_1, \ldots, \mathbf{B}_n$, *each a loop with operators, such that* $\mathbf{B}_1, \ldots, \mathbf{B}_n$ *are nilpotent and* E*-minimal, and*

$$\mathbf{Con}\ \mathbf{A} \cong \mathbf{Con}\ \mathbf{B} \overset{sd}{\hookrightarrow} \prod_1^n \mathbf{Con}\ \mathbf{B}_i.$$

PROOF. We take $\langle \alpha_1, \beta_1 \rangle, \ldots, \langle \alpha_n, \beta_n \rangle$ to be a list of all the prime quotients in $\mathbf{Con}\ \mathbf{A}$. Let $B_i \in \mathrm{M}_{\mathbf{A}}(\alpha_i, \beta_i)$ for $i = 1, \ldots, n$ and put $B = \prod_1^n B_i$. For each i, choose $1_i \in B_i$. If B_i is a two-element set, let $x \cdot_i y$ be the operation of a group on B_i with identity element 1_i. If $|B_i| > 2$ then since B_i equals its $\langle \alpha_i, \beta_i \rangle$-body and $\text{typ}(\alpha_i, \beta_i) \notin \{\mathbf{1}, \mathbf{5}\}$, we have $\text{typ}(\alpha_i, \beta_i) = \mathbf{2}$; in this case choose an operation $d_i(x, y, z) \in \mathrm{Pol}_3 \mathbf{A}|_{B_i}$ satisfying the properties of Lemma 4.20, and put $x \cdot_i y = d_i(x, 1_i, y)$ for $x, y \in B_i$. By Lemma 4.20, $\langle B_i, \cdot_i \rangle$ is a loop for $i = 1, \ldots, n$; and $\mathrm{Con}\ \langle B_i, \cdot_i \rangle \supseteq \mathrm{Con}\ \mathbf{A}|_{B_i}$. Let $x \cdot y$ be the binary operation on B such that $\langle B, \cdot \rangle = \prod_1^n \langle B_i, \cdot_i \rangle$.

Now for $i = 1, \ldots, n$, if $|B_i| > 2$ let $\mathbf{B}_i = \langle B_i, \cdot_i, \ldots \rangle$ have for its basic operations $x \cdot_i y$ and the members of $\mathrm{Pol}_1 \mathbf{A}|_{B_i}$. If $|B_i| = 2$, let $\mathbf{B}_i = \langle B_i, \cdot_i \rangle$. By Theorem 4.31 and Lemma 4.36, when $|B_i| > 2$ the algebra $\mathbf{A}|_{B_i}$ is nilpotent. Since $\mathrm{Con}\ \mathbf{B}_i = \mathrm{Con}\ \mathbf{A}|_{B_i}$ and $\mathrm{Pol}\ \mathbf{B}_i \subseteq \mathrm{Pol}\ \mathbf{A}|_{B_i}$, it follows that $\mathbf{B}_i$ is nilpotent and E-minimal. When $|B_i| = 2$, it is obvious that the Abelian group $\mathbf{B}_i$ is nilpotent, and that $\mathrm{Con}\ \mathbf{B}_i = \mathrm{Con}\ \mathbf{A}|_{B_i}$.

By Lemma 6.1, the mapping $\theta \mapsto \langle \theta|_{B_i} : 1 \leq i \leq n \rangle$ is a subdirect embedding of $\mathbf{Con}\ \mathbf{A}$ into $\prod_1^n \mathbf{Con}\ \mathbf{B}_i$.

To construct the basic operations of $\mathbf{B}$ (besides $x \cdot y$), we define for $1 \leq i, j \leq n$

$$M_{i,j} = \{f : \text{for some } g \in \ \mathrm{Pol}_1\mathbf{A}, f = g|_{B_i} \text{ and } f(B_i) \subseteq B_j\}.$$

We define Σ to be the set of all sequences $\sigma = \langle \sigma_1, \ldots, \sigma_n \rangle$ where for all $j \in \{1, \ldots, n\}$ there is an i such that $\sigma_j \in M_{i,j}$. For each $\sigma \in \Sigma$, we define a function $f_\sigma \in B^B$ by

$$f_\sigma(\langle b_1, \ldots, b_n \rangle) = \langle \sigma_1(b_{i_1}), \ldots, \sigma_n(b_{i_n}) \rangle$$

where $\sigma_j \in M_{i_j,j}$ for all $1 \leq j \leq n$. Now we take $\mathbf{B} = \langle B, \cdot, f_\sigma(\sigma \in \Sigma) \rangle$.

The proof of this theorem will be finished once it is shown that the mapping π defined by

$$\begin{aligned} \pi(\theta) &= \theta|_{B_1} \times \cdots \times \theta|_{B_n} \\ &= \{\langle b, c \rangle \in B : \langle b_i, c_i \rangle \in \theta \text{ for all } 1 \leq i \leq n\} \end{aligned}$$

is a lattice isomorphism of $\mathbf{Con}\ \mathbf{A}$ with $\mathbf{Con}\ \mathbf{B}$. It should be obvious (from the description of the subdirect representation of $\mathbf{Con}\ \mathbf{A}$ into $\prod \mathbf{Con}\ \mathbf{B}_i$) that π is one-to-one; and it is easy to see that $\pi(\mathrm{Con}\ \mathbf{A}) \subseteq \mathrm{Con}\ \mathbf{B}$. We leave it as an Exercise (in fact, 8.8 (3)) to show that $\pi(\mathrm{Con}\ \mathbf{A}) = \mathrm{Con}\ \mathbf{B}$ and π is a lattice isomorphism. □

Theorem 8.7 could be useful for the investigation of the lattice varieties of the form $\boldsymbol{HSP}(\mathrm{CON}\ \mathcal{V})$ derived from (locally finite) congruence-modular varieties $\mathcal{V}$. It has been conjectured that every such lattice variety either consists of distributive lattices or is identical with $\boldsymbol{HSP}(\mathrm{CON}_{\mathbf{R}}\mathcal{M})$ for some ring $\mathbf{R}$ with unit, where ${}_{\mathbf{R}}\mathcal{M}$ is the variety of unitary $\mathbf{R}$-modules.

Several results about the free spectra of congruence-modular varieties are proved in Chapter 12.

Exercises 8.8

(1) Let $\mathcal{V}$ be a locally finite congruence-permutable variety. Prove (i): $\mathrm{typ}\{\mathcal{V}\} \subseteq \{\mathbf{2}, \mathbf{3}\}$; and (ii): for every finite $\mathbf{A} \in \mathcal{V}$ and $\alpha \prec \beta$ in $\mathrm{Con}\ \mathbf{A}$ and $\langle a, b \rangle \in \beta - \alpha$, there exists $u \equiv b \pmod{\alpha}$ with $\{a, u\} \subseteq N$ for some $\langle \alpha, \beta \rangle$-trace N. Consult Lemmas 5.22 and 5.24. [There is an open question here. Do (i) and (ii) imply that $\mathcal{V}$ is congruence-permutable? In Theorem 9.14, we learn that $\mathrm{typ}\{\mathcal{V}\} \subseteq \{\mathbf{2}, \mathbf{3}\}$ if $\mathcal{V}$ is congruence n-permutable for some n.]

(2) Let $\mathbf{A}$ be a finite algebra such that $\mathrm{typ}\{\mathbf{A}\} = \mathbf{2}$. Prove that for every $\alpha \prec \beta$ in $\mathrm{Con}\ \mathbf{A}$ and $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, the $\langle \alpha, \beta \rangle$-tail of U is empty. (See Lemma 4.27 and note that $\mathbf{A}$ is solvable.)

(3) Complete the proof of Theorem 8.7.

(4) Let $\mathbf{G}$ be a finite group, $p_1, \ldots, p_n$ be the prime divisors of $|\mathbf{G}|$, and $\mathbf{P}_i$ be a Sylow p_i-subgroup of $\mathbf{G}$ for $1 \leq i \leq n$. Show that the mapping

$$\theta \mapsto \langle \theta|_{P_i} : 1 \leq i \leq n \rangle$$

is a lattice embedding of $\mathbf{Con}\ \mathbf{G}$ into $\prod_1^n \mathbf{Con}\, \mathbf{P}_i$, but not necessarily a subdirect embedding. (See Exercise 4.37 (6) for a proof that the groups $\mathbf{P}_i$ are E-minimal algebras.)

9. MAL'CEV CLASSIFICATION AND OMITTING TYPES

The clone of a variety $\mathcal{V}$, denoted **Clo** $\mathcal{V}$, is equal to the clone of term operations of the free algebra in $\mathcal{V}$ on denumerably many free generators. We regard clones now as multi-sorted "algebras"

$$\mathbf{C} = \langle C_n\,,\ \mathrm{comp}_\ell^k\,,\ p_i^m\ (1 \le n, k, \ell < \omega\,,\ 0 \le i < m < \omega)\rangle$$

with denumerably many universes $C_1, C_2, \ldots$, and with operations "of composition" $\mathrm{comp}_\ell^k : C_k \times C_\ell^k \to C_\ell$, and constants $p_i^m \in C_m$ where $p_i^m(x_0, \ldots, x_{m-1}) = x_i$.

W. Neumann and W. Taylor have introduced a lattice of varieties, in which $\mathcal{V} \le \mathcal{W}$ iff $\hom(\mathbf{Clo}\ \mathcal{V}, \mathbf{Clo}\ \mathcal{W}) \neq \emptyset$. The members of this lattice are equivalence classes of varieties under the equivalence relation $\mathcal{V} \sim \mathcal{W}$ iff $\mathcal{V} \le \mathcal{W} \le \mathcal{V}$. (See [13] for more details.) They say that $\mathcal{V}$ is **interpretable** into $\mathcal{W}$ when $\mathcal{V} \le \mathcal{W}$. Their lattice is called the **lattice of interpretability classes of varieties**. We mention that $\mathcal{V} \le \mathcal{W}$ holds, where $\mathcal{V}$ consists of algebras $\mathbf{A} = \langle A, f_i^{\mathbf{A}}(i \in I)\rangle$, iff there are elements t_i of $\mathbf{Clo}\,\mathcal{W}$ for $i \in I$ with t_i n-ary iff f_i is n-ary, such that for every algebra $\mathbf{B} = \langle B, \ldots\rangle \in \mathcal{W}$ the algebra $\langle B, t_i^{\mathbf{B}}(i \in I)\rangle$ belongs to $\mathcal{V}$. (When this holds, the map $f_i \mapsto t_i$ extends to a homomorphism of **Clo** $\mathcal{V}$ into **Clo** $\mathcal{W}$.)

For an example of interpretability, let $\mathcal{M}$ be the variety with one basic operation $p(x, y, z)$, consisting of all the algebras that obey the equations $p(x, y, y) \approx x$ and $p(x, x, y) \approx y$. Then a variety $\mathcal{W}$ satisfies $\mathcal{M} \le \mathcal{W}$ iff there is a term $t(x, y, z)$ in the language of $\mathcal{W}$ (or an element $t \in \mathrm{Clo}_3\mathcal{W}$) such that $t(x, y, y) \approx x$ and $t(x, x, y) \approx y$ hold in $\mathcal{W}$. The filter $\{\mathcal{W} : \mathcal{M} \le \mathcal{W}\}$ in the lattice of interpretability is just the class of congruence-permutable varieties (Theorem 0.3).

A variety $\mathcal{V}$ is called **finitely presented** iff its clone has a finite presentation—that is, iff $\mathcal{V}$ has finitely many basic operations and can be defined by a finite set of equations. By a **strong Mal'cev class** is meant a class of varieties of the form $\{\mathcal{V} : \mathcal{W} \le \mathcal{V}\}$ where $\mathcal{W}$ is finitely presented. The formula "$\mathcal{W} \le \mathcal{V}$" (where $\mathcal{W}$, but not $\mathcal{V}$, is known) is called a **strong Mal'cev condition**. By a **Mal'cev class** is meant any class of varieties of the form $\{\mathcal{V} : \exists_n \mathcal{W}_n \le \mathcal{V}\}$ where $\mathcal{W}_1 \ge \mathcal{W}_2 \ge \cdots \ge \mathcal{W}_n \ge \ldots$ and the $\mathcal{W}_n$ are finitely presented. A **weak Mal'cev class** is any class which is an intersection of countably many Mal'cev classes.

There are six principal theorems in this chapter, showing that for I an order ideal in the partially ordered set of types (Figure 10), the property $\mathrm{typ}\{\mathcal{V}\} \cap I = \emptyset$ is equivalent

to a natural Mal'cev condition. In most cases, our theorems show that a very broad range of varieties omit the types in I, and yet each of these varieties is surprisingly well-behaved, in certain respects. Taken together, the theorems provide remarkable insight into the classification of *locally finite* varieties by Mal'cev conditions.

DEFINITION 9.1. A variety $\mathcal{W}$ will be called **idempotent** iff all of its operations satisfy $f(x,\dots,x) \approx x$. A variety $\mathcal{W}$ will be called **special** iff it is finitely presented, idempotent, and can be defined by linear equations, i.e., equations of the form $\sigma \approx \tau$ where each of σ and τ has at most one occurrence of an operation symbol. A (weak, strong) Mal'cev condition will be called **special** (or **idempotent**) iff its definition involves only special varieties (or idempotent varieties).

We remark that it is apparent from Theorems 8.1 and 8.2 that congruence-modularity of a variety, and congruence-distributivity, are equivalent to special Mal'cev conditions. One aspect of the connection between Mal'cev conditions and omitting types is made manifest in our next lemmas.

LEMMA 9.2. *Let $\mathcal{V}$ and $\mathcal{W}$ be varieties and suppose that $\mathcal{W} \leq \mathcal{V}$ and $\mathcal{W}$ is special. Let $\mathbf{A} \in \mathcal{V}$, $e \in \mathrm{E}(\mathbf{A})$, $U = e(A)$, $\beta \in \mathrm{Con}\,\mathbf{A}$, and $S = a/\beta \cap U$ for some $a \in U$. Then $\mathcal{W} \leq \boldsymbol{V}(\mathbf{A}\mathrm{I}_S)$.*

PROOF. See the proof of Lemma 8.3. □

LEMMA 9.3. *Let $\mathcal{W} \leq \mathcal{V}$ where $\mathcal{W}$ is special and $\mathcal{V}$ has a finite algebra $\mathbf{A}$ with $\mathbf{1} \in \mathrm{typ}\{\mathbf{A}\}$. Then $\mathcal{W}$ is trivial, i.e., $\mathcal{W} \leq \mathcal{S}ets = \{\langle X\rangle : X \neq \emptyset\}$.*

PROOF. We can assume that $\mathbf{A}$ has a minimal congruence β of type $\mathbf{1}$. Let N be any $\langle 0,\beta\rangle$-trace. By Lemma 9.2, $\mathcal{W} \leq \boldsymbol{V}(\mathbf{A}\mathrm{I}_N)$. By Lemma 6.18, $\boldsymbol{V}(\mathbf{A}\mathrm{I}_N)$ contains a two-element algebra $\mathbf{S}$ such that every operation of $\mathbf{S}$ is constant or a projection. Every operation f in Pol $\mathbf{S}$ satisfying $f(x,\dots,x) = x$ must be a projection. Thus $\mathcal{W} \leq \boldsymbol{V}(\langle S\rangle) = \mathcal{S}ets$. □

LEMMA 9.4. *(W. Taylor [32, Cor. 5.3]) For any idempotent variety $\mathcal{V}$, the following are equivalent.*

(1) $\mathcal{V} \not\leq \mathcal{S}ets$
(2) *There exists a special variety $\mathcal{V}'$ such that $\mathcal{V}' \leq \mathcal{V}$, $\mathcal{V}' \not\leq \mathcal{S}ets$.*
(3) *For some $n > 1$ there is a term $f(x_1,\dots,x_n)$ of $\mathcal{V}$ and n linear equations satisfied in $\mathcal{V}$:*

$$\begin{aligned} f(x_{11},\dots,x_{1n}) &\approx f(y_{11},\dots,y_{1n}) \\ &\vdots \\ f(x_{n1},\dots,x_{nn}) &\approx f(y_{n1},\dots,y_{nn}) \end{aligned}$$

in which x_{ij}, y_{ij} are variables and $x_{ii} \neq y_{ii}$ for each i.

PROOF. Trivially, (3) implies (2), and (2) implies (1). To prove that (1) implies (3), we assume that $\mathcal{V} \not\leq \mathcal{S}ets$. Since $\mathrm{Clo}_n\mathcal{S}ets$ is an n-element set for each n, a compactness argument proves the existence of a finite subset of the equations of $\mathcal{V}$ which cannot be modeled in $\mathcal{S}ets$, i.e., there is a finitely presented idempotent $\mathcal{W} \leq \mathcal{V}$, $\mathcal{W} \not\leq \mathcal{S}ets$. Thus we can assume that $\mathcal{V}$ is finitely presented. We work within Clo $\mathcal{V}$ and write clone equations as ordinary equations, using $=$ in place of $\approx$. For example, in place of

$$\mathrm{comp}_2^3(f, p_0^2, p_1^2, p_1^2) = \mathrm{comp}_2^3(f, p_1^2, p_1^2, p_0^2)$$

where $f \in \mathrm{Clo}_3\mathcal{V}$, we would write $f(x,y,y) = f(y,y,x)$.

Let $f_0, \ldots, f_k$ be the elements of Clo $\mathcal{V}$ corresponding to the basic operations of $\mathcal{V}$, and let Σ be a finite set of equations in these operations which defines $\mathcal{V}$. Thus $\langle f_0, \ldots, f_k; \Sigma\rangle$ is a presentation of **Clo** $\mathcal{V}$. By introducing the clone elements $f_{k+1}, \ldots, f_\ell$ that occur as subterms in building the equations of Σ, we can find a different presentation $\langle f_0, \ldots, f_\ell; \Sigma_1\rangle$ such that Σ_1 consists of linear equations together with equations of the form

$$f_i(f_{j_1}(x_1, \ldots, x_n), \ldots, f_{j_m}(x_1, \ldots, x_n)) = f_j(x_1, \ldots, x_n) \tag{9.4.1}$$

with $f_i, f_{j_1}, \ldots, f_{j_m}, f_j$ among $f_0, \ldots, f_\ell$.

Note that for every $f, g \in$ Clo $\mathcal{V}$ there is $h \in$ Clo $\mathcal{V}$ such that f and g can be obtained from h by identifying variables. For example, if $f \in \mathrm{Clo}_2\mathcal{V}$ and $g \in \mathrm{Clo}_3\mathcal{V}$, and if we take

$$h(x,y,z,u,v,w) = f(g(x,y,z), g(u,v,w)),$$

then $h(x,y,z,x,y,z) = g(x,y,z)$ and $h(x,x,x,y,y,y) = f(x,y)$ (because $\mathcal{V}$ is idempotent). Thus there exists $h \in \mathrm{Clo}_n\mathcal{V}$ for some n such that each f_i is obtained by identifying variables in h. Let h be such an element and define λ by

$$\lambda(x_0, \ldots, x_{n^2-1}) = h(h(x_0, \ldots, x_{n-1}), \ldots, h(x_{n^2-n}, \ldots, x_{n^2-1})). \tag{9.4.2}$$

The equations (9.4.1) can now be written as linear equations of the form

$$\lambda(\text{variables}) = \lambda(\text{variables});$$

and the linear equations in Σ_1 can also be written in this form. Let Σ_2 be the set consisting of all these equations of the above form, plus

$$\begin{aligned} &\lambda(x_0, \ldots, x_0, x_1, \ldots, x_1, \ldots, x_{n-1}, \ldots, x_{n-1}) \\ &\quad = \lambda(x_0, \ldots, x_{n-1}, x_0, \ldots, x_{n-1}, \ldots, x_0, \ldots, x_{n-1}). \end{aligned} \tag{9.4.3}$$

Finally, let Σ_2' be the set obtained by adjoining (9.4.2) and $h(x, \ldots, x) = x$ to Σ_2. Note that any variety $\mathcal{W}$ interprets Σ_2' (with an n-ary and an n^2-ary term) iff $\mathcal{V} \leq \mathcal{W}$.

We claim that the clone element λ, and the set Σ_2 of linear equations, substantiates Lemma 9.4 (3). If this is false, then there must be an $m < n^2$, say $m = n \cdot i + j$ $(0 \leq i, j < n)$, such that in every equation of Σ_2, the same variable appears at the m-th place on both sides. Since equation (9.4.3) is in Σ_2, we must have $i = j$. But then we can check that $\Sigma_2{}'$ is interpretable in $\mathcal{S}ets$ by setting $h(x_0, \ldots, x_{n-1}) = x_i$, $\lambda(x_0, \ldots, x_{n^2-1}) = x_m$. (Equation (9.4.2) will be true here since $i = j$.) By the remark at the end of the previous paragraph, $\mathcal{V} \leq \mathcal{S}ets$, a contradiction. □

LEMMA 9.5. *For any idempotent variety $\mathcal{V}$, the following are equivalent.*

(1) $\mathcal{V} \not\leq \mathcal{S}emilattices$.

(2) *There exists a special variety $\mathcal{V}'$ such that $\mathcal{V}' \leq \mathcal{V}$, $\mathcal{V}' \not\leq \mathcal{S}emilattices$.*

(3) *For some $m > 1$ there is a term $f(x_1, \ldots, x_m)$ of $\mathcal{V}$ such that for every non-void set $I \subseteq \{1, \ldots, m\}$, there is an equation $f(x_{i_1}, \ldots, x_{i_m}) \approx f(y_{i_1}, \ldots, y_{i_m})$ satisfied by $\mathcal{V}$, where $\{x_{i_j} : j \in I\} \neq \{y_{i_j} : j \in I\}$ and the x_{i_j} and y_{i_j} are variables.*

PROOF. Again, it is trivial that (3) implies (2), and (2) implies (1). Now we assume that $\mathcal{V} \not\leq \mathcal{S}emilattices$. As in the last proof, we can assume that $\mathcal{V}$ is finitely presented, and in fact that **Clo** $\mathcal{V}$ has a presentation $\langle h, k; \Sigma \rangle$ where Σ consists of the equations

$$k(x_{0,0}, \ldots, x_{n-1,n-1}) = h(h(x_{0,0}, \ldots, x_{0,n-1}), \ldots, h(x_{n-1,0}, \ldots, x_{n-1,n-1})),$$
$$\text{and } h(x, \ldots, x) = x$$

together with a finite set Γ of linear equations of the form $k(\text{variables}) = k(\text{variables})$.

Let $\text{Seq} = \bigcup\{\text{Seq}(m) : 1 \leq m < \omega\}$ where $\text{Seq}(m)$ is the set of all sequences $\langle \sigma_0, \ldots, \sigma_{m-1} \rangle = \sigma$ with $\{\sigma_0, \ldots, \sigma_{m-1}\} \subseteq \{0, \ldots, n-1\}$. To define some clone elements, we select infinitely many distinct variables $x_\sigma (\sigma \in \text{Seq})$. Then we define $h^1 = h$, $h^2 = k$, and inductively,

$$h^{m+1}(\langle x_\sigma : \sigma \in \text{Seq}(m+1) \rangle) =$$
$$h(h^m(\langle x_{\langle 0 \rangle^\frown \tau} : \tau \in \text{Seq}(m) \rangle), \ldots, h^m(\langle x_{\langle n-1 \rangle^\frown \tau} : \tau \in \text{Seq}(m) \rangle)).$$

We take $\widehat{\Gamma}$ to be the set of all linear equations of the form $h^i(\text{variables}) = h^j(\text{variables})$ true in **Clo** $\mathcal{V}$.

Letting $\mathbf{C}$ be the clone of the variety of semilattices, if $\widehat{\Gamma}$ is not modeled by any sequence of elements q^1 (n-ary), q^2 (n^2-ary), ... in $\mathbf{C}$, then a finite subset of $\widehat{\Gamma}$ is not modeled. Since h^i can be obtained from h^j by identifying variables when $i < j$, we could conclude that $\mathbf{C}$ cannot model all the true linear equations of **Clo** $\mathcal{V}$ involving a single h^r (for r sufficiently large). We could take $f = h^r$ and $m = n^r$ and satisfy Lemma 9.5 (3), since if there were an I without the required equation, we could, by taking $f(x_1, \ldots, x_k) = \bigwedge\{x_i : i \in I\}$, model the linear equations for f in the clone of semilattices. Thus Lemma 9.5 (3) will hold unless $\widehat{\Gamma}$ can be modeled in $\mathbf{C}$.

To finish the proof, we now assume that $q^1, q^2, \ldots$ are elements of $\mathbf{C}$ modeling $\widehat{\Gamma}$. We shall derive a contradiction.

For each $\sigma \in \mathrm{Seq}$, put $\sigma \in D$ iff q^m depends on x_σ (where $\sigma \in \mathrm{Seq}(m)$), and put $\sigma \in I$ iff $\sigma \notin D$. Thus

(9.5.1) $q^m(\langle x_\sigma : \sigma \in \mathrm{Seq}(m)\rangle) = \bigwedge\{x_\sigma : \sigma \in D \cap \mathrm{Seq}(m)\}$ for each $1 \leq m < \omega$.

Using (9.5.1) and some of the equations in $\widehat{\Gamma}$, we can easily see that:

(9.5.2) If $\sigma \in I$ then $\tau^\frown\sigma, \sigma^\frown\tau \in I$ for all $\tau \in \mathrm{Seq}$.

(9.5.3) If $\sigma^\frown\langle j\rangle \in I$, then $\sigma^\frown\langle i, j\rangle \in I$.

(9.5.4) $\sigma \in D$ iff $D[\sigma] = \{i < n : \sigma^\frown\langle i\rangle \in D\}$ is nonempty.

Claim. For every $\sigma \in D$, there is $i < n$ such that $\sigma^\frown\langle i\rangle \in D$ and $|D[\sigma^\frown\langle i\rangle]| < |D[\sigma]|$.

To prove this claim, let $\sigma \in D$. The set $D[\sigma]$ is nonempty, by (9.5.4), and we define $p(x_0, \ldots, x_{n-1}) = \bigwedge\{x_i : i \in D[\sigma]\}$. The operation p^2 cannot satisfy all the linear equations satisfied by h^2, else we have an interpretation of $\mathcal{V}$ in semilattices. Thus there is an equation

$$h^2(\langle u_{ij} : i, j < n\rangle) = h^2(\langle v_{ij} : i, j < n\rangle)$$

true in $\mathbf{Clo}\ \mathcal{V}$, where u_{ij}, v_{ij} are variables such that

$$\{u_{i,j} : i, j \in D[\sigma]\} \neq \{v_{i,j} : i, j \in D[\sigma]\}.$$

The two sides of this equation can be substituted into h^{m+2}, where $\sigma \in \mathrm{Seq}(m)$, replacing the subterm $h^2(\langle x_{\sigma^\frown\langle i,j\rangle} : i, j < n\rangle)$ to obtain an equation in $\widehat{\Gamma}$. Since q^{m+2} must satisfy this equation, we conclude that there are $\bar{i}, \bar{j} \in D[\sigma]$ such that $\sigma^\frown\langle \bar{i}, \bar{j}\rangle \in I$. Thus $\sigma^\frown\langle \bar{i}\rangle \in D$ and $\bar{j} \in D[\sigma] - D[\sigma^\frown\langle \bar{i}\rangle]$. By (9.5.2) and (9.5.3), $D[\sigma^\frown\langle \bar{i}\rangle] \subseteq D[\sigma]$, and so the claim is established.

The claim clearly implies that $D = \emptyset$. Hence q^1 is constant. This is impossible, since the equation $h^1(x, \ldots, x) = x$ is in $\widehat{\Gamma}$. □

We are now ready for the first main theorem of this chapter.

THEOREM 9.6. *For any locally finite variety $\mathcal{V}$ the following are equivalent.*

(1) $\mathbf{1} \notin \mathrm{typ}\{\mathcal{V}\}$.

(2) *There exists an idempotent variety $\mathcal{E}$ such that $\mathcal{E} \leq \mathcal{V}$ and $\mathcal{E} \not\leq \mathcal{S}ets$.*

(3) *There is a positive integer m such that for every $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta, \gamma \in \mathrm{Con}\,\mathbf{A}$ we have $\alpha \cap (\beta \circ \gamma) \subseteq \gamma_m \circ \beta_m$ where $\beta_0 = \beta$, $\gamma_0 = \gamma$, and inductively, $\beta_{n+1} = \beta \vee (\alpha \wedge \gamma_n)$ and $\gamma_{n+1} = \gamma \vee (\alpha \wedge \beta_n)$. In symbols, $\mathcal{V} \underset{\mathrm{CON}}{\models} \alpha \cap (\beta \circ \gamma) \subseteq \gamma_m \circ \beta_m$.*

(4) $\mathbf{D}_1 \notin \boldsymbol{S}(\mathrm{CON}\ \mathcal{V})$.

(5) CON $\mathcal{V} \subseteq$ SD($\wedge$)/*Modular*.

(6) *There is a ternary term which defines a Mal'cev operation on every block of a locally solvable congruence in* $\mathcal{V}$.

(7) *Every two locally solvable congruences on an algebra in* $\mathcal{V}$ *permute.*

PROOF. The equivalence of (1), (4), (5), (6), (7) is contained in Theorem 7.9 and Theorem 7.12.

We have that (2) implies (1), easily, by Lemma 9.3 and Lemma 9.4.

To see that (1) implies (3), we must consider the free algebra $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z)$ and its congruences $\alpha = \theta(x, z)$, $\beta = \theta(x, y)$, $\gamma = \theta(y, z)$. Defining β_n and γ_n as in statement (3), it is easy to prove that $\langle \beta_n \rangle$ and $\langle \gamma_n \rangle$ are increasing sequences. Since $\mathbf{F}$ is finite, there is an $m > 0$ such that $\beta_m = \beta_{m+1}$ and $\gamma_m = \gamma_{m+1}$. Then, by the definition of β_{m+1} and γ_{m+1}, we have $\alpha \wedge \beta_m \leq \gamma_m$ and $\alpha \wedge \gamma_m \leq \beta_m$; i.e., $\alpha \wedge \beta_m = \alpha \wedge \gamma_m$. Now from this and Theorem 7.7 (2) it follows that $\alpha \wedge \beta_m \overset{s}{\sim} \alpha \wedge (\beta_m \vee \gamma_m)$. It is easy to prove, inductively, that $\beta_n \vee \gamma_n = \beta \vee \gamma = \beta_n \vee \alpha = \alpha \vee \gamma_n$ for all n. Therefore, since $\overset{s}{\sim}$ is a lattice congruence, we have

$$\begin{aligned} \alpha \wedge \beta_m &\overset{s}{\sim} \alpha \wedge (\beta_m \vee \gamma_m) = \alpha, \\ \beta_m &\overset{s}{\sim} \beta_m \vee \alpha = \beta \vee \gamma, \\ \alpha \wedge \gamma_m &\overset{s}{\sim} \alpha, \\ \gamma_m &\overset{s}{\sim} \beta \vee \gamma \overset{s}{\sim} \beta_m. \end{aligned}$$

Now by Theorem 7.12, β_m and γ_m permute. Since $\langle x, z \rangle \in \beta \circ \gamma \subseteq \beta_m \circ \gamma_m$, it follows that $\langle x, z \rangle \in \gamma_m \circ \beta_m$.

Now let $\mathbf{A}$ be any algebra in $\mathcal{V}$ and let $\alpha', \beta', \gamma' \in \operatorname{Con} \mathbf{A}$ and let $\langle a, c \rangle \in \alpha' \cap (\beta' \circ \gamma')$. Let $b \in A$ be such that $\langle a, b \rangle \in \beta'$, $\langle b, c \rangle \in \gamma'$. Define a homomorphism $\pi \in \hom(\mathbf{F}, \mathbf{A})$ by setting $\pi(x) = a$, $\pi(y) = b$, $\pi(z) = c$. Obviously $\alpha \subseteq \pi^{-1}(\alpha')$, $\beta \subseteq \pi^{-1}(\beta')$, $\gamma \subseteq \pi^{-1}(\gamma')$; therefore $\beta_m \subseteq \pi^{-1}(\beta'_m)$ and $\gamma_m \subseteq \pi^{-1}(\gamma'_m)$ since π^{-1} is a lattice isomorphism of **Con A** with the interval $\mathbf{I}[\pi^{-1}(0), 1]$ in **Con F**. It follows that $\pi(\gamma_m \circ \beta_m) \subseteq \gamma'_m \circ \beta'_m$; and so $\langle a, c \rangle = \pi(\langle x, z \rangle) \in \gamma'_m \circ \beta'_m$. We have now shown that (1) implies (3).

To prove the implication "(3) implies (2)", assume that (3) holds with a certain value m. Let $\alpha, \beta, \gamma \in \operatorname{Con} \mathbf{F}_{\mathcal{V}}(x, y, z)$ be as above. Thus we have $\langle x, z \rangle \in \gamma_m \circ \beta_m$. This property, that "$\langle x, z \rangle \in \gamma_m \circ \beta_m$", is equivalent to a special Mal'cev condition. (In fact, "$(\exists m)(\langle x, z \rangle \in \gamma_m \circ \beta_m)$" is equivalent to a certain special Mal'cev condition for varieties.) We omit the proof of this fact, although we do prove it for $m = 1$ while proving the next theorem; and the general proof is visible in that argument. Now, from the fact just noted, there must exist a special $\mathcal{E}$ such that $\mathcal{E} \leq \mathcal{V}$ and whenever $\mathcal{E} \leq \mathcal{W}$ then $\mathcal{W}$ satisfies "$\langle x, z \rangle \in \gamma_m \circ \beta_m$". We can check that *Sets* does not satisfy "$\langle x, z \rangle \in \gamma_m \circ \beta_m$". ($\mathbf{F}_{Sets}(x, y, z)$ is a 3-element algebra with universe

$\{x, y, z\}$, satisfying $\beta_n = \beta$, $\gamma_n = \gamma$ for all n.) Therefore $\mathcal{E} \not\leq \mathcal{S}ets$, and we have shown that $\mathcal{V}$ satisfies (2). □

Remark 9.7. As far as locally finite varieties are concerned, the special Mal'cev class

$$\{\mathcal{V} : \text{for some } m,\ \mathcal{V} \vDash \alpha \cap (\beta \circ \gamma) \subseteq \gamma_m \circ \beta_m\}$$

is the largest idempotent Mal'cev class distinct from the class of all varieties.

THEOREM 9.8. *For any locally finite variety $\mathcal{V}$, the following are equivalent.*

(1) $\operatorname{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{5}\} = \emptyset$.

(2) *There exists an idempotent variety $\mathcal{E}$ such that $\mathcal{E} \leq \mathcal{V}$ and $\mathcal{E} \not\leq \mathcal{S}emilattices$.*

(3) $\mathcal{V} \underset{\text{CON}}{\vDash} \alpha \cap (\beta \circ \gamma) \subseteq (\gamma \vee (\alpha \wedge \beta)) \circ (\beta \vee (\alpha \wedge \gamma))$.

(4) *For some $n \geq 0$ there are terms $d_0(x, y, z), \ldots, d_n(x, y, z)$, $p(x, y, z)$ and $e_0(x, y, z), \ldots, e_n(x, y, z)$ such that these equations hold in $\mathcal{V}$:*

$$x \approx d_0(x, y, z),$$

$$d_i(x, y, y) \approx d_{i+1}(x, y, y) \text{ and } e_i(x, y, y) \approx e_{i+1}(x, y, y)$$
$$\text{for even } i < n,$$

$$d_i(x, x, y) \approx d_{i+1}(x, x, y) \text{ and } e_i(x, x, y) \approx e_{i+1}(x, x, y)$$
$$\text{for odd } i < n,$$

$$d_n(x, y, y) \approx p(x, y, y) \text{ and } p(x, x, y) \approx e_0(x, x, y),$$

$$d_i(x, y, x) \approx d_{i+1}(x, y, x) \text{ and } e_j(x, y, x) \approx e_{j+1}(x, y, x)$$
$$\text{for odd } i < n \text{ and even } j < n,$$

$$e_n(x, y, z) \approx z.$$

(5) $\mathbf{D}_2 \notin \boldsymbol{S}(\operatorname{CON} \mathcal{V}_{fin})$.

(6) $\operatorname{CON} \mathcal{V}_{fin} \subseteq \operatorname{SD}(\vee)/\mathcal{M}odular$.

PROOF. The equivalence of (1), (5), (6) is proved in Theorem 7.10. We shall prove that (2) implies (1), (1) implies (3), (3) and (4) are equivalent, and (3) implies (2).

Now if (2) holds, then, by Lemma 9.5, there is a special variety $\mathcal{E}$ such that $\mathcal{E} \leq \mathcal{V}$ and $\mathcal{E} \not\leq \mathcal{S}emilattices$. Certainly $\mathcal{E} \not\leq \mathcal{S}ets$, so by Theorem 9.6, $\mathbf{1} \notin \operatorname{typ}\{\mathcal{V}\}$. If $\mathbf{5} \in \operatorname{typ}\{\mathcal{V}\}$ then, by Lemma 9.2, $\mathcal{E} \leq \boldsymbol{V}(\langle\{0, 1\}, \wedge, 0, 1\rangle)$. Since every idempotent polynomial of $\langle\{0, 1\}, \wedge, 0, 1\rangle$ belongs to $\operatorname{Clo}\langle\{0, 1\}, \wedge\rangle$, we actually have $\mathcal{E} \leq \boldsymbol{V}(\langle\{0, 1\}, \wedge\rangle) = \mathcal{S}emilattices$, a contradiction. Thus (2) implies (1).

Assume that (1) holds. Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z)$ and let α, β, γ be the same congruences on $\mathbf{F}$ encountered in the last proof. Since $\alpha \vee \beta = \alpha \vee \gamma = \beta \vee \gamma$, we have, by Theorem 7.7 (3), that

$$\beta_1 = \beta \vee (\alpha \wedge \gamma) \overset{s}{\sim} \beta \vee \gamma \overset{s}{\sim} \gamma \vee (\alpha \wedge \beta) = \gamma_1.$$

Thus by Theorem 7.12, $\beta_1 \circ \gamma_1 = \gamma_1 \circ \beta_1$, and we have $\langle x, z \rangle \in \gamma_1 \circ \beta_1$. By the proof of Theorem 9.6, "$\langle x, z \rangle \in \gamma_1 \circ \beta_1$" is equivalent to (3). Thus (1) implies (3).

We now show that "$\langle x, z \rangle \in \gamma_1 \circ \beta_1$" is equivalent to (4). Note that α, β and γ are respectively the kernels of the three endomorphisms of $\mathbf{F}$ defined by the conditions $\pi_1(x) = \pi_1(z) = x$, $\pi_1(y) = y$; $\pi_2(x) = \pi_2(y) = x$, $\pi_2(z) = y$; and $\pi_3(x) = x$, $\pi_3(y) = \pi_3(z) = y$. Thus for any terms $s(x, y, z)$ and $t(x, y, z)$ we have $\langle s^{\mathbf{F}}(x, y, z), t^{\mathbf{F}}(x, y, z) \rangle \in \alpha$ iff $s^{\mathbf{F}}(x, y, x) = t^{\mathbf{F}}(x, y, x)$ iff the equation $s(x, y, x) \approx t(x, y, x)$ holds in $\mathcal{V}$. Similar statements hold for β and γ. That $\langle x, z \rangle \in \gamma_1 \circ \beta_1$ iff (4) holds should now be clear from these remarks.

Now suppose that (3) (and (4)) hold. The equations (4) (for a certain n) define a special variety $\mathcal{E}_n$ with $2n+3$ basic operations such that $\mathcal{E}_n \leq \mathcal{V}$. If $\mathcal{E}_n \leq \mathcal{S}emilattices$ then, by the equivalence of (3) and (4), in the free semilattice on generators x, y, z we have $\langle x, z \rangle \in \gamma_1 \circ \beta_1$. This free semilattice has seven elements and it can be checked that here $\langle x, z \rangle \notin \gamma_1 \circ \beta_1$, although $\langle x, z \rangle \in \gamma_2 \circ \beta_2$. Therefore $\mathcal{E}_n \not\leq \mathcal{S}emilattices$. This concludes the proof that (3) implies (2). □

Remark 9.9. We shall later point out (Theorem 9.18) that if a variety satisfies a lattice equation for congruences, $\mathcal{V} \underset{\text{CON}}{\models} \varepsilon$, and if ε does not hold in every lattice (i.e., if ε is non-trivial), then $\mathcal{V}$ satisfies Theorem 9.8 (2), and so if $\mathcal{V}$ is locally finite it satisfies Theorem 9.8 (3). In this connection, we remark that Gumm's characterization of congruence-modular varieties in Theorem 8.1 is equivalent to

$$\mathcal{V} \underset{\text{CON}}{\models} \alpha \cap (\beta \circ \gamma) \subseteq [(\alpha \wedge \gamma) \vee (\alpha \wedge \beta)] \circ \beta;$$

and this inclusion trivially implies Theorem 9.8 (3).

THEOREM 9.10. *For any locally finite variety $\mathcal{V}$ the following are equivalent.*

(1) $\text{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{2}\} = \emptyset$.

(2) *There exists a special $\mathcal{E} \leq \mathcal{V}$ such that for every finite field $\mathbf{F}$ we have $\mathcal{E} \not\leq {}_{\mathbf{F}}\mathcal{V}$, where ${}_{\mathbf{F}}\mathcal{V}$ is the variety of vector spaces over $\mathbf{F}$.*

(3) $\mathcal{V} \underset{\text{CON}}{\models} \alpha \cap (\beta \circ \gamma) \subseteq \beta_m \cap \gamma_m$ *for some m (where β_m and γ_m are as in Theorem 9.6).*

(4) $\mathbf{M}_3 \notin \boldsymbol{S}(\text{CON } \mathcal{V})$.

(5) $\mathcal{V} \underset{\text{CON}}{\models} \text{SD}(\wedge)$.

(6) *The only Abelian congruence of any algebra in $\mathcal{V}$ is the identity relation.*

PROOF. It is clear that if an algebra in $\mathcal{V}$ has a non-zero Abelian or solvable congruence, then some finite algebra in $\mathcal{V}$ has such a congruence. It follows from Theorem 5.7(2) that (1) and (6) are equivalent, and equivalent to $\mathcal{V}$ having no non-trivial solvable congruence quotients—i.e., $\overset{s}{\sim} = \mathrm{id}$ on $\mathbf{Con}\,\mathbf{A}$ for every $\mathbf{A} \in \mathcal{V}$. By Theorem 7.7(2), (6) implies (5). Obviously, (5) implies (4); and (4) is equivalent to (1) by Theorem 6.22(3). Thus (1), (4), (5), (6) are equivalent.

Now suppose that (1) holds. Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z)$ and let α, β, γ be as in the proof of Theorem 9.6. Pick an $m > 0$ such that $\beta_m = \beta_{m+1}$, $\gamma_m = \gamma_{m+1}$, and so $\alpha \wedge \beta_m = \alpha \wedge \gamma_m$. Since (5) holds, then $\alpha \wedge \beta_m = \alpha \wedge (\beta_m \vee \gamma_m) = \alpha$. Thus $\alpha \leq \beta_m \wedge \gamma_m$. In particular, $\langle x, z \rangle \in \beta_m \wedge \gamma_m$. As in previous proofs, this is equivalent to (3) (for the fixed m). Thus (1) implies (3).

It should be obvious that (3) (at least for a fixed m) is equivalent to a special Mal'cev condition. (The proof is left as an exercise for the reader.) Thus, assuming (3), there exists a special $\mathcal{E}$ such that $\mathcal{E} \leq \mathcal{V}$, and whenever $\mathcal{E} \leq \mathcal{W}$ then $\mathcal{W}$ satisfies (3). To see that ${}_{\mathbf{F}}\mathcal{V}$ ($\mathbf{F}$ a finite field) does not satisfy (3), notice that $\mathbf{M}_3 \in \boldsymbol{S}(\mathrm{CON}\,{}_{\mathbf{F}}\mathcal{V})$ and that ${}_{\mathbf{F}}\mathcal{V}$ has permuting congruences. It follows that $\mathcal{E} \nleq {}_{\mathbf{F}}\mathcal{V}$, and so we have proved that (3) implies (2). Finally, (2) implies (1) via Lemma 9.2. ($\mathcal{E} \nleq {}_{\mathbf{F}}\mathcal{V}$ implies $\mathcal{E} \nleq \mathcal{S}ets$ as well.) □

THEOREM 9.11. *For any locally finite variety $\mathcal{V}$, the following are equivalent.*

(1) $\mathrm{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{2}, \mathbf{5}\} = \emptyset$.

(2) *There exists a special $\mathcal{E}$ such that $\mathcal{E} \leq \mathcal{V}$, $\mathcal{E} \nleq \mathcal{S}emilattices$, and for every finite field $\mathbf{F}$, $\mathcal{E} \nleq {}_{\mathbf{F}}\mathcal{V}$.*

(3) $\mathcal{V} \underset{\mathrm{CON}}{\models} \alpha \cap (\beta \circ \gamma) \subseteq (\beta \vee (\alpha \wedge \gamma)) \wedge (\gamma \vee (\alpha \wedge \beta))$.

(4) *For some $n \geq 0$ there are terms $d_0(x, y, z), \ldots, d_n(x, y, z)$ such that $\mathcal{V}$ satisfies:*

$$x \approx d_0(x, y, z),$$

$$d_i(x, y, y) \approx d_{i+1}(x, y, y) \text{ and } d_i(x, y, x) \approx d_{i+1}(x, y, x)$$

$$\text{for even } i < n,$$

$$d_i(x, x, y) \approx d_{i+1}(x, x, y) \text{ for odd } i < n,$$

$$d_n(x, y, z) \approx z.$$

(5) $\mathbf{D}_2, \mathbf{M}_3 \notin \boldsymbol{S}(\mathrm{CON}\,\mathcal{V}_{fin})$.

(6) $\mathcal{V}_{fin} \underset{\mathrm{CON}}{\models} \mathrm{SD}(\vee)$.

PROOF. The theorem is a little stronger than the union of Theorems 9.8 and 9.10. It can be proved by the same arguments, involving no new tricks, so we leave the proof as an exercise. □

DEFINITION 9.12. A variety $\mathcal{V}$ is called **n-permutable** iff for every $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta \in \operatorname{Con} \mathbf{A}$, we have $\alpha \circ_n \beta = \beta \circ_n \alpha$, where $\alpha \circ_n \beta = \alpha \circ \beta \circ \alpha \circ \dots$ (with $n-1$ occurences of $\circ$).

We shall see that n-permutability (for some n) is equivalent, in a locally finite variety, to the omission of types **1**, **4**, and **5**.

LEMMA 9.13 (Hagemann, Mitschke [17]). *For any variety $\mathcal{V}$ and integer $n \geq 1$, the following are equivalent.*

(1) $\mathcal{V} \underset{\text{CON}}{\models} n+1$*-permutable.*

(2) *There are terms $p_1(x,y,z), \dots, p_n(x,y,z)$ such that $\mathcal{V}$ satisfies*

$$x \approx p_1(x,y,y),$$
$$p_i(x,x,y) \approx p_{i+1}(x,y,y) \text{ for each } i,$$
$$p_n(x,x,y) \approx y.$$

(3) *For every $\mathbf{A} \in \mathcal{V}$ and subalgebra ρ of $\mathbf{A}^2$ such that $\mathrm{id}_A \subseteq \rho$ we have $\rho^{\cup} \subseteq \rho^n$.*

PROOF. This is Exercise 9.20 (4). □

THEOREM 9.14. *For any locally finite variety $\mathcal{V}$ the following are equivalent.*

(1) $\operatorname{typ}\{\mathcal{V}\} \subseteq \{\mathbf{2}, \mathbf{3}\}$.

(2) *There exists a special variety $\mathcal{E}$ such that $\mathcal{E} \leq \mathcal{V}$ and $\mathcal{E} \not\leq \mathcal{D}$ (the variety of distributive lattices).*

(3) *For some n, $\mathcal{V} \underset{\text{CON}}{\models} n$-permutable.*

PROOF. By Lemma 9.13, n-permutability is equivalent to a strong special Mal'cev condition. The variety $\mathcal{D}$ is not n-permutable for any n. Hence (3) implies (2). If (2) holds, say $\mathcal{E} \leq \mathcal{V}$ and $\mathcal{E} \not\leq \mathcal{D}$, then $\mathcal{E} \not\leq \mathcal{S}ets$ and $\mathcal{E} \not\leq \mathcal{S}emilattices$. Thus, by the now familiar argument via Lemma 9.2, $\operatorname{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{4}, \mathbf{5}\} = \emptyset$. Hence (2) implies (1).

Now assume that (1) holds. Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x,y)$ and let ρ be the subalgebra of $\mathbf{F}^2$ generated by $\{\langle x,x\rangle, \langle y,y\rangle, \langle x,y\rangle\}$. Let $\overline{\rho}$ be the transitive closure of ρ. Thus $\overline{\rho}$ is a reflexive, transitive subalgebra of $\mathbf{F}^2$. We claim that $\langle y,x\rangle \in \overline{\rho}$. Suppose that this fails. Now $\theta = \overline{\rho} \cap (\overline{\rho})^{\cup}$ is a congruence of $\mathbf{F}$, and $\langle x,y\rangle \notin \theta$. Choose congruences satisfying $\theta \leq \alpha \prec \beta$, $\langle x,y\rangle \in \beta - \alpha$. Choose an $\langle \alpha, \beta\rangle$-minimal set U and, by 5.7 (1) and 2.8 (4), an $f \in \operatorname{Pol}_1 \mathbf{F}$ with $f(F) = U$ and $\langle f(x), f(y)\rangle \in \beta - \alpha$. Let N be the $\langle \alpha, \beta\rangle$-trace $f(x)/(\beta|_U)$. Since ρ is a reflexive subalgebra of $\mathbf{F}^2$, it is closed under all polynomials of $\mathbf{F}$. Therefore $\langle f(x), f(y)\rangle \in \rho$. Since $\operatorname{typ}(\alpha, \beta) \in \{\mathbf{2}, \mathbf{3}\}$, then by Lemma 4.17 or Lemma 4.20, $\mathbf{F}|_N$ is Mal'cev. Let $d \in \operatorname{Pol}_3 \mathbf{F}$ induce a Mal'cev operation on N. Then

$$\langle f(y), f(x)\rangle = d(\langle f(x), f(x)\rangle, \langle f(x), f(y)\rangle, \langle f(y), f(y)\rangle),$$

so $\langle f(y), f(x)\rangle \in \rho$. Therefore $\langle f(x), f(y)\rangle \in \rho \cap \rho^{\cup} \subseteq \theta \subseteq \alpha$. This contradiction proves that $\langle y, x\rangle \in \overline{\rho}$.

We now choose elements $y = a_n, \ldots, a_0 = x$ in $\mathbf{F}$ such that $\langle a_{i+1}, a_i\rangle \in \rho$ for $0 \leq i < n$. We shall show that $\mathcal{V}$ is $n+1$-permutable. For each $i < n$, there must be a term $p_{i+1}(x, y, z)$ such that $p_{i+1}(\langle x, x\rangle, \langle x, y\rangle, \langle y, y\rangle) = \langle a_{i+1}, a_i\rangle$. Then we have

$$\begin{aligned} x = a_0 &= p_1(x, y, y), \\ p_1(x, x, y) &= a_1 = p_2(x, y, y), \\ &\vdots \\ p_{n-1}(x, x, y) &= a_{n-1} = p_n(x, y, y), \\ p_n(x, x, y) &= a_n = y. \end{aligned}$$

These equations holding in $\mathbf{F}_{\mathcal{V}}(x, y)$ are equivalent to equations of $\mathcal{V}$ implying $n+1$-permutability via Lemma 9.13. Thus we have proved that (1) implies (3). □

THEOREM 9.15. *For any locally finite variety $\mathcal{V}$ the following are equivalent.*

(1) $\operatorname{typ}\{\mathcal{V}\} \subseteq \{\mathbf{3}\}$.

(2) *There exists a special $\mathcal{E} \leq \mathcal{V}$ such that $\mathcal{E} \not\leq \mathcal{D}$ (distributive lattices) and for all finite fields $\mathbf{F}$, $\mathcal{E} \not\leq \mathbf{F}\mathcal{V}$.*

(3) *There are terms $f_0(x, y, z, u), \ldots, f_n(x, y, z, u)$ such that $\mathcal{V}$ satisfies:*
   (i) $x \approx f_0(x, y, y, z)$,
   (ii) $f_i(x, x, y, x) \approx f_{i+1}(x, y, y, x)$ *and* $f_i(x, x, y, y) \approx f_{i+1}(x, y, y, y)$ *for all $i < n$,*
   (iii) $f_n(x, x, y, z) \approx z$.

(4) $\mathcal{V} \underset{\text{CON}}{\models}$ *n-permutable for some n and* $\mathcal{V} \underset{\text{CON}}{\models} \mathrm{SD}(\wedge)$.

(5) $\mathcal{V} \underset{\text{CON}}{\models}$ *n-permutable for some n and* $\mathcal{V} \underset{\text{CON}}{\models} \alpha \wedge (\beta \vee \gamma) \leq \beta_m$ *for some m (where β_m is as in Theorem 9.6).*

PROOF. That (1) and (4) are equivalent follows from Theorems 9.10 and 9.14.

Now we prove that (1) implies (3). Assume that (1) holds and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z)$ and α, β, γ be the usual congruences on $\mathbf{F}$, as in the proof of Theorem 9.6. Let ρ be the subalgebra of $\mathbf{F}^2$ generated by $\{\langle x, x\rangle, \langle y, y\rangle, \langle z, z\rangle, \langle y, x\rangle\}$. Since $\mathcal{V}$ is n-permutable for some n, by Lemma 9.13 there is n such that $\rho^{\cup} \subseteq \rho^n$; i.e., the transitive closure of ρ is the congruence $\beta = \Theta(x, y)$. By Theorem 9.11 ((1) $\Leftrightarrow$ (3)), we have that $\langle x, z\rangle \in \alpha \cap (\beta \circ \gamma) \subseteq \beta \vee (\alpha \wedge \gamma)$. Since β is the transitive closure of ρ, it follows that $\langle x, z\rangle \in \rho \circ ((\alpha \wedge \gamma) \circ \rho)^n = \rho \circ_{2n+1} (\alpha \wedge \gamma)$ for some n. Thus there exist $a_0, a_1, \ldots, a_{2n+1}$ in $\mathbf{F}$ with $x = a_0$, $z = a_{2n+1}$, and $\langle a_{2i}, a_{2i+1}\rangle \in \rho$, and $\langle a_{2j+1}, a_{2(j+1)}\rangle \in \alpha \wedge \gamma$ for all $i \leq n$ and $j < n$. There are terms $f_i(x, y, z, u)$ such that

$$\langle a_{2i}, a_{2i+1}\rangle = f_i(\langle x, x\rangle, \langle y, x\rangle, \langle y, y\rangle, \langle z, z\rangle)$$

for all $i \leq n$. Here,

$$f_0(x,y,y,z) = a_0 = x, \quad f_n(x,x,y,z) = a_{2n+1} = z,$$

and the formulas

$$f_j(x,x,y,z) = a_{2j+1} \overset{\alpha\wedge\gamma}{\equiv} a_{2j+2} = f_{j+1}(x,y,y,z)$$

imply the equations 3(ii), since α is the kernel of the endomorphism π_1 of $\mathbf{F}$ sending x to x, y to y and z to x, and since γ is the kernel of π_2 sending x to x, y to y, and z to y. Then (1) does imply (3).

Now assume that (3) holds. Thus for some n we have $\mathcal{E}_n \leq \mathcal{V}$ where $\mathcal{E}_n$ is the special variety defined by the equations (3), involving the operations $f_0, \ldots, f_n$. Defining $p_{i+1}(x,y,z) = f_i(x,y,z,z)$, it is clear that in $\mathcal{E}_n$ the terms $p_1, \ldots, p_{n+1}$ satisfy the equations of Lemma 9.13. Thus $\mathcal{E}_n \underset{\text{CON}}{\models} n+2$-permutable. This implies that $\mathcal{E}_n \not\leq \mathcal{D}$. Also, the last steps in the argument of the last paragraph are reversible, showing that in $\mathbf{F} = \mathbf{F}_{\mathcal{E}_n}(x,y,z)$, $\langle x,z\rangle$ belongs to the transitive closure of $\beta \cup (\alpha \cap \gamma)$; in particular, $\langle x,z\rangle \in \beta \vee (\alpha \wedge \gamma)$. As in the proof of Theorem 9.10 (or Theorem 9.6), it follows that $\mathcal{E}_n$ satisfies all parts of Theorem 9.10, and so $\mathcal{E}_n \not\leq \mathbf{F}\mathcal{V}$ for any finite field. Thus (3) implies (2).

By Theorem 9.10 and Theorem 9.14, (2) implies (1). By the same theorems, (5) implies (1). Finally, it remains to show that (4) implies (5).

Let us assume that in $\mathcal{V}$, congruences are n-permutable and congruence lattices satisfy SD($\wedge$). We can work in the finite algebra $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x_0, x_1, \ldots, x_n)$. We consider three congruences of $\mathbf{F}$:

$$\alpha = \Theta(x_0, x_n),$$
$$\beta = \Theta(\langle x_0, x_1\rangle, \langle x_2, x_3\rangle, \ldots),$$
$$\gamma = \Theta(\langle x_1, x_2\rangle, \langle x_3, x_4\rangle, \ldots).$$

Note that $\langle x_0, x_n\rangle \in \alpha \wedge (\beta \circ_n \gamma)$. We define β_k, γ_k for all $k \geq 0$ as in Theorem 9.6. Since $\mathbf{F}$ is finite, we can choose $m > 0$ such that $\beta_{m+1} = \beta_m$, $\gamma_{m+1} = \gamma_m$, and so $\alpha \wedge \beta_m = \alpha \wedge \gamma_m$. By SD($\wedge$), this implies that $\alpha \wedge (\beta_m \vee \gamma_m) = \alpha \wedge \beta_m$; and just as before we find that $\langle x_0, x_n\rangle \in \beta_m$.

Now let $\mathbf{A} \in \mathcal{V}$ and $\alpha', \beta', \gamma' \in \operatorname{Con}\mathbf{A}$. To see that $\alpha' \wedge (\beta' \vee \gamma') \leq \beta'_m$, choose $\langle a,b\rangle \in \alpha' \wedge (\beta' \vee \gamma')$. Since congruences in $\mathcal{V}$ are n-permutable, there exist $a_0, \ldots, a_n \in A$ with $a_0 = a$, $a_n = b$, $\langle a_i, a_{i+1}\rangle \in \beta'$ for even $i < n$, and $\langle a_i, a_{i+1}\rangle \in \gamma'$ for odd $i < n$. Let $\pi : \mathbf{F} \to \mathbf{A}$ be the homomorphism defined by $\pi(x_i) = a_i$ $(i = 0, \ldots, n)$. Noting that $\pi(\alpha) \subseteq \alpha'$, $\pi(\beta) \subseteq \beta'$, $\pi(\gamma) \subseteq \gamma'$, we easily deduce that $\pi(\beta_m) \subseteq \beta'_m$. Thus $\langle a,b\rangle = \langle \pi(x_0), \pi(x_n)\rangle \in \beta'_m$, as desired. □

The theorems of this chapter demonstrate that the lattice-theoretic concepts of meet and join semi-distributivity are closely bound up with the classification of locally

finite varieties according to the strength of the special Mal'cev conditions that they satisfy. Each of the two semi-distributive laws for all congruence lattices in a variety is equivalent to a weak special Mal'cev condition. G. Czedli ([6] and [7]) found specific, but not particularly useful, weak Mal'cev conditions equivalent to each of these properties. Historically, the semi-distributive laws for congruences in a variety have been little understood and infrequently applied. Czedli proved the equivalence of Theorem 9.15 (4) $\Leftrightarrow$ (5) for every variety, not just for locally finite ones. His result states that for an n-permutable variety $\mathcal{V}$, congruence meet semi-distributivity is equivalent to the satisfaction, for some m, of the lattice equation $(\varepsilon_m) : \alpha \wedge (\beta \vee \gamma) \leq \beta_m$ in all congruence lattices of $\mathcal{V}$. Moreover, he proved that if $\mathcal{V}$ is congruence n-permutable, then $\mathcal{V}$ is congruence join semi-distributive iff for some m, $\mathcal{V} \underset{\text{CON}}{\models} \varepsilon_m^*$ where ε_m^* is obtained from ε_m by exchanging $\vee$ and $\wedge$.

We see by Theorems 9.10 and 9.11 that for locally finite $\mathcal{V}$, the satisfaction of SD($\vee$) in the congruence lattices of the finite algebras in $\mathcal{V}$ implies the satisfaction of SD($\wedge$) in the congruence lattices of all algebras in $\mathcal{V}$. (For a related implication, see Exercise 7.14 (10).) Whether SD($\vee$) for the finite algebras implies SD($\vee$) for all algebras is an open question, even if we assume that $\mathcal{V}$ has n-permuting congruences.

B. Jónsson and I. Rival [20] proved that a *variety of lattices* consists entirely of lattices satisfying SD($\wedge$) iff for some m the members of the variety all satisfy ε_m. In contrast with the mentioned results of Czedli and Jónsson and Rival, we have the following, due to R. Freese and J. B. Nation [12].

THEOREM 9.16. *The variety of bounded semilattices is congruence meet-semi-distributive, but any lattice equation holding in all its congruence lattices holds in every lattice.*

This theorem does not really contradict Theorem 9.10. In fact, congruences of semilattices satisfy the inclusion $\alpha \cap (\beta \circ \gamma) \subseteq \beta_2$, but this inclusion is not equivalent to a lattice equation, due to the occurrence of composition in it.

We can draw an interesting conclusion by combining Theorem 9.16 with a basic result of A. Pixley [28] and R. Wille [33], which we reproduce below.

THEOREM 9.17. *Let ε be any equation for lattices. The class of varieties whose congruence lattices satisfy ε is defined by a weak special Mal'cev condition.*

From Theorems 9.16, 9.17 and 9.8 we have the following.

THEOREM 9.18. *Let $\mathcal{V}$ be a locally finite variety of algebras and ε be an equation for lattices. If $\mathcal{V} \underset{\text{CON}}{\models} \varepsilon$ and ε does not hold in every lattice, then* $\operatorname{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{5}\} = \emptyset$.

In the next two chapters, we shall study residual properties and decidability in locally finite varieties which omit types **1** and **5**. The results obtained there apply to every locally finite variety whose congruence lattices satisfy a non-trivial lattice

equation, or are n-permutable for some n. To finish this chapter, we present a partial converse to Theorem 9.18.

THEOREM 9.19. *Let $\mathcal{V}$ be a locally finite variety. If $\mathcal{V} \underset{\text{CON}}{\models}$ n-permutable for some n (i.e., if $\text{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{4}, \mathbf{5}\} = \emptyset$), then there exists a lattice equation which fails to hold in some lattice but is satisfied by the congruence lattice of every algebra in $\mathcal{V}$.*

PROOF. Let u, v, x, y, z be lattice variables. Define $y_0 = y$, $z_0 = z$, and inductively, $y_{k+1} = y \vee (x \wedge z_k)$ and $z_{k+1} = z \vee (x \wedge y_k)$. Consider the lattice equation (depending on m)

$$u \wedge ((u \wedge v) \vee (x \wedge (y \vee z))) \leq v \vee (x \wedge (u \vee (x \wedge y_m))). \tag{9.19.1}$$

Assuming that $\mathcal{V} \underset{\text{CON}}{\models}$ n-permutable for a fixed n, we shall prove that (9.19.1) holds in the congruence lattices of $\mathcal{V}$ if m is sufficiently large.

If $\mathbf{A} \in \mathcal{V}$ and $\lambda, \tau, \alpha, \beta, \gamma \in \text{Con } \mathbf{A}$, and $a, b \in A$, then since $\mathcal{V}$ is congruence n-permutable, we have

$$\langle a, b \rangle \in \lambda \wedge ((\lambda \wedge \tau) \vee (\alpha \wedge (\beta \vee \gamma)))$$

iff there exist elements of $\mathbf{A}$ satisfying the congruences graphed in Figure 25, and also $\langle a_i, a_{i+1} \rangle \in \alpha$ for all odd $i < n$. (We can assume that n is odd.)

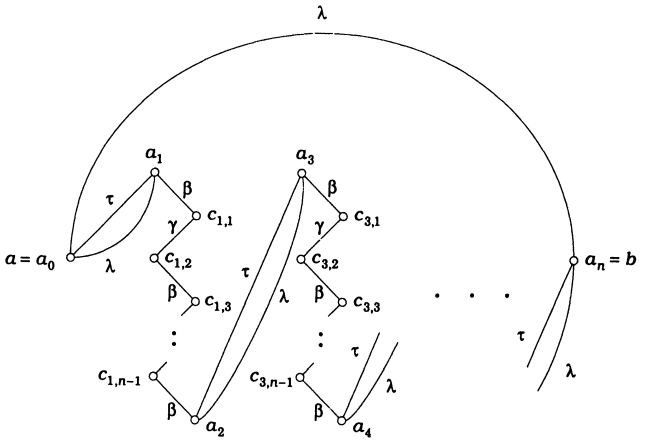


Figure 25

We consider the algebra

$$\mathbf{A} = \mathbf{F} = \mathbf{F}_{\mathcal{V}}(x_0, x_1, \ldots, x_n, y_{ij}\ (1 \leq i < n,\ i \text{ odd},\ 1 \leq j \leq n-1))\,,$$

and examine the generic congruences of $\mathbf{F}$ for this graph. They are

$$\lambda = \Theta(\langle x_0, x_n\rangle, \langle x_0, x_1\rangle, \langle x_2, x_3\rangle, \ldots, \langle x_{n-1}, x_n\rangle),$$

$$\tau = \Theta(\langle x_0, x_1\rangle, \langle x_2, x_3\rangle, \ldots, \langle x_{n-1}, x_n\rangle),$$

$$\alpha = \Theta(\langle x_1, x_2\rangle, \langle x_3, x_4\rangle, \ldots, \langle x_{n-2}, x_{n-1}\rangle),$$

$$\beta = \Theta(\{\langle y_{i,2j+2}, y_{i,2j+3}\rangle : i \text{ odd}, j < \frac{n-4}{2}\} \cup \{\langle x_i, y_{i,1}\rangle, \langle y_{i,n-1}, x_{i+1}\rangle : i \text{ odd}\}),$$

$$\gamma = \Theta(\{\langle y_{i,2j-1}, y_{i,2j}\rangle : i \text{ odd}, 1 \leq j \leq \frac{n-1}{2}\}).$$

Here $\langle x_0, x_n\rangle \in \lambda \wedge ((\lambda \wedge \tau) \vee (\alpha \wedge (\beta \vee \gamma)))$, via Figure 25, with $x_i = a_i$, $y_{ij} = c_{ij}$.

We construct β_m, γ_m from α, β, γ in the usual way, and choose m large enough so that $\beta_m = \beta_{m+1}$, $\gamma_m = \gamma_{m+1}$. Since $\alpha \wedge \beta_m = \alpha \wedge \gamma_m$, we have

$$\alpha \wedge \beta_m \overset{s}{\sim} \alpha \wedge (\beta_m \vee \gamma_m) = \alpha \wedge (\beta \vee \gamma)$$

(by Theorem 7.7 (2)). Thus **Con F** has the sublattice pictured in Figure 26.

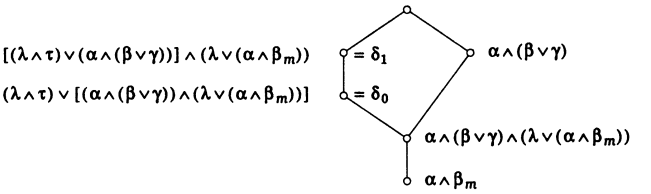


Figure 26

Since the lower right interval in the pentagon is solvable, then $\text{typ}\{\delta_0, \delta_1\} \subseteq \{\mathbf{1}\}$ by Lemma 6.5. But $\mathbf{1} \notin \text{typ}\{\mathcal{V}\}$, hence $\delta_0 = \delta_1$. This certainly implies that

$$\lambda \wedge ((\lambda \wedge \tau) \vee (\alpha \wedge (\beta \vee \gamma))) \leq \tau \vee (\alpha \wedge (\lambda \vee (\alpha \wedge \beta_m))). \tag{9.19.2}$$

In other words, (9.19.1) holds for the specific 5-tuple $\langle u, v, x, y, z\rangle = \langle \lambda, \tau, \alpha, \beta, \gamma\rangle$ in Con $\mathbf{F}$. Then the familiar arguments with homomorphisms will easily prove that (9.19.1) holds for any 5-tuple of elements in **Con A**, for any $\mathbf{A} \in \mathcal{V}$.

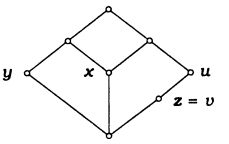


Figure 27

To finish the proof, we need to see that (9.19.1) fails to hold in some lattice. In fact, for every m, this equation fails to hold in the lattice pictured in Figure 27. □

Exercises 9.20

(1) Let $\mathbf{A}$ be an Abelian algebra in a locally finite variety and suppose that $\mathbf{A}$ has a polynomial $f(x,y)$ satisfying the equations $f(x,x) \approx x$, $f(x,y) \approx f(y,x)$. Show (using Theorem 9.6, or directly) that $\mathbf{A}$ is Mal'cev. Show that the non-locally finite algebra $\langle \mathbb{Q}, \frac{x+y}{2} \rangle$ is Abelian and not Mal'cev, where $\mathbb{Q}$ is the set of rational numbers.

(2) Let $\mathbf{A}$ be an Abelian algebra in a not necessarily locally finite variety satisfying Theorem 9.8(4). Prove that $\mathbf{A}$ is Mal'cev. (Hint: Show that $d_i(x,y,y) \approx x$ and $e_i(x,x,y) \approx y$ in $\mathbf{A}$.)

(3) Prove Theorem 9.11.

(4) Prove Theorem 9.13.

(5) Prove (3) ⇒ (2) in Theorem 9.14.

(6) (Polin's variety) The variety $\mathcal{P}$ generated by the pair of two-element algebras $\langle \{0,1\}, \wedge, 0, 1, f_0, g_0 \rangle$ and $\langle \{0,1\}, \wedge, 0, 1, f_1, g_1 \rangle$ where $f_0(x) = 1-x$, $f_1(x) = x$, $g_0(x) = 1$, $g_1(x) = 1-x$, discovered by S. V. Polin, was the first example of a non-congruence-modular variety $\mathcal{V}$ such that $\mathcal{V} \underset{\text{CON}}{\models} \varepsilon$ for some lattice equation ε not holding in all lattices. Show that $\mathcal{P}$ satisfies the equivalent conditions of Theorem 9.15. Show, via Theorem 8.5, that $\mathcal{P}$ is not congruence-modular.

(7) Let $\mathcal{V}$ be any variety of semigroups (it need not be locally finite) which is not equivalent to a variety of groups of finite exponent. Prove that $\mathcal{V}$ contains a two-element strongly Abelian semigroup, or a two-element semilattice. Therefore $\text{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{5}\} \neq \emptyset$.

10. RESIDUALLY SMALL VARIETIES

A variety $\mathcal{V}$ is called **residually small** iff there is a cardinal number λ such that every subdirectly irreducible algebra in $\mathcal{V}$ has at most λ elements. Varieties that are not residually small are called **residually large**. We use $\mathcal{V}_{SI}$ to denote the class of subdirectly irreducible algebras in $\mathcal{V}$, and $\text{Spec}(\mathcal{V}_{SI})$ to denote the class of cardinalities of the members of $\mathcal{V}_{SI}$.

We conjecture that if $\mathcal{V}$ is generated by a finite algebra then $\text{Spec}(\mathcal{V}_{SI})$ must be either a finite set of finite cardinals, or an unbounded set of cardinals. (In the latter case, $\text{Spec}(\mathcal{V}_{SI})$ contains all of the infinite cardinals, at least if $\mathcal{V}$ is locally finite.) The truth of this conjecture has been established for several important families of varieties. For congruence-modular varieties, it was proved in [10], and the finite algebras which generate residually small congruence-modular varieties were characterized. For example, a finite group has this property if and only if all of its nilpotent subgroups are Abelian. The conjecture was established for varieties of semigroups in [23].

We shall prove in this chapter that if a locally finite variety $\mathcal{V}$ satisfies $\text{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{5}\} = \emptyset$, and is residually small, then $\mathcal{V}$ is congruence-modular. Thus the above-stated conjecture is true for those locally finite varieties that omit the types **1** and **5**; and the conjecture is true, a fortiori, for every locally finite variety whose congruence lattices obey a non-trivial lattice equation.

LEMMA 10.1. *Let* $\mathbf{L}$ *be any finite non-modular lattice. Either* $\mathbf{L}$ *has a sublattice isomorphic to* $\mathbf{D}_2$ *(Figure 12), or* $\mathbf{L}$ *has a sublattice as pictured in Figure 28 with* $u_0 \prec u_1 \prec x_2$ *and* $x_0 \prec x_1$.

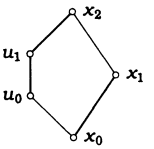


Figure 28

PROOF. For $x < y$ in $\mathbf{L}$, define $f(x,y) = |I[x,y]|$. A pentagon in $\mathbf{L}$ is a 5-tuple of elements $\langle x_0, x_1, x_2, u_1, u_0 \rangle$ with $x_1 \vee u_0 = x_2 \geq u_1$, $x_1 \wedge u_1 = x_0 \leq u_0$, $u_0 < u_1$. Since $\mathbf{L}$ is non-modular, it has a pentagon. Let $\langle x_0, x_1, x_2, u_1, u_0 \rangle$ be

a pentagon such that $f(x_0, x_2) = n$ is the minimum for all pentagons, and such that $f(x_0, x_1) + f(u_1, x_2) = m$ is the minimum over all pentagons $\langle y_0, y_1, y_2, v_1, v_0 \rangle$ satisfying $f(y_0, y_2) = n$.

Case 1. $f(u_1, x_2) > 2$. Choose an element e with $u_1 < e < x_2$. If $e \wedge x_1 = x_0$ then the pentagon $\langle x_0, x_1, x_2, e, u_0 \rangle$ has $f(x_0, x_1) + f(e, x_2) < f(x_0, x_1) + f(u_1, x_2)$, contradicting the minimality. Thus $e \wedge x_1 > x_0$. If $u_0 \vee (e \wedge x_1) < e$, then the pentagon $\langle e \wedge x_1, x_1, x_2, e, u_0 \vee (e \wedge x_1) \rangle$ has $f(e \wedge x_1, x_2) < f(x_0, x_2)$, contradicting the minimality. Thus $u_0 \vee (e \wedge x_1) = e$. But then the pentagon $\langle x_0, e \wedge x_1, e, u_1, u_0 \rangle$ contradicts minimality. Thus Case 1 cannot occur.

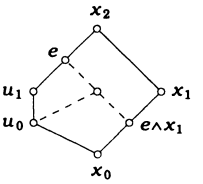


Figure 29

We thus have $u_1 \prec x_2$. We can assume that $u_0 \prec u_1$ (else replace u_0 by an element u_0' satisfying $u_0 \leq u_0' \prec u_1$).

Case 2. $f(x_0, x_1) > 2$. Choose an element e such that $x_0 \prec e < x_1$. Now $d = e \vee u_0 \not\geq u_1$, else $\langle x_0, e, d, u_1, u_0 \rangle$ is a pentagon with $f(x_0, d) \leq f(x_0, x_2)$ and $f(x_0, e) + f(u_1, d) < f(x_0, x_1) + f(u_1, x_2)$, contradicting minimality. It is easy now to check that $d \wedge u_1 = u_0$ (since $u_0 \prec u_1$), that $d \vee u_1 = x_2$ (since $u_1 \prec x_2$), and that $d \vee x_1 = x_2$.

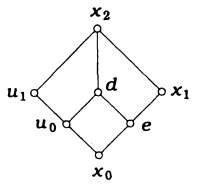


Figure 30

If $d \wedge x_1 > e$, then again, the pentagon $\langle x_0, u_0, d, d \wedge x_1, e \rangle$ contradicts minimality. Thus we have a sublattice of $\mathbf{L}$ isomorphic to $\mathbf{D}_2$.

In the remaining case, we have $u_1 \prec x_2$ and $x_0 \prec x_1$ and, as we remarked, we can arrange that $u_0 \prec u_1$. □

LEMMA 10.2. *Let* $\mathbf{A}$ *be a finite algebra having a pentagon in* $\mathbf{Con}\,\mathbf{A}$ *as pictured*

in Figure 31, with $\alpha \prec \beta$, $0 \prec \delta$, $\operatorname{typ}(\alpha, \beta) = \mathbf{2}$, *and* $\operatorname{typ}(0, \delta) \in \{\mathbf{3}, \mathbf{4}\}$. *Then* $\boldsymbol{V}(\mathbf{A})$ *is residually large.*

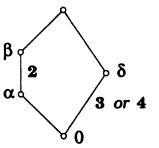


Figure 31

PROOF. Let $\{0,1\}$ be a $\langle 0_A, \delta\rangle$-trace. (See Lemma 4.17 and Remark 5.4.) Thus $\mathbf{A}|_{\{0,1\}}$ is a lattice or Boolean algebra. Since $0_A \prec \delta$, we have $\delta = \Theta(0,1)$; thus $\beta < \alpha \vee \Theta(0,1)$. It is easy to see that our assumptions imply that $C(\beta, \delta; \alpha)$ holds. (See Definition 3.3.)

Put $\mathbf{B} = \mathbf{A}/\alpha$ and change notation, so that β denotes the image in $\mathbf{B}$, under the quotient map, of the congruence in $\mathbf{A}$ with the same name, and so that 0 and 1 denote the elements of $\mathbf{B}$ corresponding to the elements of $\mathbf{A}$ with these names. We have secured the following facts.

(10.2.1) β is minimal and $\operatorname{typ}(0, \beta) = \mathbf{2}$.

(10.2.2) $\beta < \Theta(0,1)$, and $\mathbf{B}|_{\{0,1\}}$ is a minimal algebra of type **3** or **4**.

(10.2.3) For all polynomials $f(x, \bar{y})$ of $\mathbf{B}$, pairs $\langle a, b\rangle \in \beta$, and sequences $\bar{u}, \bar{v} \in \{0,1\}^n$ (where f is $n+1$-ary), we have $f(a, \bar{u}) = f(a, \bar{v}) \leftrightarrow f(b, \bar{u}) = f(b, \bar{v})$.

Now we choose $U \in \mathrm{M}_{\mathbf{B}}(0, \beta)$, choose a $\langle 0, \beta\rangle$-trace $N \subseteq U$, and a 3-ary polynomial $d(x, y, z)$ of $\mathbf{B}$ such that $d(B^3) \subseteq U$, $d|_U$ is pseudo-Mal'cev, and $d|_N$ is the operation $x - y + z$ in an $\mathbf{F}$-vector space $\mathbf{V} = \langle N, \dots\rangle$ polynomially equivalent to $\mathbf{B}|_N$. (See Lemma 4.20. Here, $\mathbf{F}$ is some finite field.) The zero element of this vector space will be denoted by e.

To prove this lemma, let κ be an arbitrary infinite cardinal. We shall construct a subdirectly irreducible algebra in $\boldsymbol{HS}(\mathbf{B}^\kappa)$ whose cardinality is at least as great as κ.

We denote by $B_\kappa(\beta)$ the set of all functions $f \in B^\kappa$ such that $\langle f(i), f(j)\rangle \in \beta$ for all $i, j < \kappa$. By $\mathbf{S}$ we denote the subalgebra of $\mathbf{B}^\kappa$ generated by $\{0,1\}^\kappa \cup B_\kappa(\beta)$. We put

$$\Sigma_e = \left\{ f \in N^\kappa \colon \{i \colon f(i) \neq e\} \text{ is finite and } \sum_{i<\kappa} f(i) = e \right\}.$$

(The sum is taken in the vector space $\mathbf{V}$, and is meaningful since it is essentially a finite sum.) Notice that Σ_e is a subset of $\mathbf{S}$ and a subspace of the vector space $\mathbf{V}^\kappa$.

We define θ to be the congruence of $\mathbf{S}$ generated by $(\Sigma_e)^2$. We define $\hat{e} = \langle e, \dots \rangle$, the zero element of the vector space $\mathbf{V}^\kappa$. We proceed to prove that

$$\hat{e}/\theta \cap U^\kappa = \Sigma_e \,. \tag{10.2.4}$$

For this proof and later, we need to observe that the polynomial operations of $\mathbf{S}$ are precisely those operations on S of the form $H(\bar{x}) = F^{(\kappa)}(\bar{z}, \bar{b}, \bar{x})$ where (for some m, n, k) $\bar{z}$ is an m-tuple of members of $\{0,1\}^\kappa$, $\bar{b}$ is an n-tuple of members of $B_\kappa(\beta)$, $\bar{x}$ is a k-tuple of variables, and F is an $m+n+k$-ary polynomial operation of $\mathbf{B}$. It is understood that for $\bar{f} = \langle f_0, \dots, f_{k-1} \rangle \in S^k$, $F^{(\kappa)}(\bar{z}, \bar{b}, \bar{f})$ is computed coordinate-wise (i.e., for $i < \kappa$, $H(\bar{f})(i) = F(\bar{z}(i), \bar{b}(i), \bar{f}(i))$).

To prove (10.2.4), we note that since U is the range of an idempotent polynomial function of $\mathbf{B}$, we have $S \cap U^\kappa = \sigma(S)$ for some unary polynomial σ of $\mathbf{S}$ satisfying $\sigma = \sigma^2$. Thus

$$\theta^* = \{\langle f, g \rangle \in S^2 : \text{ for all } H \in \mathrm{Pol}_1\mathbf{S}\,, \\ \{H(f), H(g)\} \subseteq U^\kappa \text{ implies } H(f) \in \Sigma_e \text{ iff } H(g) \in \Sigma_e\}$$

is a congruence of $\mathbf{S}$. Hence, to prove (10.2.4), it will be sufficient to show that $(\Sigma_e)^2 \subseteq \theta^*$.

So let $u_0, u_1 \in \Sigma_e$, $H \in \mathrm{Pol}_1\mathbf{S}$, $\{H(u_0), H(u_1)\} \subseteq U^\kappa$, $H(u_0) \in \Sigma_e$. We have to prove that $H(u_1) \in \Sigma_e$. Let $v_i = H(u_i)$ $(i = 0, 1)$. We write $H(x) = F^{(\kappa)}(\bar{z}, \bar{b}, \bar{x})$ as in the last paragraph. We can assume that the range of $F^{(\kappa)}$ (acting in $\mathbf{S}$) is contained in U^κ (or replace H by σH). Now since $F(\bar{z}(i), \bar{b}(i), u_0(i)) \in N$ for all $i < \kappa$, we have that $F(\bar{z}(i), \bar{b}(j), u) \in N$ for all $i, j < \kappa$ and $u \in N$ (as N is a $\beta|_U$-class and $\bar{b}(i) \equiv \bar{b}(j) (\mathrm{mod}\ \beta)$). We can therefore make some calculations in the vector space $\mathbf{V}$.

Using (10.2.3), from the equation

$$F(\bar{z}(i), \underline{\bar{b}(0)}, \underline{e}) - F(\bar{z}(i), \bar{b}(0), e) = F(\bar{z}(0), \underline{\bar{b}(0)}, \underline{e}) - F(\bar{z}(0), \bar{b}(0), e),$$

by replacing the underlined $\bar{b}(0)$, e by $\bar{b}(i)$, u we obtain

$$F(\bar{z}(i), \bar{b}(i), u) = F(\bar{z}(0), \bar{b}(i), u) - F(\bar{z}(0), \bar{b}(0), e) + F(\bar{z}(i), \bar{b}(0), e)$$

for all $i < \kappa$ and $u \in N$. A similar argument, using that β is an Abelian congruence (Theorem 5.7 (3)), shows that

$$F(\bar{z}(0), \bar{b}(i), u) = F(\bar{z}(0), \bar{b}(0), u) - F(\bar{z}(0), \bar{b}(0), e) + F(\bar{z}(0), \bar{b}(i), e)\,.$$

Thus we have, for certain $c_i \in N$,

$$F(\bar{z}(i), \bar{b}(i), u) = F(\bar{z}(0), \bar{b}(0), u) - F(\bar{z}(0), \bar{b}(0), e) + c_i \\ \text{for all } i < \kappa \text{ and } u \in N.$$

The mapping $\lambda(x) = F(\bar{z}(0), \bar{b}(0), x) - F(\bar{z}(0), \bar{b}(0), e)$ (for $x \in N$) is a polynomial of $\mathbf{B}|_N$, hence also of $\mathbf{V}$. Since $\lambda(e) = e$, there is an element $\lambda \in \mathbf{F}$ with $\lambda(x) = \lambda \cdot x$. Hence we have the equation

$$F(\bar{z}(i), \bar{b}(i), u) = \lambda \cdot u + c_i \ ,$$

so long as $u \in N$. Let $c = \langle c_i : i < \kappa \rangle$, a member of $\mathbf{V}^\kappa$. Then for $\varepsilon \in \{0,1\}$ we have $v_\varepsilon = H(u_\varepsilon) = \lambda \cdot u_\varepsilon + c$. Since $u_1 - u_0 \in \Sigma_e$, then $v_1 - v_0 = \lambda \cdot (u_1 - u_0)$ belongs to Σ_e. Since $v_0 \in \Sigma_e$, we then get that $v_1 \in \Sigma_e$, which is what we set out to prove. This finishes our proof of (10.2.4).

We choose now any element $a \in N - \{e\}$ and define, for $i < \kappa$, a_i and s_i to be the elements of $\mathbf{S}$ such that $a_i(j) = e$ and $s_i(j) = 0$ for $j \neq i$, while $a_i(i) = a$ and $s_i(i) = 1$. Note that $a_i \equiv a_j \pmod{\theta}$ for all $i, j < \kappa$; and that $a_i \not\equiv \hat{e} \pmod{\theta}$, by (10.2.4). Let us choose a maximal element $\hat{\theta}$ in the set

$$\{\psi \in \operatorname{Con} \mathbf{S} : \ \theta \leq \psi \text{ and } \langle a_0, \hat{e} \rangle \notin \psi\} \ .$$

There is a smallest congruence of $\mathbf{S}$ strictly larger than $\hat{\theta}$, namely $\hat{\theta} \vee \Theta(a_0, \hat{e})$; thus $\mathbf{S}/\hat{\theta}$ is subdirectly irreducible.

We can prove that $\mathbf{S}/\hat{\theta}$ has at least κ distinct elements by showing that $s_i/\hat{\theta} \neq s_j/\hat{\theta}$ for all $i \neq j$. Suppose otherwise, and without loss of generality, assume that $\langle s_0, s_1 \rangle \in \hat{\theta}$. We shall now employ (10.2.2), the fact that $\beta \leq \Theta(0,1)$ in **Con B**.

Case 1. Where Q is the body of U with respect to $\langle 0, \beta \rangle$, there are $h_0, \ldots, h_n \in \operatorname{Pol}_1 \mathbf{B}$ such that $\{h_0(0), h_0(1), \ldots, h_n(0), h_1(1)\} \subseteq Q$ and $\langle a, e \rangle$ lies in the equivalence relation on Q generated by the set $\rho = \{\langle h_i(0), h_i(1) \rangle : i \leq n\}$. Then since $\mathbf{B}|_Q$ is Mal'cev, the congruence on $\mathbf{B}|_Q$ generated by ρ is identical to the least reflexive subalgebra of $(\mathbf{B}|_Q)^2$ containing ρ (see Lemma 5.22), and it follows that there is some $h \in \operatorname{Pol}_1 \mathbf{B}$ with $h(0) = a$, $h(1) = e$. Since $\langle s_0, s_1 \rangle \in \hat{\theta}$, using the polynomials of $\mathbf{S}$ which act on $\{0,1\}^\kappa$ as the lattice operations of $\langle \{0,1\}, \vee, \wedge \rangle^\kappa$, we find that

$$\langle 0, 1, \ldots, 1, \ldots \rangle = s_1 \vee \langle 0, 1, \ldots, 1, \ldots \rangle \overset{\hat{\theta}}{\equiv} s_0 \vee \langle 0, 1, \ldots, 1, \ldots \rangle = \langle 1, 1, \ldots, 1, \ldots \rangle.$$

Then applying h co-ordinatewise, we get that

$$\langle a, e, \ldots, e, \ldots \rangle \overset{\hat{\theta}}{\equiv} \langle e, e, \ldots, e, \ldots \rangle,$$

i.e., that $\langle a_0, \bar{e} \rangle \in \hat{\theta}$. This contradicts our choice of $\hat{\theta}$.

Case 2. Suppose that Case 1 fails. Since $U = \sigma(B)$, $\sigma = \sigma^2$, and $\beta \leq \Theta(0,1)$, we have that $\beta|_U$ is contained in the equivalence relation generated by

$$\{\langle h(0), h(1) \rangle : h \in \operatorname{Pol}_1 \mathbf{B} \text{ and } h(0), h(1) \in U\}.$$

It follows from the failure of Case 1 that there is $h \in \mathrm{Pol}_1\mathbf{B}$ with $h(0) \in Q$ (the body of U) and $h(1) \in U - Q$ (or the same with 0 and 1 interchanged). The polynomial $f(x) = d(x, h(0), e)$ is a permutation of U (see Lemma 4.20). Hence with $q(x) = fh(x)$, we have $q(0) = e$ and $q(1) = u \in U - Q$ (since $f(Q) = Q$).

Since $s_0 \overset{\hat{\theta}}{\equiv} s_0 \wedge s_1 = \langle 0, 0, \dots \rangle$, applying q we obtain $\langle u, e, e, e, \dots \rangle \overset{\hat{\theta}}{\equiv} \bar{e}$. Therefore

$$d(\langle u, e, e, e, \dots \rangle, \bar{e}, a_0) \overset{\hat{\theta}}{\equiv} d(\bar{e}, \bar{e}, a_0) \text{ , i.e.,}$$
$$\langle d(u, e, a), e, e, e, \dots \rangle \overset{\hat{\theta}}{\equiv} a_0 \text{ .}$$

But $d(u, e, a) \overset{\beta}{\equiv} d(u, e, e) = u$, implying $d(u, e, a) = u$ since $u \in U - Q$. Thus we have

$$a_0 \overset{\hat{\theta}}{\equiv} \langle u, e, e, e, \dots \rangle \overset{\hat{\theta}}{\equiv} \bar{e} \text{ ,}$$

the same contradiction as before. This concludes the proof of the lemma. □

LEMMA 10.3. *Let* $\mathbf{A}$ *be a finite algebra having a pentagon in* $\mathbf{Con}\,\mathbf{A}$ *as pictured in Figure 32, with* $\alpha \prec \beta$ *and* $\mathrm{typ}(\alpha, \beta) \in \{\mathbf{3}, \mathbf{4}\}$. *If* $\mathbf{5} \notin \mathrm{typ}\{\boldsymbol{V}(\mathbf{A})\}$, *then* $\boldsymbol{V}(\mathbf{A})$ *is residually large.*

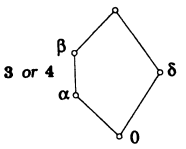


Figure 32

PROOF. We choose $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and denote its trace by $\{0, 1\}$, and its pseudo-meet operation by $p(x, y)$ (see Lemma 4.17). Since $\delta|_U \vee \alpha|_U \geq \beta|_U$ and $\delta|_U \wedge \beta|_U = 0_U$, there must exist $v \in (U - \{0, 1\}) \cap 1/\delta$. We choose such an element v and put $u = p(0, v)$. By Lemma 4.17, $u \overset{\delta}{\equiv} p(0, 1) = 0$ and $u \overset{\alpha}{\equiv} v$.

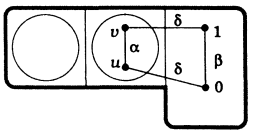


Figure 33

Letting κ be any infinite cardinal, we define elements s_i and t_i of A^κ (for $i < \kappa$) by

$$s_i(j) = 0,\ t_i(j) = 1 \text{ (for } j \neq i) \text{ and } s_i(i) = u,\ t_i(i) = v.$$

We define $\mathbf{S}$ to be the subalgebra of $\mathbf{A}^\kappa$ generated by the set

$$\{\text{constant functions}\} \cup \{s_i : i < \kappa\} \cup \{t_i : i < \kappa\}.$$

We define some congruences of $\mathbf{S}$.

$$\theta = \Theta(\{\langle s_j, t_j\rangle : j < \kappa\})$$
$$\rho_i = \Theta(\{\langle s_i, \hat{0}\rangle, \langle t_i, \hat{1}\rangle\}) \quad \text{for } i < \kappa.$$

where $\hat{0}$ and $\hat{1}$ are the constant functions. Now we claim that $\hat{1}/\theta \cap U^\kappa = \{\hat{1}\}$.

The claim can be proved by the same general method used to prove assertion (10.2.4) of the preceding proof. Let $H \in \mathrm{Pol}_1\mathbf{S}$ and $i < \kappa$ be such that $H(S) \subseteq U^\kappa$ and $H(s_i) = \hat{1}$ (or $H(t_i) = \hat{1}$, but the details of the proof would be the same). We have to prove that $H(t_i) = \hat{1}$. It is clear that $S \subseteq A_\kappa(\delta)$ and $\theta \subseteq \beta^{(\kappa)}$ (i.e., $\langle f, g\rangle \in \theta$ implies $\langle f_i, g_i\rangle \in \beta$ for all $i < \kappa$). Thus, writing $w = H(t_i)$, we have $w(j) \overset{\delta}{\equiv} w(\ell)$ and $w(j) \overset{\beta}{\equiv} 1 \overset{\beta}{\equiv} w(\ell)$ for all $j, \ell < \kappa$. Hence w is constant (since $\delta \cap \beta = 0_A$) and $w = \hat{0}$ or $w = \hat{1}$ (since $1/\beta \cap U = \{0, 1\}$). Furthermore, $w(i) \overset{\alpha}{\equiv} 1$, since $s_i(i) \overset{\alpha}{\equiv} t_i(i)$. Thus $w = \hat{1}$, as desired (since $\langle 0, 1\rangle \notin \alpha$).

From the claim, we get in particular that $\langle \hat{0}, \hat{1}\rangle \notin \theta$. Let $\hat{\theta}$ denote a congruence of $\mathbf{S}$ maximal in the set of ψ such that $\theta \leq \psi$, $\langle \hat{0}, \hat{1}\rangle \notin \psi$.

The subdirectly irreducible algebra $\mathbf{S}/\hat{\Theta}$ has cardinality κ. To prove it, we simply show that the congruences $\hat{\theta} \vee \rho_i$ are all distinct, and thus that $\mathbf{S}/\hat{\theta}$ has κ many distinct finitely generated congruences. Suppose, to the contrary, that $\hat{\theta} \vee \rho_i = \hat{\theta} \vee \rho_j$ with $i \neq j$. Note that $\langle \hat{0}, \hat{1}\rangle \in \hat{\theta} \vee \rho_i$. Since ρ_i and ρ_j are finitely generated, there must exist a finite (= finitely generated) algebra $\mathbf{T} \subseteq \mathbf{S}$ such that $\mathbf{T}$ contains all of the constant functions and the elements s_i, t_i, s_j and t_j, and

$$\hat{\theta}|_T \vee \rho_i' = \hat{\theta}|_T \vee \rho_j',$$
$$\langle \hat{0}, \hat{1}\rangle \in \hat{\theta}|_T \vee \rho_i'$$

where $\rho_i' = \Theta_{\mathbf{T}}(\{\langle s_i, \hat{0}\rangle, \langle t_i, \hat{1}\rangle\})$ and $\rho_j' = \Theta_{\mathbf{T}}(\{\langle s_j, \hat{0}\rangle, \langle t_j, \hat{1}\rangle\})$. By Theorem 7.7 (3), the congruence $\hat{\theta}|_T \vee \rho_i'$ is solvable over $\hat{\theta}|_T = \hat{\theta}|_T \vee (\rho_i' \wedge \rho_j')$. (Note that $\rho_i \wedge \rho_j = 0_S$.) However, since T contains the constant functions, $\{\hat{0}, \hat{1}\}$ is a 2-snag in $(\hat{\theta}|_T \vee \rho_i') - \hat{\theta}|_T$, which contradicts Theorem 7.2. □

THEOREM 10.4. *Every locally finite variety that omits the types* **1** *and* **5**, *and is residually small, is congruence-modular.*

PROOF. Let $\mathcal{V}$ be a locally finite variety such that $\mathrm{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{5}\} = \emptyset$ and $\mathcal{V}$ is not congruence-modular. There is a pentagon in the congruence lattice of the finite algebra $\mathbf{F}_{\mathcal{V}}(x, y, z, u)$. By Theorem 9.8, the lattice $\mathbf{D}_2$ cannot be embedded into this congruence lattice. Thus $\mathbf{Con}\,\mathbf{F}_{\mathcal{V}}(x, y, z, u)$ contains a pentagon as described in

Lemma 10.1. In a quotient algebra, we have a sublattice of congruences with $\alpha \prec \beta$ and $0 \prec \delta$. By Lemma 6.5, $\mathrm{typ}(0, \delta)$ cannot be **2**.

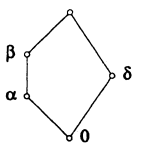


Figure 34

Using Lemma 10.2 or Lemma 10.3, we conclude that $\mathcal{V}$ is not residually small. □

Exercise 10.5. Let $\mathbf{A}$ be the eight-element algebra whose basic operations are just all the operations preserving the order of the partially ordered set depicted in Figure 35.

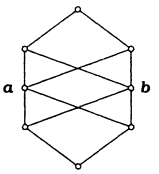


Figure 35

Prove that $\boldsymbol{V}(\mathbf{A})$ is not congruence-modular. (Assuming that there are 3-ary operations $d_0, \ldots, d_n, p$ of $\mathbf{A}$ satisfying the equations in Theorem 8.1, show that $d_i(a, x, b) = a$ for all $x \in A$, $i \leq n$; then derive a contradiction.) Prove that $\boldsymbol{V}(\mathbf{A})$ omits the types **1** and **5**. (Show that $\mathbf{A}$ has operations obeying the equations in Theorem 9.8 (4) with $n = 6$.) Conclude, by Theorem 10.4, that $\boldsymbol{V}(\mathbf{A})$ is residually large. [The algebra $\mathbf{A}$ is **pre-primal**, that is, Clo $\mathbf{A}$ is a maximal proper subclone of the clone of all operations on its universe. This seems to be the first example of a residually large variety generated by a pre-primal algebra. It is also probably the most difficult exercise in this book.]

11. DECIDABLE VARIETIES

Loosely speaking, a class of algebras is **decidable** if there is an algorithm that can be applied to any sentence to determine if the sentence is valid in all members of the class. One of the most important achievements of mathematical logic in this century has been to supply a precise and workable mathematical definition of this concept—a class is decidable if and only if its first order theory is a **recursive** set of first order sentences. By mid-century, the decidability or undecidability of many specific classes of algebras and relational structures had been determined.

If a class is decidable then, in a certain sense, its members cannot be very complex. The theory of graphs is non-recursive; indeed, there is no recursive set of sentences containing every sentence valid in all graphs and containing no sentence which fails to be valid in some finite graph. ("Sentence" here is understood to mean sentence in the first order language of graphs. The result was proved by I.A. Lavrov [21].) For the classes which are varieties, most of the classes known to be undecidable were proved to be so by interpreting into them some class of graphs, including all finite graphs, in such a way that the undecidability follows from Lavrov's result. By constructing such interpretations, A.P. Zamyatin [34] proved that every non-Abelian variety of groups is undecidable. Finite graphs can certainly be enormously complicated. A variety into which finite graphs can be interpreted contains algebras at least as complicated as any given finite graph.

Decidable varieties are really quite rare. The varieties of semilattices, of distributive lattices, of lattices, and of algebras with two unary operations are undecidable. On the other hand, every variety of Abelian groups, every variety of algebras with one unary operation, the variety of Boolean algebras, and any variety of rings generated by finitely many finite fields, is decidable. (References for all facts stated here can be found in [5].)

We believe that in seeking to find an algebraic characterization of the family of all decidable varieties, one will be led to a clearer understanding of the ways in which a variety can be well-structured (i.e., possess algebras whose structural features are classifiable and describable, in some sense), or poorly structured. In this chapter, we show that tame congruence theory is a powerful tool for the investigation of decidability in locally finite varieties. We prove that every locally finite, decidable variety satisfying a non-trivial idempotent Mal'cev condition (i.e., omitting the unary type) is congruence-modular. Combining this result with the chief theorem of [5]

(Theorem 9.1), we conclude that in such a variety every algebra decomposes as the direct product of an Abelian algebra and a centerless algebra, and the centerless algebras in the variety constitute a discriminator variety. As in [5], the decidability question for finitely generated varieties that omit the unary type reduces to the decidability question for varieties of modules over finite rings. These results were proved in [5] for congruence-modular varieties.

Here is the plan of this chapter. It contains four constructions of interpretations. For locally finite $\mathcal{V}$ admitting one of the types **4** and **5**, we show how to interpret the variety of bounded distributive lattices or the variety of bounded semilattices into $\mathcal{V}$. In either case, it follows that $\mathcal{V}$ is **hereditarily undecidable**—if $\mathcal{K}$ is any class of algebras similar to those in $\mathcal{V}$ and if $\mathcal{V} \subseteq \mathcal{K}$, then $\mathcal{K}$ must be undecidable. Then, assuming that some finite algebra in $\mathcal{V}$ has a prime quotient $\langle \alpha, \beta \rangle$ of type **2** or **3** and an $\langle \alpha, \beta \rangle$-minimal set with a non-empty tail, we show how to interpret the class of "atomic Boolean pairs" (relational structures defined in [5]) into $\mathcal{V}$. From these results, and Theorem 8.5 in this book, it follows that if $\mathbf{1} \notin \text{typ}\{\mathcal{V}\}$ and $\mathcal{V}$ fails to be congruence-modular, then $\mathcal{V}$ is hereditarily undecidable.

LEMMA 11.1. *Every locally finite variety $\mathcal{V}$ such that $\text{typ}\{\mathcal{V}\} \cap \{\mathbf{4}, \mathbf{5}\} \neq \emptyset$ is hereditarily undecidable.*

PROOF. We assume that $\mathbf{5} \in \text{typ}\{\mathcal{V}\}$ and show how to interpret bounded semilattices into $\mathcal{V}$. (If $\mathbf{4} \in \text{typ}\{\mathcal{V}\}$, a very similar construction interprets bounded distributive lattices into $\mathcal{V}$.) It is well known that the variety of bounded semilattices (and the variety of bounded distributive lattices) interpret the class of all graphs. Each of these classes is finitely axiomatizable and undecidable. Hence it follows that $\mathcal{V}$ is hereditarily undecidable, if we can interpret one of these classes into it. The interpretation we use has been more or less defined in Chapter 6 (starting with Definition 6.12), but was not shown there to be first order definable.

We begin by fixing a finite algebra $\mathbf{A} \in \mathcal{V}$ and a minimal congruence β on $\mathbf{A}$ with $\text{typ}(0_A, \beta) = \mathbf{5}$. Let $U \in \text{M}_{\mathbf{A}}(0, \beta)$, and let $N = \{0, 1\}$ be the $\langle 0, \beta \rangle$-trace in U, and let $p(x, y)$ be a polynomial of $\mathbf{A}$ such that $p|_U$ is a pseudo-meet operation with respect to $\langle 0_U, \beta|_U \rangle$. (See Lemma 4.15–Definition 4.16.) Notice that $N = \{x \in U : p(x, 0) = 0\}$ and $U - \{1\} = \{x \in U : p(x, 0) = x\}$.

Now let $\mathbf{S} = \langle S, \wedge, \overline{0}, \overline{1} \rangle$ be any bounded semilattice. There is only one subdirectly irreducible bounded semilattice, within isomorphism, namely $\langle \{0, 1\}, \wedge, 0, 1 \rangle$. Thus $\mathbf{S}$ is isomorphic to, and we may assume it is equal to, a subalgebra of $\langle \{0, 1\}, \wedge, 0, 1 \rangle^\kappa$ for some finite or infinite cardinal κ. (Here, $\kappa = 0$ and $|S| = 1$ is an allowed possibility.)

We define $\mathbf{B} = \mathbf{A}_\kappa(S)$, the subalgebra of $\mathbf{A}^\kappa$ generated by all the constant functions together with the members of the set $S \subseteq N^\kappa$. It follows from Lemma 6.14 (2) that $S = B \cap N^\kappa$ (since the term operations of $\langle \{0, 1\}, \wedge, 0, 1 \rangle$ are the same as those of $\mathbf{A}|_N$). We can now show that the algebra $\mathbf{S}$ is first order definable in $\mathbf{B}$. (The

formulas to be used depend on $\mathbf{A}$, but not on $\mathbf{S}$.)

Let $e \in \mathrm{E}(\mathbf{A})$ with $U = e(A)$. There are terms $\varepsilon(x, \bar{y})$ and $\rho(x, y, \bar{z})$ in the language of $\mathcal{V}$ and elements $a_1, \ldots, a_n, b_1, \ldots, b_m$ in A such that

$$e(x) = \varepsilon(x, a_1, \ldots, a_n)$$
$$p(x, y) = \rho(x, y, b_1, \ldots, b_m)$$

for all $x, y \in A$. Let $\hat{0}, \hat{1}, \hat{a}_1, \ldots, \hat{b}_m$ be the constant functions (elements of B) constructed from the corresponding elements of A. It is now trivial to see that where μ, η, θ are the formulas

$$\mu(x): \ \varepsilon(x, \hat{a}_1, \ldots, \hat{a}_n) = x$$
$$\eta(x): \ \mu(x) \ \& \ \rho(x, \hat{0}, \hat{b}_1, \ldots, \hat{b}_m) = \hat{0}$$
$$\theta(x, y, z): \ \rho(x, y, \hat{b}_1, \ldots, \hat{b}_m) = z,$$

for any $f, g, h \in B$ we have

$$f \in U^{\kappa} \ \leftrightarrow \ \mathbf{B} \models \mu(f)$$
$$f \in S \ \leftrightarrow \ \mathbf{B} \models \eta(f)$$
$$f \wedge g = h \ \leftrightarrow \ \mathbf{B} \models \theta(f, g, h) \quad \text{if } f, g, h \in S.$$

Thus the algebra $\mathbf{S}$ is definable in $\mathbf{B}$ by these fixed formulas using the parameters $\hat{0}, \hat{1}, \hat{a}_1, \ldots, \hat{b}_m$.

For every bounded semilattice $\mathbf{S}$, there is an algebra $\mathbf{B} \in \mathcal{V}$ and elements $\hat{0}, \hat{1}, \hat{a}_1, \ldots, \hat{b}_m \in B$ such that our formulas define in $\mathbf{B}$ an algebra isomorphic to $\mathbf{S}$ (as was shown above). Thus we have an interpretation, in the sense defined and used in [5], of bounded semilattices in $\mathcal{V}$. □

LEMMA 11.2. *Let $\mathcal{V}$ be a locally finite variety having a finite algebra $\mathbf{A}$ with a prime quotient $\langle \alpha, \beta \rangle$ of type 3 and a set $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ with a non-empty $\langle \alpha, \beta \rangle$-tail. $\mathcal{V}$ is hereditarily undecidable.*

PROOF. Let $\delta \geq \alpha$ be maximal in $\mathbf{Con}\ \mathbf{A}$ with $\delta \not\geq \beta$. Thus $\delta \prec \gamma = \delta \vee \beta$ and $\delta \wedge \beta = \alpha$. By Lemma 6.2, combined with the detailed picture of $\langle \alpha, \beta \rangle$-minimal sets supplied in Lemma 4.17, we have the same facts with regard to $\langle \delta, \gamma \rangle$ that we have assumed to hold for $\langle \alpha, \beta \rangle$. By Lemma 2.18, this situation persists when we factor $\mathbf{A}$ by δ. Thus we can assume that $\alpha = 0_A$ and that $\mathbf{A}$ is subdirectly irreducible with monolith (smallest non-zero congruence) β.

Let X be a set and $\langle B_1, B_0, \leq \rangle$ be a structure of the following kind. Each of B_0 and B_1 is a subset of the set of all subsets of X, closed under Boolean operations of union, intersection and complementation (i.e., they are subalgebras of the Boolean algebra

Su (X)); $B_0 \subseteq B_1$; every finite subset of X belongs to B_0; and $\leq$ is set-inclusion restricted to B_1. The class of all such structures, $\mathcal{BP}_1$, has a finitely axiomatizable, undecidable theory [5, Theorem 6.2]. While working with a specific member of $\mathcal{BP}_1$, we will show how to interpret the whole class into $\mathcal{V}$.

Choose and fix a set $U \in \mathrm{M}_{\mathbf{A}}(0_A, \beta)$, and let $N = \{0,1\}$ be the $\langle 0_A, \beta\rangle$-trace in U, and $p(x,y)$, $q(x,y)$ be polynomials of $\mathbf{A}$ under which U and N are closed and such that $\langle \{0,1\}, p|_N, q|_N\rangle = \langle \{0,1\}, \wedge, \vee\rangle$ and $p|_U$, $q|_U$ have the properties of pseudo-meet and pseudo-join operations (Lemma 4.17–Definition 4.18). Given $C \subseteq A$ and $B_i \in \{B_0, B_1\}$, define

$$C[B_i] \;=\; \{f \in C^X : f^{-1}(c) \in B_i \text{ for all } c \in C\}\,.$$

Choose an element $u \in U - \{0,1\}$ (the tail of U). Let $\mathbf{D}'$ be the subalgebra of $\mathbf{A}^X$ generated by

$$\{\text{constant functions}\} \cup \{0,u\}[B_0] \cup \{0,1\}[B_1].$$

Let $\mathbf{D}$ be the ae-closure of $\mathbf{D}'$, i.e., $f \in D$ iff $f \in A^X$ and for some $g \in D'$ the set

$$[\![f \neq g]\!] = \{x\colon f(x) \neq g(x)\}$$

is finite.

Our goal is to interpret the structure $\langle B_1, B_0, \leq\rangle$ into $\mathbf{D}$, using first order formulas with finitely many constant functions $\hat{a}$ $(a \in A)$ as parameters. Below, "definable" means definable in $\mathbf{D}$ by first order formulas using constant functions as parameters. We shall not bother to actually write out all the formulas to be used.

Notice that $\mathbf{D}$ is contained in the subalgebra $\mathbf{A}[B_1]$ of $\mathbf{A}^X$. In particular, $D \cap \{0,1\}^X \subseteq \{0,1\}[B_1]$, and this inclusion is an equality. We shall write $D(0,1)$ for the set $D \cap \{0,1\}^X$.

(11.2.1) $D(0,1) = \{0,1\}[B_1]$ and this set is definable.

(11.2.2) The natural order on $D(0,1)$, i.e., $f \leq g$ iff $f^{-1}(1) \subseteq g^{-1}(1)$, is a definable relation.

The first claim follows easily by the argument used in the last proof. The second claim is also easy to prove; for $f, g \in D(0,1)$ we have $f \leq g$ iff $p^{(X)}(f,g) = f$, where $p^{(X)}$ is the binary polynomial of D which acts coordinate-wise like p.

For $x \in X$ we define 1_x to be the element $f \in D(0,1)$ such that $f^{-1}(1) = \{x\}$. We put $\tilde{X} = \{1_x\colon x \in X\}$. We now assert that

(11.2.3) $\langle D(0,1)\,,\, \leq\rangle$ is isomorphic to $\langle B_1\,,\, \subseteq\rangle$.

(11.2.4) $\tilde{X}$ is definable.

(11.2.5) This relation is definable:

$$\Xi = \{\langle f,g\rangle \in D^2 : f \in U^X \text{ and } g = 1_x \text{ for an } x \text{ such that } f(x) \neq 1\}\,.$$

Claim (11.2.3) should be obvious, after the earlier claims. Then (11.2.4) follows from the observation that $\tilde{X}$ is the set of covers of $\hat{0}$ in the partially ordered set $D(0,1)$. Now $D \cap U^X$ is definable, as in the proof of Lemma 11.1. To verify (11.2.5), note that when $f \in U^X$ and $g = 1_x$ then $f(x) = 1$ iff $p^{(X)}(f,g) \neq p^{(X)}(f,\hat{0})$. (Recall from Lemma 4.17 that $p(a,0) = p(a,1) = a$ for all $a \in U - \{1\}$ while $p(1,0) = 0$, $p(1,1) = 1$.)

(11.2.6) This relation is definable:

$$\Lambda = \{\langle f,g,h\rangle \in D^3 : \ h = 1_x \text{ for an } x \text{ such that } f(x) \neq g(x)\}\,.$$

The proof of (11.2.6) is the hardest piece of our argument. The relation

$$\{\langle a,b\rangle \in A^2 : \text{ for all } f \in \mathrm{Pol}_1\mathbf{A}\,,\ f(A) \subseteq U \text{ implies } f(a) = 1 \text{ iff } f(b) = 1\}$$

is easily seen to be a congruence of $\mathbf{A}$ separating 0 and 1. Since $\langle 0,1\rangle$ belongs to the monolith, β, the congruence just defined is trivial. Thus whenever $a \neq b$ there is $f \in \mathrm{Pol}_1\mathbf{A}$ with $f(A) \subseteq U$ and $f(a) = 1 \leftrightarrow f(b) \neq 1$. We list all unary polynomials mapping A into U as $f_1,\dots,f_m$. Letting $A = \{a_1,\dots,a_n\}$, we select $n+1$-ary terms $t_1,\dots,t_m$ so that $f_i(y) = t_i(y,a_1,\dots,a_n)$. Now if $f,g \in D$ and $x \in X$ then $f(x) \neq g(x)$ iff for at least one $i \in \{1,\dots,m\}$,

$$\langle t_i(f,\bar{a}_1,\dots,\bar{a}_m),1_x\rangle \in \Xi \leftrightarrow \langle t_i(g,\bar{a}_1,\dots,\bar{a}_m),1_x\rangle \notin \Xi$$

(with Ξ specified by (11.2.5)). Thus Λ is definable.

Recalling that u is an element we selected in the tail of U, we define $D(0,u) = D \cap \{0,u\}^X$.

(11.2.7) $D(0,u)$ is a definable set.

Indeed, $f \in D(0,u)$ iff $f \in D$ and for no $g \in \tilde{X}$ do we have both $\Lambda(f,\hat{0},g)$ and $\Lambda(f,\hat{u},g)$.

(11.2.8) $D(0,u) = \{0,u\}[B_0]$.

It is clear that $\{0,u\}[B_0] \subseteq D(0,u)$. To prove the other inclusion, suppose that $f \in D$ and $f(X) \subseteq \{0,u\}$. From our definition of D, there is some f' in D' which agrees with f at all but finitely many $x \in X$; and there are are finitely many elements

$$f_1,\dots,f_k \in \{0,u\}[B_0]\,;\ g_1,\dots,g_\ell \in \{0,1\}[B_1]$$

and a polynomial $t(y_1,\dots,y_k,z_1,\dots,z_\ell)$ of $\mathbf{A}$ such that

$$f' = t^{(X)}(f_1,\dots,f_k,g_1,\dots,g_\ell) = t^{(X)}(\bar{f},\bar{g})\,.$$

We can assume that $t(A^{k+\ell}) \subseteq U$ (or compose t with an idempotent polynomial whose range is U). Now if $t(\bar{a}, \bar{b}) = u$ for elements $\bar{a} \in A^k$, $\bar{b} \in \{0,1\}^\ell$, then $t(\bar{a}, \bar{c}) \equiv u \pmod{\beta}$ for any $\bar{c} \in \{0,1\}^\ell$, and thus $t(\bar{a}, \bar{c}) = u$ since $u/\beta \cap U = \{u\}$. Thus if we put

$$f'' = t^{(X)}(f_1, \ldots, f_k, \hat{0}, \ldots, \hat{0})$$

then $f''^{-1}(u) = f'^{-1}(u)$. Since obviously $f'' \in A[B_0]$, we have $f'^{-1}(u) \in B_0$. But then $f^{-1}(u) \in B_0$, because B_0 contains all the finite subsets of X and f and f' agree almost everywhere. Thus $f^{-1}(0) = X - f^{-1}(u) \in B_0$ also, and $f \in \{0,u\}[B_0]$ as we claimed.

(11.2.9) $\{0,1\}[B_0]$ is definable.

To prove this, we note that any $f \in D(0,1)$ belongs to $\{0,1\}[B_0]$ iff for some (unique) $g \in \{0,u\}[B_0]$, $f^{-1}(1) = g^{-1}(u)$. When $f \in D(0,1)$ and $g \in D(0,u)$ then $f^{-1}(1) \subseteq g^{-1}(u)$ iff $q^{(X)}(f,g) = g$. (Recall that q is the pseudo-join operation, which means that $q(1,u) = u$, $q(1,0) = 1$ and $q(0,a) = a$ for all $a \in U$.) Thus the formula $f \in \{0,1\}[B_0]$ is equivalent to: for some $g \in D(0,u)$, f is the largest (under $\leq$) member of $D(0,1)$ such that $q^{(X)}(f,g) = g$.

Now the structure $\langle \{0,1\}[B_1], \{0,1\}[B_0], \leq \rangle$ is isomorphic to $\langle B_1, B_0, \subseteq \rangle$; and by (11.2.1), (11.2.2) and (11.2.9) this structure is definable in $\mathbf{D}$. □

LEMMA 11.3. *Let $\mathcal{V}$ be a locally finite variety having a finite algebra $\mathbf{A}$ with a prime quotient $\langle \alpha, \beta \rangle$ of type 2 and a set $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ with a non-empty $\langle \alpha, \beta \rangle$-tail. $\mathcal{V}$ is hereditarily undecidable.*

PROOF. As before, we can assume that $\alpha = 0_A$. Let $d(x,y,z)$ be a polynomial of $\mathbf{A}$ for which $d|_U$ is a pseudo-Mal'cev operation on U with respect to $\langle 0_U, \beta|_U \rangle$ (See Lemma 4.20–Definition 4.22.) Let Q be the body and $T \neq \emptyset$ be the tail of U with respect to $\langle 0_U, \beta|_U \rangle$. Let $0 \in Q$, $N = 0/\beta|_U$, and $1 \in N - \{0\}$. We know that for $u \in Q$, the polynomial $f_u(x) = d(u,0,x)$ defines a permutation on U, while, for $u \in T$, $f_u(x)$ is constant on N. For any $u \in U$, let

$$k(u) = \ker f_u|_U = \{\langle x, y \rangle \in U^2 \colon d(u,0,x) = d(u,0,y)\} .$$

Then choose $u_0 \in T$ with $k(u_0)$ minimal. Thus $N^2 \subseteq k(u_0)$; and every $u \in U$ satisfies: $k(u) < k(u_0) \Leftrightarrow k(u) = 0_U \Leftrightarrow u \in Q$.

Having chosen $0, 1, u_0$, we now consider any structure $\langle B_1, B_0, \subseteq \rangle$ with $B_0 \subseteq B_1 \subseteq \mathrm{Su}(X)$, of the kind we used in proving the last lemma. Again we take for $\mathbf{D}$ the ae-closure of the subalgebra of $\mathbf{A}^X$ generated by

$$\{\text{constant functions}\} \cup \{u_0, 0\}[B_0] \cup \{0,1\}[B_1].$$

For $a, b \in U$ we write $a \trianglelefteq b$ iff $k(a) \subseteq k(b)$ (defined above); and for $f, g \in D \cap U^X$ we write $f \trianglelefteq g$ iff $k(f) \subseteq k(g)$ where

$$k(f) = \{\langle r, s \rangle \in D \cap U^X \ : \ d^{(X)}(f, \hat{0}, r) = d^{(X)}(f, \hat{0}, s)\} .$$

(11.3.1) The sets $D(U) = D \cap U^X$, $D(Q) = D \cap Q^X$, $D(T) = D \cap T^X$ are definable, as is the relation $\trianglelefteq$ on $D(U)$.
For $f, g \in D(u)$, $f \trianglelefteq g$ iff for all $x \in X$, $f(x) \trianglelefteq g(x)$.

The proof of this is quite easy. $D(U)$ is definable as in previous proofs. Then $\trianglelefteq$ in D is definable (we defined it), and its claimed property is easily established using the ae-closed property of D. We have $f \in D(Q)$ iff $f \in D(U)$ and $f \trianglelefteq \hat{0}$; and we have $f \in D(T)$ iff $f \in D(U)$ and $d^{(X)}(f, \hat{0}, \hat{1}) = f$.

We write $a \sim b$ (where $a, b \in U$) for $a \trianglelefteq b \trianglelefteq a$; and we write $f \sim g$ (where $f, g \in D(U)$) for $f \trianglelefteq g \trianglelefteq f$. We write $a \triangleleft b$ for "$a \trianglelefteq b$ and not $b \trianglelefteq a$", and similarly with $f \triangleleft g$. Notice that for $f \in D(U)$, $f \trianglelefteq \hat{u}_0$ iff for all x, $f(x) \in Q$ or $f(x) \sim u_0$.

(11.3.2) The set $D(0,1) = D \cap \{0,1\}^X$ is definable and equals $\{0,1\}[B_1]$.
The natural order in $D(0,1)$ is definable.

That $D(0,1) = \{0,1\}[B_1]$ should be obvious since, as in the last proof,

$$\{0,1\}[B_1] \subseteq D \subseteq A[B_1] .$$

An element $f \in D(U)$ belongs to $D(0,1)$ iff for every $g \in D(U)$ such that $g \triangleleft \hat{u}_0$ there is $h \in D(U)$ with $g \trianglelefteq h \triangleleft \hat{u}_0$ and $\langle f, \hat{0} \rangle \in k(h)$ or $\langle f, \hat{1} \rangle \in k(h)$. We ask the reader to verify this assertion, which shows that $D(0,1)$ is definable. To define the natural order in $D(0,1)$, we note that when $f, g \in D(0,1)$ then $f \leq g$ iff whenever $h \in D(U)$ and $h \trianglelefteq \hat{u}_0$ then $\langle g, \hat{0} \rangle \in k(h)$ implies $\langle f, \hat{0} \rangle \in k(h)$.

(11.3.3) For every $f \in D(U)$, $f^{-1}(T) \in B_0$.

This claim is demonstrated in exactly the same manner that we used in showing, in the proof of Lemma 11.2, that $D(0,u) = \{0,1\}[B_0]$. (Details left to the reader.)

(11.3.4) The set $\{0,1\}[B_0] \subseteq D(0,1)$ is definable.

To see this, observe that if $f \in D(U)$, $g \in D(0,1)$, and $f \trianglelefteq \hat{u}_0$, then $g^{-1}(1) \subseteq f^{-1}(T)$ iff $\langle g, \hat{0} \rangle \in k(f)$. Now by (11.3.3), since $\{0, u_0\}[B_0] \subseteq D$ we have

$$B_0 = \{f^{-1}(T) : f \in D(U) \text{ and } f \trianglelefteq \hat{u}_0\} ;$$

and thus any $g \in D(0,1)$ belongs to $\{0,1\}[B_0]$ iff there is a smallest (in the sense of $\trianglelefteq$) $f \trianglelefteq \hat{u}_0$ such that $f \in D(U)$ and $\langle g, \hat{0} \rangle \in k(f)$.

Now (11.3.2) and (11.3.4) yield the definability of $\langle \{0,1\}[B_1] , \{0,1\}[B_0] , \leq \rangle$. As with the previous lemma, that concludes our proof. □

THEOREM 11.4. *Every locally finite variety $\mathcal{V}$ with $\mathbf{1} \notin \mathrm{typ}\{\mathcal{V}\}$ is either hereditarily undecidable or congruence-modular.*

PROOF. If $\mathbf{1} \notin \mathrm{typ}\{\mathcal{V}\}$ and $\mathcal{V}$ is not hereditarily undecidable, then Theorem 8.5 and Lemmas 11.1–11.3 imply that $\mathcal{V}$ is congruence-modular. □

Remark 11.5. In April 1986, R. McKenzie and M. Valeriote completed a proof that every locally finite and not hereditarily undecidable variety $\mathcal{V}$ decomposes as a varietal product, $\mathcal{V} = \mathcal{V}_1 \otimes \mathcal{V}_2 \otimes \mathcal{V}_3$, of three special varieties satisfying $\text{typ}\{\mathcal{V}_i\} = \{\mathbf{i}\}$. As in [5], the precise result obtained reduces the decidability question for all finitely generated varieties to the same question for varieties of modules over finite rings. The proof of this result is being prepared for publication; it makes heavy use of tame congruence theory.

12. FREE SPECTRA

The **free spectrum** of a variety $\mathcal{V}$ is the function, denoted $f_{\mathcal{V}}$, with domain the set of positive integers, such that $f_{\mathcal{V}}(n)$ is the cardinality of the free algebra in $\mathcal{V}$ freely generated by n elements. For example, the free spectrum of Boolean algebras is

$$f(n) = 2^{2^n}.$$

The precise determination of the free spectrum, $d(n)$, of the variety of distributive lattices is an old problem in combinatorics—still unsolved, although various asymptotic formulas are known. It is easy to see that

$$2^{\binom{n}{[\frac{n}{2}]}} \leq d(n) < 2^{2^n}.$$

A variety is locally finite iff its free spectrum is a finite-valued function. Various properties of locally finite varieties seem to be loosely related to the magnitude and the rate of growth of their free spectra. If $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$ then $f_{\mathcal{V}}(n) = |\mathrm{Clo}_n\mathbf{A}|$ for all n. The free spectrum of a variety enumerates the cardinalities of the sets of n-ary members of the clone of that variety (for $n = 1, 2, 3, \ldots$) and may be thought of as simply the "cardinality" of the clone. If $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$ and $\mathbf{A}$ is a finite k-element algebra, then $f_{\mathcal{V}}(n) \leq k^{k^n} \leq 2^{2^{cn}}$ for some constant c.

One of the few results showing an influence of the free spectrum is described in H. Neumann's book [25], p. 180: A finitely generated variety of groups is nilpotent of class k iff $f_{\mathcal{V}}(n) \leq 2^{c \cdot n^k}$ for some constant c. Part of this result, for $k = 1$, generalizes: If $\mathbf{A}$ is a finite Abelian algebra (see Chapter 3) and $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$, then $f_{\mathcal{V}}(n) \leq 2^{c \cdot n}$ for a constant c (see [3]).

Tame congruence theory yields several new results regarding free spectra which we have no idea how to prove outside the theory. We begin with a known result.

THEOREM 12.1. *(J. Berman [2]) The following are equivalent for any variety $\mathcal{V}$ and integer $k \geq 1$.*

(1) *$f_{\mathcal{V}}(n) \leq c \cdot n^k$ for some c (and for all n).*
(2) *There is a polynomial $p(x)$ with rational coefficients and of degree $\leq k$ such that $f_{\mathcal{V}}(n) = p(n)$ for large n.*
(3) *$\mathcal{V}$ is locally finite and has no term operations depending on more than k variables.*

PROOF. Suppose that (3) holds. Let $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$ so that $f_{\mathcal{V}}(n) = |\mathrm{Clo}_n\mathbf{A}|$ for all n. Let $e_n (0 \leq n < \omega)$ be the number of operations in $\mathrm{Clo}_n\mathbf{A}$ that depend on all n arguments. Then e_n is finite, and $= 0$ if $n > k$. For $n \geq k$, since each member of $\mathrm{Clo}_n\mathbf{A}$ depends on a unique set of at most k of its arguments, we can calculate that

$$f_{\mathcal{V}}(n) = \sum_{i=0}^{k} e_i \cdot \binom{n}{i} = p(n)$$

where $p(x)$ is obviously a polynomial. Thus (3) implies (2).

Clearly (2) implies (1). Finally, if (1) holds, then for all $n > k' > k$, we have $e_{k'} \cdot \binom{n}{k'} \leq f_{\mathcal{V}}(n) \leq c \cdot n^k$, which implies that $e_{k'} = 0$. Thus (1) implies (3). □

THEOREM 12.2. *Let $\mathcal{V}$ be a finitely generated variety. Either $f_{\mathcal{V}}(n) \leq c \cdot n^k$ for some finite c and k, or else $f_{\mathcal{V}}(n) \geq 2^{n-k}$ for some positive integer k and for all n.*

PROOF. Let $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$ where $\mathbf{A}$ is a finite k-element algebra, and suppose that Theorem 12.1(1) fails. Thus for all n, $\mathbf{A}$ has term operations depending on at least n arguments. Let $p_n = |\mathrm{Pol}_n\mathbf{A}|$ and let e_n be the number of operations in $\mathrm{Pol}_n\mathbf{A} = \mathrm{Clo}_n(\mathbf{A}, a\ (a \in A))$ that depend on all n arguments. By Theorem 12.1 and Corollary 4.2, we have $e_n \geq 1$ for all $n \geq 1$. Thus

$$p_n = k + \sum_{u=1}^{n} e_u \cdot \binom{n}{u} \geq$$

$$k + \sum_{u=1}^{n} \binom{n}{u} = k - 1 + 2^n.$$

Let $A = \{a_0, \ldots, a_{k-1}\}$ and $\bar{a} = \langle a_0, \ldots, a_{k-1}\rangle$. Since every f in $\mathrm{Pol}_n\mathbf{A}$ is of the form $f(\bar{x}) = g(\bar{x}, \bar{a})$, $g \in \mathrm{Clo}_{n+k}\mathbf{A}$, it follows that

$$f_{\mathcal{V}}(n+k) = |\mathrm{Clo}_{n+k}\mathbf{A}| \geq p_n \geq 2^n.$$

Thus $f_{\mathcal{V}}(n) \geq 2^{n-k}$ for all $n \geq k$, and this trivially holds for $n < k$. □

THEOREM 12.3. *Let $\mathcal{V}$ be a non-trivial locally finite, congruence-distributive variety (or more generally, assume that $\mathrm{typ}\{\mathcal{V}\} \cap \{\mathbf{3}, \mathbf{4}\} \neq \emptyset$). Then for every c such that $0 < c < 1$, and for large n, we have $f_{\mathcal{V}}(n) \geq 2^{2^{cn}}$.*

PROOF. It follows from Theorem 8.6 that if $\mathcal{V}$ is non-trivial (i.e., if $f_{\mathcal{V}}(2) > 1$), locally finite, and congruence distributive, then $\{\mathbf{3}, \mathbf{4}\} \cap \mathrm{typ}\{\mathcal{V}\} \neq \emptyset$.

Let $\mathbf{A}$ be a finite algebra in $\mathcal{V}$ and $\langle \alpha, \beta\rangle$ a prime quotient in $\mathbf{A}$ of type **3** or **4**. Let $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, $N = \{0, 1\}$ be the $\langle \alpha, \beta\rangle$-trace of U, and $p(x, y)$ and $q(x, y)$ be polynomials of $\mathbf{A}$ inducing pseudo-meet and pseudo-join operations in U (Lemma 4.17–Definition 4.18). Assume that $\mathbf{A}$ has k elements. Thus for all n,

$$f_{\mathcal{V}}(n+k) \geq |\mathrm{Clo}_{n+k}\mathbf{A}| \geq |\mathrm{Pol}_n\mathbf{A}|\,.$$

Let $d(n) = |\mathrm{Clo}_n\langle\{0,1\}, \wedge, \vee\rangle|$, the free spectrum of distributive lattices. Since $p|_{\{0,1\}} = \wedge$ and $q|_{\{0,1\}} = \vee$, we have that $|\mathrm{Pol}_n\mathbf{A}| \geq d(n)$ for all n. Thus

$$f_{\mathcal{V}}(n) \geq d(n-k) \text{ for } n > k\,.$$

Now $d(n)$ is equal to the number of non-void anti-chains (sets of incomparable elements) in the partially ordered set of non-empty subsets of an n-element set. Any collection of subsets which are all the same size is an anti-chain, so

$$d(n) \geq 2^{\binom{n}{[\frac{n}{2}]}}.$$

Given any c with $0 < c < 1$, choose r so that $c < r < 1$. Using Stirling's formula, it can be shown that for large n,

$$\binom{n}{[\frac{n}{2}]} \geq 2^{rn}.$$

Thus

$$f_{\mathcal{V}}(n) \geq 2^{2^{r(n-k)}},$$

and for large n this will be $\geq 2^{2^{cn}}$. (The argument in this paragraph was supplied by J. Berman.) □

The next results involve the concepts of nilpotency introduced in Definition 4.35.

LEMMA 12.4. *Let* $\mathbf{A}$ *be a finite algebra such that* $\mathrm{typ}\{\mathbf{A}\} \cap \{\mathbf{1}, \mathbf{5}\} = \emptyset$ *and* $\mathbf{A}$ *is not right nilpotent. There is a constant* $c > 0$ *such that* $|\mathrm{Clo}_n\mathbf{A}| \geq 2^{2^{cn}}$ *for large* n.

PROOF. Since $1_A \geq [1)^2 \geq [1)^3 \geq \ldots$, $\mathbf{A}$ must have a non-zero congruence β such that $[\beta, 1_A] = \beta$. By choosing any α such that $\alpha \prec \beta$, and considering $\mathbf{A}/\alpha$ in place of $\mathbf{A}$, we can arrange that $0_A \prec \beta$ and $[\beta, 1_A] = \beta$. Now if $\mathrm{typ}(0_A, \beta) = \mathbf{3}$ or $\mathbf{4}$ then the desired conclusion follows from Theorem 12.3, applied to $\boldsymbol{V}(\mathbf{A})$. Thus we only have to demonstrate the desired conclusion under the hypothesis that $\mathrm{typ}(0_A, \beta) = \mathbf{2}$. Let this be the case, let $U \in \mathrm{M}_{\mathbf{A}}(0_A, \beta)$, and let N be a $\langle 0_A, \beta\rangle$-trace in U.

Choose any $a \neq b$ in N. The center of $\mathbf{A}$, $Z(\mathbf{A})$, defined in Exercise 3.2(5), is the largest congruence δ for which $[\delta, 1_A] = 0_A$. Now $\beta \not\leq Z(\mathbf{A})$, hence $\langle a, b\rangle \notin Z(\mathbf{A})$, as $\beta = \Theta(a, b)$. Thus there exists a polynomial $f(x, y_1, \ldots, y_m)$ and $\bar{c}, \bar{d} \in A^m$ such that $f(a, \bar{c}) = f(a, \bar{d})$ and $f(b, \bar{c}) \neq f(b, \bar{d})$ (or the same with a and b interchanged). Here

$$f(b, \bar{c}) \overset{\beta}{\equiv} f(a, \bar{c}) = f(a, \bar{d}) \overset{\beta}{\equiv} f(b, \bar{d})\,;$$

so by Theorem 2.8(4), there is $g \in \mathrm{Pol}_1\mathbf{A}$ with $g(A) \subseteq U$ and $gf(b, \bar{c}) \neq gf(b, \bar{d})$. We have $\{gf(b, \bar{c}), gf(b, \bar{d})\} \subseteq N'$ for a trace $N' \subseteq U$. Since all of the $\langle 0_A, \beta\rangle$-traces

in U are polynomially isomorphic (Lemma 4.20), there is $h : N' \simeq N$. Redenoting $hgf(x, \bar{y})$ by $f(x, \bar{y})$, we now have

(12.4.1) $f(a, \bar{c}) = f(a, \bar{d}), f(b, \bar{c}) \neq f(b, \bar{d}), f(N \times \{\bar{c}, \bar{d}\}) \subseteq N$.

Let $\langle N, x+y, -x, 0, \lambda \cdot x (\lambda \in \mathbf{F})\rangle$ ($\mathbf{F}$ is a finite field) be the vector space polynomially equivalent to $\mathbf{A}|_N$. We will also use $x + y$, $-x$ for the polynomial operations of $\mathbf{A}$ whose restrictions to N are the vector space operations. Define new polynomials of $\mathbf{A}$:

$$g_0(x, \bar{y}) = f(x + a, \bar{d}) - f(x + a, \bar{y}) ,$$

$$g_1(x, \bar{y}) = f(x + a, \bar{y}) - f(x + a, \bar{c}) .$$

(12.4.2) There exists $\lambda \neq 0$ in $\mathbf{F}$ such that for $x \in N$,

$$g_0(x, \bar{d}) = 0 = g_1(x, \bar{c}) \text{ and } g_0(x, \bar{c}) = \lambda \cdot x = g_1(x, \bar{d}) .$$

Indeed, the functions $g_i(x, \bar{c})$, $g_i(x, \bar{d})$ are unary polynomials of the vector space which map 0 to 0. So (12.4.2) follows easily. Multiplying by λ^{-1}, or iterating, we create polynomials $h_0(x, \bar{y})$, $h_1(x, \bar{y})$ of $\mathbf{A}$ satisfying

(12.4.3) $h_0(x, \bar{d}) = h_1(x, \bar{c}) = 0$ and $h_0(x, \bar{c}) = h_1(x, \bar{d}) = x$ for $x \in N$.

For any $n \geq 1$ we will define 2^{2^n} polynomials in the $1 + m \cdot n$ variables $x, \bar{y}_0, \bar{y}_1, \ldots,$ $\bar{y}_{n-1}$ ($\bar{y}_0, \ldots, \bar{y}_{n-1}$ are disjoint m-tuples of variables). Let $\mathrm{Su}(n)$ be the set of all subsets of $\{0, \ldots, n-1\}$. For each $S \in \mathrm{Su}(n)$ we put

$$\Phi_S(x, \bar{y}_0, \ldots, \bar{y}_{n-1}) = h_{\varepsilon_0}^{\bar{y}_0} \circ \cdots \circ h_{\varepsilon_{n-1}}^{\bar{y}_{n-1}}(x)$$

where $\varepsilon_i = 0$ if $i \notin S$ and $\varepsilon_i = 1$ if $i \in S$, and where $h_j^{\bar{y}_k}(x) = h_j(x, \bar{y}_k)$. (Thus $\Phi_S(x, \bar{y}_0, \ldots, \bar{y}_{n-1})$ is a composition of n unary functions, $h_{\varepsilon_i}^{\bar{y}_i}$, applied to x.) We can see from (12.4.3) that

(12.4.4) For any $S \in \mathrm{Su}(n)$ and $\bar{e}_0, \ldots, \bar{e}_{n-1} \in \{\bar{c}, \bar{d}\}$ and $x \in N$,
$\Phi_S(x, \bar{e}_0, \ldots, \bar{e}_{n-1}) = x$ if $\{i : \bar{e}_i = \bar{d}\} = S$,
and $\Phi_S(x, \bar{e}_0, \ldots, \bar{e}_{n-1}) = 0$ if $\{i : \bar{e}_i = \bar{d}\} \neq S$.

Now for any set $\mathcal{S} \subseteq \mathrm{Su}(n)$ we put

$$\Lambda_{\mathcal{S}}(x, \bar{y}_0, \ldots, \bar{y}_{n-1}) = \sum_{S \in \mathcal{S}} \Phi_S(x, \bar{y}_0, \ldots, \bar{y}_{n-1}).$$

Suppose that $\mathcal{S}_1 \neq \mathcal{S}_2$, $\{\mathcal{S}_1, \mathcal{S}_2\} \subseteq \mathrm{Su}(\mathrm{Su}(n))$. We can choose, say, $S \in \mathcal{S}_1 - \mathcal{S}_2$. Taking $\bar{e}_i = \bar{d}$ when $i \in S$ and $\bar{e}_i = \bar{c}$ when $i \notin S$, we see from (12.4.4) that for all $x \in N$ and $T \in \mathrm{Su}(n)$, $\Phi_T(x, \bar{e}_0, \ldots, \bar{e}_{n-1}) = x$ if $T = S$ and $= 0$ if $T \neq S$. Thus $\Lambda_{\mathcal{S}_1}(x, \bar{e}_0, \ldots, \bar{e}_{n-1}) = x$ and $\Lambda_{\mathcal{S}_2}(x, \bar{e}_0, \ldots, \bar{e}_{n-1}) = 0$ for $x \in N$.

We have proved that $|\mathrm{Pol}_{1+mn}\mathbf{A}| \geq 2^{2^n}$. Now if $k = |A|$ and $n \geq k+1$, then it follows that

$$|\mathrm{Clo}_n\mathbf{A}| \geq |\mathrm{Pol}_{n-k}\mathbf{A}| \geq 2^{2^{\left[\frac{n-k-1}{m}\right]}}.$$

The desired result follows easily from this. □

Every locally finite variety whose congruence lattices obey a non-trivial equation in joins and meets satisfies the hypothesis of the next theorem. (See Theorems 9.18 and 9.19.)

THEOREM 12.5. *Let $\mathcal{V}$ be a locally finite variety such that $\{\mathbf{1},\mathbf{5}\} \cap \mathrm{typ}\{\mathcal{V}\} = \emptyset$. If $f_{\mathcal{V}}(n)$ fails to be $\geq 2^{2^{cn}}$ for large n and some $c > 0$, then $\mathcal{V}$ has permuting congruences and every finite algebra in $\mathcal{V}$ is nilpotent.*

PROOF. We assume the hypothesis, and also that $f_{\mathcal{V}}$ is not at least doubly exponential in growth. By the preceding lemma, every finite algebra $\mathbf{A}$ in $\mathcal{V}$ is right nilpotent. It easily follows from this that $\mathrm{typ}\{\mathcal{V}\} \subseteq \mathbf{2}$. By Theorem 7.11 (3), $\mathcal{V}$ has permuting congruences. In varieties with permuting congruences, the commutator is symmetric. (See Exercise 3.8 (4).) Thus the finite algebras in $\mathcal{V}$ are (left and right) nilpotent. □

Exercise 12.6. Construct a finite nil-2 Mal'cev algebra $\mathbf{A}$ (with infinitely many basic operations) such that $|\mathrm{Clo}_n\mathbf{A}| \geq 2^{2^n}$ for all n.

13. TAME ALGEBRAS AND E-MINIMAL ALGEBRAS

We defined a finite algebra to be **tame** just in case its congruence quotient $\langle 0,1\rangle$ is tame. For a tame algebra $\mathbf{A}$, we write $\mathrm{M}(\mathbf{A})$ in place of $\mathrm{M}_{\mathbf{A}}(0_A, 1_A)$; and we call the members of $\mathrm{M}(\mathbf{A})$ the **minimal sets** of $\mathbf{A}$. The minimal sets of a tame algebra $\mathbf{A}$ are the same as the $\langle 0_A, 1_A\rangle$-traces in $\mathbf{A}$. The statements in Theorem 2.8 have a simpler form and meaning when $\langle \alpha, \beta\rangle = \langle 0_A, 1_A\rangle$; the reader should review that theorem now and consider its meaning for tame algebras.

The shape of the congruence lattice of a finite algebra can determine that the algebra is tame. For example, the class of tame algebras includes all finite simple algebras. Any tame algebra that is not simple is Abelian. (These remarks are justified by Theorem 2.11, Examples 1.11–1.13, and Theorem 5.7.) Tame algebras are of five types. The type of a tame algebra $\mathbf{A}$, written $\mathrm{typ}(\mathbf{A})$, is equal to $\mathrm{typ}(0_A, 1_A)$. In this chapter, we obtain special representations for tame algebras of types **1** and **2**; we look at an ordering property of tame algebras of types **4** and **5**; and we demonstrate a representation over finite fields for the E-minimal algebras of type **2** which we studied at length in the last half of Chapter 4.

LEMMA 13.1. *Let $\mathbf{A}$ be a tame Abelian algebra; let N be a minimal set of $\mathbf{A}$ and let $0 \in N$; define F' to be the set of all $f \in \mathrm{Pol}_1\mathbf{A}$ with $f(A) \subseteq N$ and $f(0) = 0$; and define F as the set of all $f \in \mathrm{Pol}_1\mathbf{A}$ with $f(A) = N$.*

(1) *If $\mathrm{typ}(\mathbf{A}) = \mathbf{1}$ and $\kappa = |\mathrm{Clo}_1\mathbf{A}|$ then $|F| \leq \kappa$, $|A| \leq |N|^\kappa$, and if $\mathbf{A}$ is simple then $|N| \leq \max(\kappa, 2)$.*

(2) *If $\mathrm{typ}(\mathbf{A}) = \mathbf{2}$ and $\kappa = |\mathrm{Clo}_2\mathbf{A}|$ then $|F'| \leq \kappa$, $|A| \leq |N|^\kappa$, and if $\mathbf{A}$ is simple then $|N| \leq \kappa$.*

PROOF. Choose $e \in F$ such that $e = e^2$ (Theorem 2.8 (2)). We suppose first that $\mathrm{typ}(\mathbf{A}) = \mathbf{1}$. For any $f \in F$ there exists $g \in \mathrm{Clo}_{n+1}\mathbf{A}$ (for some n) and $\langle a_1, \ldots, a_n\rangle = \bar{a} \in A^n$ such that $f(x) = g(x, \bar{a})$. By Exercise 5.11 (2) (or Claim 3 in the proof of Theorem 5.6), the polynomial $eg(x, y_1, \ldots, y_n)$ depends on at most one variable. It certainly depends on x; thus $eg(x, y_1, \ldots, y_n) = eg(x, x, \ldots, x)$. Therefore we have $h \in \mathrm{Clo}_1\mathbf{A}$ such that $f(x) = eh(x)$. From this it follows that $|F| \leq |\mathrm{Clo}_1\mathbf{A}|$. By 2.8 (4), for any $x \neq y$ in A there is $f \in F$ with $f(x) \neq f(y)$. Thus $x \mapsto \langle f(x) : f \in F\rangle$ is an embedding of A into N^F; so we have $|A| \leq |N|^{|F|}$.

Finally, suppose that $\mathbf{A}$ is simple. Let $\Pi = (\mathrm{Pol}_1\mathbf{A}|_N) \cap (\mathrm{Sym}\ N)$. Every unary polynomial of $\mathbf{A}|_N$ is constant or belongs to Π (as $\mathbf{A}|_N$ is a minimal algebra). There-

fore Con $\mathbf{A}|_N$ = Con$\langle N, \Pi\rangle$. Now $\mathbf{A}|_N$ is simple, since restriction maps Con $\mathbf{A}$ onto Con $\mathbf{A}|_N$. In order that $\langle N, \Pi\rangle$ be simple, if $|N| > 2$ then Π must be transitive on N. Since $|\Pi| \leq |F|$, we get the last inequality in statement (1).

Now suppose that typ($\mathbf{A}$) = **2**. Then $\mathbf{A}|_N$ is polynomially equivalent to a vector space $\langle N,\ x+y,\ 0,\ \lambda x\,(\lambda \in \mathbf{K})\rangle$ over a finite field $\mathbf{K}$. Let $|F'| = m$ and $F' = \{f_0, \ldots, f_{m-1}\}$ where for each $i < m$, $f_i(x)$ is of the form $eg_i(x, \bar{a})$ with $g_i \in \mathrm{Clo}_{\ell+1}\mathbf{A}$ and $\bar{a} \in A^\ell$ (where $\ell = |A|$). Let $g_i'(x,y) = g_i(x,y,\ldots,y)$, choose $a \in A$, and set $f_i'(x) = eg_i'(x,a) - eg_i'(0,a)$. Then we claim that $F' = \{f_0', \ldots, f_{m-1}'\}$. It is clear that $f_i' \in F'$. If $f_i' = f_j'$ then the function $f_i'(x) - f_j'(x)$ is constant. Using that $\mathbf{A}$ is Abelian, we derive that $f_i(x) - f_j(x) = f_i(y) - f_j(y)$ for all x, y, which implies that $f_i = f_j$ since $f_i(0) = f_j(0) = 0$. Thus we have m distinct functions f_i', and it follows that $m = |F'| \leq |\mathrm{Clo}_2\mathbf{A}|$.

Now using 2.8 (4) and the fact that $(\mathrm{Pol}_1\mathbf{A}|_N) \cap (\mathrm{Sym}\ N)$ is transitive on N in this case, we can easily see that F' separates points of A, and so $|A| \leq |N|^{|F'|}$. Finally, suppose that $\mathbf{A}$ is simple. Then our vector space is simple, and of dimension 1, and it follows that $|N| = |\mathbf{K}| = |F'|_N| \leq |F'|$. □

This lemma just proved will be useful in the next chapter, and it introduces us to the idea of representing a tame algebra as a set of functions into a minimal set.

DEFINITION 13.2. Let $\mathbf{A}$ be an algebra and k be a positive integer. We define an algebra, the **[k]-th matrix power** of $\mathbf{A}$, which we shall denote by $\mathbf{A}^{[k]}$. The universe of this algebra will be the direct power set A^k. For any $n \geq 0$ and $f_0, \ldots, f_{k-1} \in \mathrm{Clo}_{nk}\mathbf{A}$ we define an n-ary operation $[f_0, \ldots, f_{k-1}] = f$ on A^k by the rule:

$$f(\bar{x}^0, \ldots, \bar{x}^{n-1}) = \langle f_0(\bar{x}^0 \cdots \bar{x}^{n-1}), \ldots, f_{k-1}(\bar{x}^0 \cdots \bar{x}^{n-1})\rangle$$

Here $\bar{x}^i = \langle x_0^i, \ldots, x_{k-1}^i\rangle \in A^k$ and

$$\bar{x}^0 \cdots \bar{x}^{n-1} = \langle x_0^0, \ldots, x_{k-1}^0, \ldots, x_0^{n-1}, \ldots, x_{k-1}^{n-1}\rangle \in A^{nk}.$$

$\mathbf{A}^{[k]}$ is the non-indexed algebra $\langle A^k, F\rangle$ where F is the set of all operations of the form $[f_0, \ldots, f_{k-1}]$ with $\{f_0, \ldots, f_{k-1}\} \subseteq \mathrm{Clo}_{nk}\mathbf{A}$ for some $n \geq 0$. (Note that F is a clone.)

For the purpose of formulating the next two theorems, we introduce some more concepts. An algebra $\mathbf{A} = \langle A, \ldots\rangle$ will be called a **reduct** of $\mathbf{B} = \langle B, \ldots\rangle$ iff $A = B$ and Clo $\mathbf{A} \subseteq$ Clo $\mathbf{B}$. The algebra $\mathbf{A}$ will be called a **subreduct** of $\mathbf{B}$ iff it is a subalgebra of some reduct of $\mathbf{B}$. Algebras $\mathbf{A}$ and $\mathbf{B}$ are said to be **weakly isomorphic** iff $\mathbf{A}$ is isomorphic to an algebra $\mathbf{B}' = \langle B, \ldots\rangle$ such that Clo $\mathbf{B}'$ = Clo $\mathbf{B}$.

If $\mathbf{B}$ is a unary algebra (i.e., if its basic operations are unary) and if $\mathbf{A}$ is a subreduct of $\mathbf{B}^{[k]}$ for some $k \geq 1$, then it can easily be seen that $\mathbf{A}$ is strongly Abelian. We

shall now prove a converse of this fact for strongly Abelian tame algebras. In [22] it was proved that any strongly Abelian tame algebra $\mathbf{A} = \langle A, f\rangle$, having just one basic operation f which is not constant, is weakly isomorphic to $\langle N, \sigma\rangle^{[k]}$ for some k, where N is a minimal set of $\mathbf{A}$ and σ is a permutation of N. A consequence was that any finite algebra whose congruence lattice is, say, $\mathbf{M}_7$ has at least two basic operations. For strongly Abelian tame algebras in general, we have only been able to obtain the weaker result of the next theorem.

THEOREM 13.3. *Let* $\mathbf{A}$ *be a tame algebra of type* 1 *(strongly Abelian) and let* $N \in \mathrm{M}(\mathbf{A})$ *and* $k = |\mathrm{Clo}_1\mathbf{A}|$. *The algebra* $\mathbf{A}$ *is isomorphic to a subreduct of* $\mathbf{N}^{[k]}$, *where* $\mathbf{N} = \langle N, c(c \in N)\rangle$ *has only constant operations.*

PROOF. We let F be as in Lemma 13.1 and, using 13.1 (1), we choose an enumeration $f_0, \dots, f_{k-1}$ of F. As in the proof of 13.1 (1), the map $\pi(x) = \langle f_0(x), \dots, f_{k-1}(x)\rangle$ is a bijection of $\mathbf{A}$ with a subset $E = \pi(A)$ of N^k. Letting p_i be the projections of N^k onto N, we have $p_i\pi = f_i$ for $i = 0, \dots, k-1$. For each operation g on the set A, there is a unique operation g_π on E (having the same arity) such that $\pi : \langle A, g\rangle \to \langle E, g_\pi\rangle$ is an isomorphism. Thus π is an isomorphism of $\mathbf{A}$ with a certain algebra $\mathbf{E} = \langle E, \dots\rangle$. Now we just have to show that every basic operation of $\mathbf{E}$ is a restriction to E of one of the operations of $\mathbf{N}^{[k]}$.

Let g be a basic n-ary operation of $\mathbf{A}$ and g_π be the corresponding operation of $\mathbf{E}$. For each $i < k$ consider the polynomial operation $f_i g(x_0, \dots, x_{n-1})$ of $\mathbf{A}$. By Exercise 5.11 (2), this operation depends on at most one variable. Thus there is $n_i < n$ and $f_i' \in \mathrm{Pol}_1\mathbf{A}$ such that $f_i g(x_0, \dots, x_{n-1}) = f_i'(x_{n_i})$. If f_i' is not constant, then $f_i'(A) = N$ (since $N \in \mathrm{M}(\mathbf{A})$), and there is $k_i < k$ such that $f_i' = f_{k_i}$. In this case, take $h_i(x_0^0, \dots, x_{k-1}^{n-1}) = x_{k_i}^{n_i}$, so that $h_i \in \mathrm{Clo}_{nk}\mathbf{N}$. We have, for $\bar{y}^0 = \pi(x_0), \dots, \bar{y}^{n-1} = \pi(x_{n-1})$ in E, that

$$\begin{aligned} p_i g_\pi(\bar{y}^0, \dots, \bar{y}^{n-1}) &= f_i g(x_0, \dots, x_{n-1}) = f_i'(x_{n_i}) = f_{k_i}(x_{n_i}) \\ &= p_{k_i}(\bar{y}^{n_i}) = y_{k_i}^{n_i} = h_i(\bar{y}^0 \cdots \bar{y}^{n-1}). \end{aligned}$$

If f_i' is constant, say $= c$, then we take $h_i = c$, $h_i \in \mathrm{Clo}_{nk}\mathbf{N}$.

We have now defined $h_0, \dots, h_{k-1} \in \mathrm{Clo}_{nk}\mathbf{N}$, and in the notation of Definition 13.2, it is obvious that g_π is the restriction to E of the operation $[h_0, \dots, h_{k-1}]$ of $\mathbf{N}^{[k]}$. □

Remark 13.4. The definition of $\mathbf{A}^{[k]}$ is related to the formation of rings of matrices. If $\mathbf{M}$ is a module over a ring $\mathbf{R}$, then M^k can be given the structure of a module over the ring of k-by-k matrices with entries from $\mathbf{R}$, and this module has the same clone of term operations as $\mathbf{M}^{[k]}$. Note that $\mathbf{A}^{[k]}$ has the same clone of term operations as the algebra defined in Exercise 3.12 (4). The next theorem was discovered independently by P.P. Pálfy and by the authors.

THEOREM 13.5. *Let* $\mathbf{A}$ *be a tame algebra of type* **2** *(Abelian, not strongly Abelian) and let* $N \in \mathrm{M}(\mathbf{A})$ *and* $\mathbf{N} = \mathbf{A}|_N$. *Then* $\mathbf{N}$ *is polynomially equivalent to a vector space* $\mathbf{V}$ *over a finite field* $\mathbf{K}$; *and for some* $k \leq |\mathrm{Clo}_2\mathbf{A}|$, $\mathbf{A}$ *is isomorphic to a subreduct* $\mathbf{E}$ *of* $\mathbf{N}^{[k]}$ *(where* E *spans* $\mathbf{V}^k$ *as a* $\mathbf{K}$*-vector space if* $\mathbf{A}$ *is simple).*

PROOF. We choose $0 \in N$ and let F' be defined as in Lemma 13.1. By 13.1 (2), $|F'| \leq |\mathrm{Clo}_2\mathbf{A}|$. Since $\mathbf{A}|_N$ is a minimal algebra of type **2**, we have a vector space $\langle N, +, -, 0, \dots\rangle = \mathbf{V}$ over a finite field $\mathbf{K}$, which is polynomially equivalent to $\mathbf{A}|_N$. Let $I = \{f \in F' : f = f^2 \text{ and } f(A) = N\}$. By 2.8 (2), $I \neq \emptyset$. Notice that F' is a vector subspace of $\mathbf{V}^A$ (direct power of $\mathbf{V}$).

We claim that I spans F' as vector space. Indeed, let $f \in F'$. There exists $\lambda \in \mathbf{K}$ such that $f(x) = \lambda \cdot x$ when $x \in N$ (since $f|_N \in \mathrm{Pol}_1\mathbf{V}$ and $f|_N(0) = 0$). If $\lambda \neq 0$ then $\frac{1}{\lambda} \cdot f \in I$. If $\lambda = 0$ then for any $e \in I$ we have $e - f \in I$. (Note that $e - f$ is defined on A since $e(A) \cup f(A) \subseteq N$.) Thus in either event, f is a linear combination of vectors in I.

Now let $e_0, \dots, e_{k-1}$ form a maximal linearly independent subset of I. By the claim just proved, $e_0, \dots, e_{k-1}$ span the space F'; and by 13.1 (2), $k \leq |\mathrm{Clo}_2\mathbf{A}|$. Hence using 2.8 (4) we can easily prove that $e_0, \dots, e_{k-1}$ separate points of $\mathbf{A}$, i.e., the map $\pi(x) = \langle e_0(x), \dots, e_{k-1}(x)\rangle$ is a bijection of A with a subset $E = \pi(A)$ of N^k. As in the last proof, $\pi : \mathbf{A} \cong \mathbf{E}$ for a certain algebra $\mathbf{E}$ with basic operations g_π (g a basic operation of $\mathbf{A}$). The projections p_i of N^k onto N satisfy $e_i = p_i\pi$ for $i = 0, \dots, k-1$.

Now let g be an n-ary basic operation of $\mathbf{A}$, and g_π be the corresponding operation of $\mathbf{E}$. For $i < k$, using the Abelian property of $\mathbf{A}$, we can prove that there are $c \in N$ and $\alpha_0, \dots, \alpha_{n-1} \in F'$ such that

$$e_i g(x_0, \dots, x_{n-1}) = \sum_0^{n-1} \alpha_j(x_j) + c.$$

Since $e_0, \dots, e_{k-1}$ span F', there are $\lambda_{ji} \in K$ such that

$$e_i g(x_0, \dots, x_{n-1}) = \sum_{\substack{j<n \\ m<k}} \lambda_{jm} e_m(x_j) + c.$$

This translates into: For $\bar{y}^0, \dots, \bar{y}^{n-1} \in E$,

$$p_i g_\pi(\bar{y}^0, \dots, \bar{y}^{n-1}) = \sum_{j,m} \lambda_{jm} y^j_m + c.$$

Since there is a similar equation for each basic operation g, and for each $i < k$, we conclude that $\mathbf{E}$ is a subreduct of $\mathbf{N}^{[k]}$.

Finally, suppose that $\mathbf{A}$ is simple. Then $\mathbf{N}$ is simple and $\dim \mathbf{V} = 1$. Therefore $\mathbf{V}^k$ is a k-dimensional vector space. If, now, E spans a space $\overline{E} < N^k$, then there exist

$\lambda_0, \ldots, \lambda_{k-1}$, not all 0, such that $\sum \lambda_i y_i = 0$ for all $\bar{y} = \langle y_0, \ldots, y_{k-1} \rangle \in \overline{E}$. (Since $\overline{E}$ cannot have k linearly independent linear functionals $p_0, \ldots, p_{k-1}$.) But this means that $\sum \lambda_i e_i = 0$ in the space F', contradicting the choice of e_i. Thus E spans $\mathbf{V}^k$. □

For tame algebras of types **4** and **5**, we have found no representation result analogous to Theorems 13.3 and 13.5. (An analogous result can be proved for type **3**; but it is essentially meaningless, since every finite algebra is isomorphic to a subreduct of a $[k]$-th power of the two-element Boolean algebra.) Tame algebras of types **4** and **5** do, however, possess an interesting property which we shall now examine.

In Chapter 5 we introduced the notion of an $\langle \alpha, \beta \rangle$ **pre-order** and proved (Theorem 5.26) that a tame quotient $\langle \alpha, \beta \rangle$ in a finite algebra $\mathbf{A}$ has type **4** or **5** (assuming $\text{typ}(\alpha, \beta) \neq \mathbf{1}$) iff $\mathbf{A}$ admits an $\langle \alpha, \beta \rangle$ pre-order. When this result is specialized to the case $\langle \alpha, \beta \rangle = \langle 0_A, 1_A \rangle$, it states: A finite, tame, and not strongly Abelian algebra $\mathbf{A}$ has type **4** or **5** iff $\mathbf{A}$ has an admissible, connected, partial order; i.e., iff there exists a partial ordering $\leq$ of the set A such that all polynomials of $\mathbf{A}$ are monotone with respect to $\leq$ and the transitive-symmetric closure of $\leq$ is $A \times A$. These facts can be summarized in the statement that tame algebras of types **4** and **5** are **orderable**, while those of types **2** and **3** are not orderable. The following theorem is an immediate consequence of Theorems 5.24 and 5.26.

THEOREM 13.6. *Let* $\mathbf{A}$ *be any finite simple algebra of type* **4** *or* **5**. *There are six subalgebras* $\rho_0, \rho_1, \zeta_0, \zeta_1, \xi_0, \xi_1$ *of* $\mathbf{A}^2$ *such that* $0_A \subset \rho_i \subseteq \zeta_i \subseteq \xi_i$ $(i = 0, 1)$, $\rho_1 = \rho_0^{\cup}$, $\zeta_1 = \zeta_0^{\cup}$, $\xi_1 = \xi_0^{\cup}$, $\xi_0 \cap \xi_1 = 0_A$, *and*

(1) ρ_0 *and* ρ_1 *are the minimal reflexive admissible relations on* $\mathbf{A}$, *and*

$$\rho_0 \cup \rho_1 = 0_A \cup \bigcup \{N^2 : N \in \mathrm{M}(\mathbf{A})\};$$

(2) ζ_0, ξ_0 *are connected partial orderings of* A, *and* ζ_0 *is the transitive closure of* ρ_0;

(3) *for every admissible partial ordering* μ *of* $\mathbf{A}$ *such that* $0_A < \mu$, *either* $\zeta_0 \leq \mu \leq \xi_0$ *or* $\zeta_1 \leq \mu \leq \xi_1$.

If $\mathbf{A}$, ρ_i, ζ_i, ξ_i satisfy the statements of this theorem and $N = \{u, v\}$ is one of the minimal sets of $\mathbf{A}$, then for one of $i = 0, 1$ we have that ρ_i is the subalgebra of $\mathbf{A}^2$ generated by $0_A \cup \{\langle u, v \rangle\}$, ζ_i is the transitive closure of ρ_i, and ξ_i is the set of pairs $\langle x, y \rangle \in A^2$ such that for every $f \in \mathrm{Pol}_1 \mathbf{A}$, $f(\{x, y\}) = N$ implies $f(y) = v$.

Some examples of simple algebras of type **5**, the graph algebras of C. Shallon, and their orderings, are defined and studied in the exercises ending the next chapter. Every finite simple lattice has type **4**, and the lattice ordering is one of the two minimal admissible partial orderings ζ_i.

The final topic of this chapter is a representation theorem for E-minimal algebras of type **2**. The E-minimal algebras were introduced and classified into five types in

Definition 2.14, Lemma 4.28, and Lemma 4.32. The most interesting of these are the E-minimal algebras of type **2**. These algebras are characterized as finite, non-trivial, nilpotent algebras having a Mal'cev 3-ary polynomial, and having no non-constant idempotent unary polynomials other than the identity function. Our interest in them is heightened by Theorem 8.7.

We remark that the topic we are now discussing is nearly disjoint from the earlier topic of this chapter; an algebra is both tame and E-minimal iff it is minimal.

A **local ring** is any ring with identity in which the non-invertible elements form an ideal. It is easy to see that any finite non-trivial unitary module over a local ring is an Abelian E-minimal algebra of type **2**. In Exercise 13.10 (3), the reader is asked to show that, conversely, every Abelian E-minimal algebra of type **2** is polynomially equivalent to a unitary module over a finite local ring.

DEFINITION 13.7. Let $\mathbf{GF}(q)$ be a finite field of q elements and let k be a positive integer. An algebra $\mathbf{E}(q,k)$ is defined as follows. The universe is the set $E(q,k) = (GF(q))^k$. The basic operations are simply all the operations f on $E(q,k)$ for which (if f is n-ary) there exist $\lambda_0,\dots,\lambda_{n-1} \in GF(q)$ and operations $h_0,\dots,h_{k-1}$ on $GF(q)$ (completely arbitrary except that h_i is $n\cdot i$-ary) so that for all $\bar{x}^0,\dots,\bar{x}^{n-1} \in E(q,k)$:

$$f(\bar{x}^0,\dots,\bar{x}^{n-1}) = \langle y_0,\dots,y_{k-1}\rangle \text{ where for } i<k,$$
$$y_i = \sum_{j<n} \lambda_j x_i^j + h_i(x_0^0,\dots,x_{i-1}^0,\dots,x_0^{n-1},\dots,x_{i-1}^{n-1}).$$

The operation f defined by the formula is denoted by $[\lambda_0,\dots,\lambda_{n-1};\ h_0,\dots,h_{k-1}]$, or by $[\bar{\lambda};\bar{h}]$.

Remark 13.8. The basic operations of $\mathbf{E}(q,k)$ constitute a polynomial clone containing all the polynomial operations of the vector space $GF(q)^k$. The congruence lattice of $\mathbf{E}(q,k)$ is a $k+1$-element chain; the congruences are the relations

$$\theta_i = \{\langle \bar{x},\bar{y}\rangle : x_j = y_j \text{ for all } j<i\},$$

and they satisfy $1 = \theta_0 > \theta_1 > \theta_2 > \cdots > \theta_k = 0$. It is quite easy to check that $[\theta_i,1] = \theta_{i+1}$ for $i<k$, so $\mathbf{E}(q,k)$ is nilpotent. It is also easy to see that every $e \in \mathrm{Pol}_1(\mathbf{E}(q,k))$ satisfying $e^2 = e$ must be constant or the identity, using that e has the form $e = [\lambda_0;\bar{h}]$. In sum, $\mathbf{E}(q,k)$ is an E-minimal algebra of type **2**.

THEOREM 13.9. *For any finite, non-trivial algebra* $\mathbf{A}$ *the following are equivalent.*

(1) $\mathbf{A}$ *is* E*-minimal and of type* **2**.

(2) $\mathbf{A}$ *is Mal'cev and isomorphic to a reduct of some algebra* $\mathbf{E}(q,k)$, *where* k *is the height of* $\mathbf{Con}\,\mathbf{A}$.

PROOF. The proof that (2) implies (1) is an easy deduction from the remarks above. The proof that (1) implies (2) occupies several pages.

Let $\mathbf{A}$ be a finite algebra satisfying (1). Taking $\theta \in \operatorname{Con} \mathbf{A}$ with $\theta \prec 1_A$, A is the body of a $\langle \theta, 1 \rangle$-minimal set. Thus by Lemma 4.20, $\mathbf{A}$ has a Mal'cev polynomial d that is a permutation when any two of its variables are fixed. By Lemma 4.36, $\mathbf{A}$ is nilpotent. We define $\operatorname{ht}(\mathbf{A})$ to be the length of a maximal chain in $\mathbf{Con}\ \mathbf{A}$. (All maximal chains have the same length, since $\mathbf{Con}\ \mathbf{A}$ is modular.) By induction on $k = \operatorname{ht}(\mathbf{A})$, we shall prove that $\mathbf{A}$ is isomorphic to a reduct of some $\mathbf{E}(q, k)$.

If $k = 1$, then $\mathbf{A}$ is simple. Thus $\mathbf{A}$ is $\langle 0_A, 1_A \rangle$-minimal (by Lemma 4.28); i.e., it is minimal. In this case, $\mathbf{A}$ is polynomially equivalent to a vector space of dimension one over $\mathbf{GF}(q)$ for some q (see 4.7, 4.10, 4.11); and so $\mathbf{A}$ is isomorphic to a reduct of $\mathbf{E}(q, 1)$.

Now assume that $k > 1$, and that every finite, non-trivial algebra $\mathbf{B}$ satisfying (1), of height $< k$, satisfies (2). Let δ be any minimal congruence of $\mathbf{A}$. From the proof of Lemma 4.36, and the result of Exercise 3.8 (4), we have that $[1_A, \delta] = [\delta, 1_A] = 0_A$; i.e., $\delta \subseteq Z(\mathbf{A})$. (The center of $\mathbf{A}$, or $Z(\mathbf{A})$, is defined in Exercise 3.2 (5).) The algebra $\mathbf{A}' = \mathbf{A}/\delta$ satisfies (1), and $\operatorname{ht}(\mathbf{A}') = k - 1$. Let $\phi' : \mathbf{A}' \twoheadrightarrow \langle E(q', k-1), \dots \rangle$ be an isomorphism of $\mathbf{A}'$ with a reduct of $\mathbf{E}(q', k-1)$ (for some q', by the induction assumption).

Let $T_0 = \phi'^{-1}(\langle 0, \dots, 0 \rangle)$, an equivalence class of δ, and put $\mathbf{T}_0 = \mathbf{A}|_{T_0}$. By Lemma 4.28 and Theorem 4.31, T_0 is a $\langle 0, \delta \rangle$-trace; and so $\mathbf{T}_0$ is polynomially equivalent to a 1-dimensional vector space over $\mathbf{GF}(q)$ for some q. Passing to an algebra isomorphic to $\mathbf{A}$, if necessary, we can assume that $T_0 = GF(q)$ and $\mathbf{T}_0$ is polynomially equivalent to $\mathbf{E}(q, 1)$.

The next step is to set up a bijection between $\mathbf{A}$ and $\mathbf{E}(q', k-1) \times \mathbf{E}(q, 1)$. We may assume that $A' = \{T_0, \dots, T_{u-1}\}$ $(u = (q')^{k-1})$ with $T_0 = GF(q) = E(q, 1)$. For each $i < u$ choose an element $a_i \in T_i$, and choose $a_0 = 0$. Define a function s' on A by $s'(x) = a_i$ whenever $x \in T_i$. For $a \in A$, put $p'(a) = \phi'(a/\delta)$, and $p(a) = d(0, s'(a), a)$. Finally, for $a \in A$, put $\phi(a) = \langle p'(a), p(a) \rangle$. From the properties of $d(x, y, z)$, we easily deduce that ϕ is a bijection between A and $E(q', k-1) \times E(q, 1)$.

Replacing $\mathbf{A}$ by an isomorphic algebra, we can now assume that

$$A = E(q', k-1) \times E(q, 1) = E(q', 1) \times \cdots \times E(q', 1) \times E(q, 1).$$

(The second equation is not strictly true, but it is a harmless identification of two sets by a bijection.) The elements of $\mathbf{A}$ will be written either as

$$x = \langle \bar{x}, y \rangle, \quad (\bar{x} \in E(q', k-1)\,;\, y \in E(q, 1))\,,$$

or as

$$x = \langle x_0, \dots, x_{k-1} \rangle, \quad (x_0, \dots, x_{k-2} \in E(q', 1)\,;\, x_{k-1} \in E(q, 1)).$$

For $x = \langle x_0, \ldots, x_{k-1} \rangle$ in A and $0 < i < k$, we define

$$p_i'(x) = \langle x_0, \ldots, x_{i-1} \rangle,$$

$$p_i(x) = x_i,$$

$$s(x) = \langle 0, \ldots, 0, x_{k-1} \rangle,$$

$$\theta_i = \ker p_i'.$$

We also put $p_0(x) = x_0$, $\theta_0 = 1_A$ and $p = p_{k-1}$. Note that $p' = p_{k-1}'$, $s'(x) = \langle x_0, \ldots, x_{k-2}, 0 \rangle$ and $\delta = \ker p' = \ker s'$. We have secured the following facts.

(13.9.1) $\{\theta_i : i < k\} \subseteq \operatorname{Con} \mathbf{A}$, and since $\operatorname{ht}(\mathbf{A}) = k$,

$$1_A = \theta_0 \succ \theta_1 \succ \cdots \succ \theta_{k-2} \succ \delta \succ 0_A .$$

Moreover, $\delta \leq Z(\mathbf{A})$.

(13.9.2) $p' = p_{k-1}'$ is a homomorphism of $\mathbf{A}$ onto a reduct of $\mathbf{E}(q', k-1)$.

(13.9.3) Where $T_0 = s(A)$, we have that $p|_{T_0}$ is an isomorphism of $\mathbf{A}|_{T_0}$ with an algebra polynomially equivalent to $\mathbf{E}(q, 1)$. This implies that $d(\langle \bar{0}, y \rangle, \langle \bar{0}, z \rangle, \langle \bar{0}, u \rangle) = \langle \bar{0}, y - z + u \rangle$, since $\mathbf{E}(q, 1)$ has a unique Mal'cev operation.

(13.9.4) Writing 0 for the element $\langle \bar{0}, 0 \rangle$ in A, we have $d(0, s'(x), x) = s(x)$ for all $x \in A$.

We begin our examination of the operations of $\mathbf{A}$ by establishing some more facts.

(13.9.5)

(i) For any $f \in \operatorname{Pol}_n \mathbf{A}$ and $u \in A$, and for $\tilde{x}, \tilde{y}, \tilde{z} \in A^n$ satisfying $\langle y_i, z_i \rangle \in \delta$ for $i < n$, we have

$$d(u, f(\tilde{x}), f(d(\tilde{x}, \tilde{y}, \tilde{z}))) = d(u, f(\tilde{y}), f(\tilde{z})).$$

(Here $f(d(\tilde{x}, \tilde{y}, \tilde{z}))$ denotes $f(d(x_0, y_0, z_0), \ldots, d(x_{n-1}, y_{n-1}, z_{n-1}))$.)

(ii) If $\langle y, z \rangle \in \delta$ then

$$d(u, y, z) = d(z, y, u)$$

and

$$d(y, u, d(u, y, z)) = d(d(u, y, z), u, y) = z.$$

(iii) If $y \equiv z \equiv w \pmod{\delta}$ then

$$d(u, y, z) = d(d(u, y, w), u, d(u, w, z)).$$

These equations follow from the fact that $\delta \subseteq Z(\mathbf{A})$. For (i), observe that

$$d(u, f(\tilde{x}), f(d(\tilde{x}, \tilde{y}, \underline{\tilde{y}})) = d(u, f(\tilde{y}), f(d(\tilde{y}, \tilde{y}, \underline{\tilde{y}})) = u.$$

Replacing the underlined occurrences of $y_0, \ldots, y_{n-1}$ by $z_0, \ldots, z_{n-1}$ gives the desired equation. For (ii), in the equation $d(u, \underline{z}, z) = d(z, \underline{z}, u)$, replace the underlined z's by y, obtaining that $d(u, y, z) = d(z, y, u)$ (where $\langle y, z \rangle \in Z(\mathbf{A})$). For the second equation of (ii), take $n = 1$ and $f(x) = x$ in (i), obtaining

$$d(y, u, d(u, y, z)) = d(y, y, z) = z$$

(and $d(d(u, y, z), u, y) = d(y, u, d(u, y, z))$ since $\langle u, d(u, y, z) \rangle \in \delta$). For (iii), again by (i) with $f(x) = x$, we have

$$\begin{aligned} d(d(u, y, w), u, d(u, w, z)) &= d(d(u, y, w), w, z) \\ &= d(z, \underline{w}, d(\underline{w}, y, u)); \text{ and} \\ d(u, y, z) &= d(u, \underline{w}, d(\underline{w}, y, z)). \end{aligned}$$

Replacing all four underlined occurrences of w by y gives the elements $d(z, y, u)$ and $d(u, y, z)$, which are equal by (ii). Thus we can conclude that (iii) holds.

(13.9.6) For $x \in A$ we have $x = d(s(x), 0, s'(x)) = d(s'(x), 0, s(x))$.

This follows from (13.9.4) and (13.9.5)(ii). Our next goal is to prove

(13.9.7) For every $f \in \mathrm{Pol}_n \mathbf{A}$, there exist $g \in \mathrm{Pol}_n(\mathbf{E}(q', k-1))$, and $h' : E(q', k-1)^n \to E(q, 1)$, and $\lambda_0, \ldots, \lambda_{n-1} \in GF(q)$ so that for all $x_0 = \langle \bar{x}_0, y_0 \rangle, \ldots, x_{n-1} = \langle \bar{x}_{n-1}, y_{n-1} \rangle$ in A,

$$f(x_0, \ldots, x_{n-1}) = \left\langle g(\bar{x}_0, \ldots, \bar{x}_{n-1}) \, , \, \sum \lambda_i \cdot y_i + h'(\bar{x}_0, \ldots, \bar{x}_{n-1}) \right\rangle .$$

This formula can be rewritten as

(13.9.7′) $p' f(\tilde{x}) = g(p'(\tilde{x}))$ and $p(f(\tilde{x})) = h(p(\tilde{x})) + h'(p'(\tilde{x}))$ for $\tilde{x} \in A^n$, where $h : E(q, 1)^n \to E(q, 1)$ is linear and h' is arbitrary. (Here $p(\tilde{x})$ denotes the string $p(x_0), \ldots, p(x_{n-1})$.)

We know by (13.9.2) that g exists. We have to find h and h', given $f \in \mathrm{Pol}_n \mathbf{A}$. To that end, we define

$$h_0(\tilde{x}) = d(0, f(s'(\tilde{x})), f(\tilde{x})),$$

$$h_1(\tilde{x}) = d(0, s'(f(\tilde{x})), f(s'(\tilde{x})).$$

(13.9.8) We have that $h_0, h_1 : A^n \to T_0$ and

$$\begin{aligned} &\text{(i)} \quad h_0(\tilde{x}) = h_0(s(\tilde{x})), \\ &\text{(ii)} \quad h_1(\tilde{x}) = h_1(s'(\tilde{x})), \\ &\text{(iii)} \quad s(f(\tilde{x})) = d(h_0(\tilde{x}), 0, h_1(\tilde{x})). \end{aligned}$$

The truth of (13.9.8) will follow from (13.9.4) and (13.9.5) and the fact that $f(\tilde{x})$, $f(s'(\tilde{x}))$, and $s'(f(\tilde{x}))$ $(= s'(f(s'(\tilde{x})))$) are congruent modulo δ. To get (i), substitute $0, \tilde{0}, s'(\tilde{x}), \tilde{x}$ for $u, \tilde{x}, \tilde{y}, \tilde{z}$ in (13.9.5)(i). Then we get

$$\begin{aligned} h_0(s(\tilde{x})) &= d(0, f(s'(s(\tilde{x}))), f(s(\tilde{x}))) \\ &= d(0, f(\tilde{0}), f(d(\tilde{0}, s'(\tilde{x}), \tilde{x}))) \\ &= d(0, f(s'(\tilde{x})), f(\tilde{x})) \\ &= h_0(\tilde{x}). \end{aligned}$$

For (ii),

$$h_1(s'(\tilde{x})) = d(0, s'(f(s'(\tilde{x}))), f(s'(s'(\tilde{x})))) = d(0, s'(f(\tilde{x})), f(s'(\tilde{x}))) = h_1(\tilde{x}).$$

For (iii), take u, y, z, w in (13.9.5)(iii) to be $0, s'(f(\tilde{x})), f(\tilde{x}), f(s'(\tilde{x}))$ and obtain

$$\begin{aligned} s(f(\tilde{x})) &= d(0, s'f(\tilde{x}), f(\tilde{x})) = d(h_1(\tilde{x}), 0, h_0(\tilde{x})) \\ &= d(h_0(\tilde{x}), 0, h_1(\tilde{x})). \end{aligned}$$

(The last equality is by (13.9.5)(ii), since we have $\langle 0, h_0(\tilde{x})\rangle \in \delta$.)

Now for $\tilde{x} \in T_0^n$, $h_0(\tilde{x})$ is congruent to 0 modulo δ, so $h_0(\tilde{x}) \in T_0$. This implies that $h_0|_{T_0} \in \mathrm{Pol}_n \mathbf{T}_0$, so by (13.9.3) there is $h \in \mathrm{Pol}_n(\mathbf{E}(q,1))$ such that $p(h_0(\tilde{x})) = h(p(\tilde{x}))$ for all $\tilde{x} \in T_0^n$. Thus we have

$$h_0(\tilde{x}) = h_0(s(\tilde{x})) = \langle \bar{0}, p(h_0(\tilde{x}))\rangle = \langle \bar{0}, h(p(\tilde{x}))\rangle,$$

for all $\tilde{x} \in A^n$. Moreover, h must be linear, since $h_0(\tilde{0}) = 0$. Similarly (13.9.8)(ii) implies that there is $h' : E(q', k-1)^n \to E(q,1)$ satisfying $h_1(\tilde{x}) = \langle \bar{0}, h'(p'(\tilde{x}))\rangle$. Finally (13.9.8)(iii) and the equation in (13.9.3) then imply that

$$\langle \bar{0}, p(f(\tilde{x}))\rangle = s(f(\tilde{x})) = d(h_0(\tilde{x}), 0, h_1(\tilde{x})) = \langle \bar{0}, h(p(\tilde{x})) + h'(p'(\tilde{x}))\rangle.$$

This completes the proof of (13.9.7′) and of (13.9.7).

It remains to show that $q = q'$ and to "un-twist" our representation and show that $\mathbf{A}$ is isomorphic to a reduct of $\mathbf{E}(q,k)$. To do that, we study $\mathrm{Pol}_1 \mathbf{A}$, and begin by noting that (13.9.7) implies

(13.9.9) For every $f \in \mathrm{Pol}_1\mathbf{A}$, there are $\lambda' \in GF(q')$ and $\lambda \in GF(q)$ such that for all $x = \langle x_0, \dots, x_{k-2}, y\rangle \in A$ and for $i \leq k-2$, we have:

$p_i(f(x)) - \lambda' x_i$ depends only on $p_i'(x) = \langle x_0, \dots, x_{i-1}\rangle$;
and $p(f(x)) - \lambda y$ depends only on $p'(x) = \langle x_0, \dots, x_{k-2}\rangle$.

We define Σ to be the set of triples

$$\langle f, \lambda', \lambda\rangle \in (\mathrm{Pol}_1\mathbf{A}) \times GF(q') \times GF(q)$$

that satisfy (13.9.9); and we define σ to be the set of pairs $\langle \lambda', \lambda\rangle$ such that $\langle f, \lambda', \lambda\rangle \in \Sigma$ for some f. We shall show that σ is an isomorphism of $\mathbf{GF}(q')$ with $\mathbf{GF}(q)$. Note that for each $f \in \mathrm{Pol}_1\mathbf{A}$ there is a unique $\langle \lambda', \lambda\rangle$ with $\langle f, \lambda', \lambda\rangle \in \Sigma$.

(13.9.10) For $i \leq k-1$,

$$p_i(d(x,y,z)) - (p_i(x) - p_i(y) + p_i(z))$$

depends only on $p_i'(x)$, $p_i'(y)$, $p_i'(z)$. If $\langle f, \lambda', \lambda\rangle$, $\langle g, \gamma', \gamma\rangle \in \Sigma$, then $\langle f \circ g, \lambda'\gamma', \lambda\gamma\rangle \in \Sigma$ and $\langle h, \lambda' + \gamma', \lambda + \gamma\rangle \in \Sigma$, where $h(x) = d(f(x), 0, g(x))$.

In (13.9.10), the claimed property of d follows easily from (13.9.7) and the Mal'cev equations for d; the other statement is then easily derived from (13.9.7).

(13.9.11) The domain of σ is $GF(q')$.

To prove this claim, we recall that $\theta_1 \prec 1_A$ where $\theta_1 = \ker p_1' = \ker p_0$. Thus $\mathbf{A}$ is minimal of type **2** with respect to $\langle \theta_1, 1_A\rangle$. This implies that $\mathbf{A}/\theta_1$ is polynomially equivalent to a vector space of dimension 1 over some $\mathbf{GF}(q'')$. The algebra $p_0(\mathbf{A}) \cong \mathbf{A}/\theta_1$ thus has precisely as many unary polynomials fixing 0 as it has elements; i.e., it has q' of them. In other words, $f(x) = \lambda' x$ is a polynomial of $p_0(\mathbf{A})$ for all $\lambda' \in GF(q')$. This implies statement (13.9.11).

(13.9.12) The range of σ is $GF(q)$.

This claim follows easily from (13.9.3). For every $\lambda \in GF(q)$ there is $f \in \mathrm{Pol}_1\mathbf{A}$ with $f(\langle \bar{0}, y\rangle) = \langle \bar{0}, \lambda y\rangle$ for all y. By (13.9.9) we have $\langle f, \gamma', \gamma\rangle \in \Sigma$ for some γ', γ. Then

$$pf(\langle \bar{0}, y\rangle) - \gamma \cdot y = \lambda \cdot y - \gamma \cdot y$$

is constant, so $\lambda = \gamma$.

(13.9.13) σ is an isomorphism of $\mathbf{GF}(q')$ onto $\mathbf{GF}(q)$.

This will follow by (13.9.10), (13.9.11), (13.9.12), if we establish that σ is a one-to-one function. At least, σ is a subring of $\mathbf{GF}(q') \times \mathbf{GF}(q)$ projecting onto both factors. Thus it suffices to show that if $\langle \lambda', 0\rangle \in \sigma$ then $\lambda' = 0$, and if $\langle 0, \lambda\rangle \in \sigma$ then $\lambda = 0$. Suppose that $\langle 0, \lambda\rangle \in \sigma$ and, say, $\langle f, 0, \lambda\rangle \in \Sigma$. Then $p_0 f$ is constant, so f is not a permutation of $\mathbf{A}$. Since $\mathbf{A}$ is minimal relative to $\langle 0_A, \delta\rangle$, it follows that $f|_{T_0}$ is constant. This implies that $\lambda = 0$. Similarly, if $\langle f, \lambda', 0\rangle \in \Sigma$, then f cannot be a permutation, and so $f(1_A) \subseteq \theta_1$ (again we use the E-minimality). This implies that $\lambda' = 0$.

We now have that $q' = q$ and $A = E(q, k)$. Let $\mathbf{B} = \langle A, \dots\rangle$ be the algebra satisfying $\pi : \mathbf{B} \cong \mathbf{A}$ where $\pi(\langle \bar{x}, y\rangle) = \langle \bar{x}, \sigma(y)\rangle$. We claim that $\mathbf{B}$ is a reduct of $\mathbf{E}(q, k)$. To prove it, we examine any polynomial $f \in \mathrm{Pol}_n\mathbf{B}$. By (13.9.7) and Definition 13.7, there are $\lambda_0, \lambda_0', \dots, \lambda_{n-1}, \lambda_{n-1}' \in GF(q)$ and $h_0, \dots, h_{k-1}$ such that for any $\tilde{x} \in B^n$ we have:

(13.9.14) For all $i \leq k-2$,

$$p_i(f(\tilde{x})) = \sum_j \lambda_j' \cdot p_i(x_j) + h_i(p_i'(\tilde{x})); \quad \text{while}$$

$$p(f(\tilde{x})) = \sigma^{-1}\left(\sum_j \lambda_j \cdot \sigma p(x_j) + h_{k-1}(p'(\tilde{x}))\right)$$

$$= \sum_j \sigma^{-1}(\lambda_j) \cdot p(x_j) + \sigma^{-1} h_{k-1}(p'(\tilde{x})).$$

These formulas will imply that f is a polynomial of $\mathbf{E}(q, k)$, as soon as we know that $\sigma^{-1}(\lambda_j) = \lambda_j'$. This is easily seen to be the case, by replacing all variables of f except the j th by 0. The formulas (13.9.14) imply that the resulting unary polynomial f_j corresponds to a unary polynomial h_j of $\mathbf{A}$ such that $\langle h_j, \lambda_j', \lambda_j\rangle \in \Sigma$. Thus $\sigma(\lambda_j') = \lambda_j$. This completes our proof. □

Exercises 13.10

(1) Let $\mathbf{A}$ be a tame algebra of type **1**. Let $\mathbf{B} = \langle N^k, \dots\rangle$ be the reduct of $\mathbf{N}^{[k]}$ constructed in Theorem 13.3, which has a subalgebra isomorphic to $\mathbf{A}$. Prove that $\mathbf{A}$ and $\mathbf{B}$ generate the same variety.

(2) This exercise refers to Theorem 13.5, but otherwise is the same as the first exercise.

(3) Using the result in Exercise 3.2 (3), show that an E-minimal algebra of type **2** is Abelian iff it is polynomially equivalent to a unitary module over a finite local ring.

(4) Show that an E-minimal algebra of type **2** has a Mal'cev *term* operation that is one-to-one in each variable when the others are held fixed. {Outline: Choose any maximal congruence δ. Then $\mathbf{A}$ is $\langle \delta, 1_A \rangle$-minimal of type **2**. We are in the situation of Lemma 4.20 with $A = C =$ the $\langle \delta, 1_A \rangle$-body. Choose a term $h(x, y, z, \bar{u})$ and choose $\bar{a} \in A^n$ so that the polynomial operation $h(x, y, z, \bar{a})$ corresponds to $x - y + z$ in the vector space $\mathbf{A}/\delta$. Then the term operation $f(x, y, z) = h(x, h(y, y, y, \ldots, y), z, y, \ldots, y)$ can be shown to also correspond to $x-y+z$ in $\mathbf{A}/\delta$. Moreover $f \in \mathrm{Clo}_3\mathbf{A}$. Starting with this f, the construction in the proof of Lemma 4.20 will produce a Mal'cev term operation having the desired property.}

(5) Let f be an n-ary operation and d be a Mal'cev operation of an algebra $\mathbf{A}$. Suppose that a_i and b_i are congruent modulo the center of $\mathbf{A}$ for $i = 0, \ldots, n-1$. Prove that $d(f(\bar{a}), f(\bar{b}), f(\bar{c})) = f(d(\bar{a}, \bar{b}, \bar{c}))$.

14. SIMPLE ALGEBRAS IN VARIETIES

It is known that two finite subdirectly irreducible algebras that generate the same congruence distributive variety must be isomorphic [19]; that two finite simple algebras that generate the same congruence modular variety must be isomorphic; that if $\mathbf{B}$ is finite, $\boldsymbol{V}(\mathbf{B})$ is congruence modular, $\mathbf{A}$ is simple and $\mathbf{A} \in \boldsymbol{V}(\mathbf{B})$, then $|\mathbf{A}| \leq |\mathbf{B}|$. (The second and third assertions are proved in [10].) To what extent can these results be generalized and extended outside congruence modular varieties?

Every finite simple algebra is tame, and has a type. Lemma 13.1 makes it clear that a locally finite variety $\mathcal{V}$ can have only a finite number (up to isomorphism) of finite, simple, Abelian algebras, for they are all homomorphic images of $\mathbf{F}_{\mathcal{V}}(k^k)$ where $k = |\mathbf{F}_{\mathcal{V}}(2)|$. We shall find that an infinite, simple, Abelian algebra cannot belong to any locally finite variety. Considering a variety $\mathcal{V} = \boldsymbol{V}(\mathbf{B})$ where $\mathbf{B}$ is finite, we shall show that if $\mathbf{5} \notin \operatorname{typ}\{\mathcal{V}\}$, then $\mathcal{V}$ has only finitely many simple algebras and they are finite; and if $\{\mathbf{1}, \mathbf{5}\} \cap \operatorname{typ}\{\mathcal{V}\} = \emptyset$, then a minimal congruence of an algebra in $\mathcal{V}$ cannot have an equivalence class of size exceeding $|\mathbf{B}|$, and any two simple algebras in $\mathcal{V}$ which generate equal varieties are isomorphic.

To start things off, we establish some bounds on the cardinalities of traces and of equivalence classes of minimal congruences in certain varieties. For any pair of congruences $\alpha \leq \beta$ in an algebra $\mathbf{A}$, $\sharp(\beta/\alpha)$ is defined to be the supremum of the cardinalities of the β/α equivalence classes in the algebra $\mathbf{A}/\alpha$. Our first lemma generalizes part of the content of Lemma 13.1.

LEMMA 14.1. *Let $\mathcal{V}$ be a locally finite variety generated by Abelian algebras. Let $\mathbf{A} \in \mathcal{V}$ and $\alpha \prec \beta$ in* Con $\mathbf{A}$. *If $\langle \alpha, \beta \rangle$ is not strongly Abelian then $\sharp(\beta/\alpha) \leq k^k$ where $k = |\mathbf{F}_{\mathcal{V}}(x, y)|$.*

PROOF. We assume the hypotheses, including that $\langle \alpha, \beta \rangle$ is not strongly Abelian. Factor by α and change notation, so that now $\alpha = 0$. We assume that $\sharp(\beta/0) > \ell = k^k$ ($k = |\mathbf{F}_{\mathcal{V}}(x, y)|$) and derive a contradiction. First we pass to a finite algebra. There exists (Definition 3.9) $f \in \operatorname{Pol}_{n+1}\mathbf{A}$ for some n, and $\bar{a}, \bar{b}, \bar{c} \in A^{n+1}$, such that

$$
\begin{aligned}
&f(a_0, \ldots, a_n) = f(b_0, \ldots, b_n), \\
&f(a_0, c_1, \ldots, c_n) = u \neq v = f(b_0, c_1, \ldots, c_n), \\
&a_0 \equiv b_0 \text{ and } a_i \equiv b_i \equiv c_i \pmod{\beta} \text{ for } i = 1, \ldots, n.
\end{aligned} \tag{14.1.1}
$$

Also there exist elements $d_0, \dots, d_\ell \in A$, all distinct and congruent modulo β. Note that since $0_A \prec \beta$,

$$\{\langle a_i, b_i\rangle : i \le n\} \cup \{\langle b_i, c_i\rangle : 1 \le i \le n\} \subseteq \Theta_{\mathbf{A}}(u, v)\,, \tag{14.1.2}$$
$$\Theta_{\mathbf{A}}(u, v) = \Theta_{\mathbf{A}}(d_p, d_q) \text{ for all } p < q \le \ell.$$

There exists a finite algebra $\mathbf{A}' \subseteq \mathbf{A}$ such that $\mathbf{A}'$ includes all the above mentioned elements, $f|_{A'}$ is a polynomial of $\mathbf{A}'$, and the formulas (14.1.2) are true in $\mathbf{A}'$. Choosing a maximal congruence δ among all those of $\mathbf{A}'$ not containing $\langle u, v\rangle$, and a cover $\gamma \succ \delta$ of δ, we find that $\sharp(\gamma/\delta) \ge \ell + 1$ and $\langle \delta, \gamma\rangle$ is not strongly Abelian.

We choose a finite free algebra $\mathbf{F} \in \mathcal{V}$ with a homomorphism π of $\mathbf{F}$ onto $\mathbf{A}'$. $\mathbf{F}$ is Abelian, since it can be embedded in a product of Abelian generating algebras of $\mathcal{V}$. We now change the original notation, setting $\alpha = \pi^{-1}(\delta)$, $\beta = \pi^{-1}(\gamma)$, and $\mathbf{A} = \mathbf{F}$. Thus we have a finite Abelian algebra $\mathbf{A} \in \mathcal{V}$ and a prime quotient $\langle \alpha, \beta\rangle$, not strongly Abelian, such that $\sharp(\beta/\alpha) \ge \ell + 1$. Using Theorem 7.2, we conclude that $\operatorname{typ}(\alpha, \beta) = \mathbf{2}$.

We can now virtually repeat the argument of Lemma 13.1 (2) to obtain the sought-after contradiction. Let $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, let $0 \in U$, and let T be a β-equivalence class. Since $\mathbf{A}$ is Abelian, so is $\mathbf{A}|_U$; hence every prime quotient of $\mathbf{A}|_U$ is Abelian (Theorem 7.2), and it follows by 4.27 (4) that U has empty tail with respect to $\langle \alpha|_U, \beta|_U\rangle$. Therefore, by Lemma 4.20, we have a polynomial $d(x, y, z)$ of $\mathbf{A}$ under which U is closed, such that $d|_U$ is Mal'cev and satisfies 4.20 with $C = B = U$.

Let $F' = \{f \in \operatorname{Pol}_1\mathbf{A} : f(A) \subseteq U \text{ and } f(0) = 0\}$. Suppose that $|F'| = m$, and enumerate $F' = \{f_0, \dots, f_{m-1}\}$ with $f_i(x) = e g_i(x, \bar{a})$ where $e \in F'$, $e^2 = e$, $e(A) = U$, $\bar{a} \in A^n$ (with $n = |A|$) and $g_i \in \operatorname{Clo}\mathbf{A}$. Let $g_i'(x, y) = g_i(x, y, \dots, y)$ and, choosing $a \in A$, put

$$f_i'(x) = d(e g_i'(x, a), e g_i'(0, a), 0).$$

If $f_i' = f_j'$ then $d(f_i'(x), f_j'(x), 0) = 0$. Using the Abelian property, we conclude that

$$d(d(e g_i(x, \bar{a}), e g_i(0, \bar{a}), 0), d(e g_j(x, \bar{a}), e g_j(0, \bar{a}), 0), 0)$$

is independent of x. Since its value is simply $d(f_i(x), f_j(x), 0)$, and since $f_i(0) = f_j(0) = 0$, we conclude that $d(f_i(x), f_j(x), 0) = 0$, which implies that $f_i(x) = f_j(x)$ by 4.20. Thus $f_i' = f_j'$ implies $i = j$; so $F' = \{f_0', \dots, f_{m-1}'\}$, and we have $m = |F'| \le |\operatorname{Clo}_2\mathbf{A}| \le k$.

By the properties of $d(x, y, z)$ on $U(= B)$ (Lemma 4.20), the group $(\operatorname{Pol}_1\mathbf{A}|_U) \cap (\operatorname{Sym} U)$ is transitive on U. Hence by 2.8 (4), for every $\langle x, y\rangle \in T^2 - \alpha$ there is $f \in F'$ with $\langle f(x), f(y)\rangle \notin \alpha$. The mapping

$$\pi(x) = \langle f_0(x)/\alpha, \dots, f_{m-1}(x)/\alpha\rangle, \text{ for } x \in T$$

therefore has kernel $\alpha|_T$, and serves to embed T/α into $\prod\{f_i(T)/\alpha : 0 \le i \le m-1\}$. To get that $|T/\alpha| \le \ell$, it suffices to show that $|f_i(T)/\alpha| \le k$, since $m \le k$.

For each $i < m$, $f_i(T)$ is contained in one $\beta|_U$ equivalence class N', which is an $\langle \alpha|_U, \beta|_U\rangle$-trace since U has no tail. We have $N' \simeq N$ where N is the trace containing 0. The elements of the field over which $(\mathbf{A}|_N)/\alpha$ is a vector space are just the $(f|_N)_\alpha$, $f \in F'$; hence the 1-dimensional vector space $(\mathbf{A}|_N)/\alpha$ has cardinality $\leq m \leq k$. The same is true for $|N'/\alpha|$. This concludes our proof that $|T/\alpha| \leq k^k = \ell$. This is true for all β-equivalence classes T, contradicting that $\sharp(\beta/\alpha) > \ell$. □

LEMMA 14.2. *Let $\mathcal{V}$ be a locally finite variety generated by strongly Abelian algebras. For $\mathbf{A} \in \mathcal{V}$ and $\alpha \prec \beta$ in $\operatorname{Con}\mathbf{A}$ we have $\sharp(\beta/\alpha) \leq \max(2, k_1)^{k_2}$, where $k_1 = |\mathbf{F}_\mathcal{V}(x)|$ and $k_2 = |\mathbf{F}_\mathcal{V}(x, y)|$.*

PROOF. Following the lines of the last argument, we see that it is sufficient to consider a finite strongly Abelian algebra $\mathbf{A} \in \mathcal{V}$ and a prime quotient $\langle \alpha, \beta\rangle$ of $\mathbf{A}$. This we now do. By Theorem 7.2, we have $\operatorname{typ}(\alpha, \beta) = \mathbf{1}$.

To begin, we claim that for every $\langle x, y\rangle \in \beta - \alpha$, there is an element $e \in \mathrm{E}(\mathbf{A})$ such that $e(A) \in \mathrm{M}_\mathbf{A}(\alpha, \beta)$ and $\langle e(x), e(y)\rangle \notin \alpha$. Indeed, by 2.8 (4) there is $f \in \mathrm{Pol}_1\mathbf{A}$ such that $f(A) \in \mathrm{M}_\mathbf{A}(\alpha, \beta)$ and $\langle f(x), f(y)\rangle \notin \alpha$. By 2.8 (6), for this f, there is $U \in \mathrm{M}_\mathbf{A}(\alpha, \beta)$ such that $f : U \simeq f(U)$. Thus there is $g \in \mathrm{Pol}_1\mathbf{A}$ such that $gf|_U = \mathrm{id}_U$. By 2.8 (1), $f(A) \simeq U \simeq f(U)$, hence $f(U) = f(A)$ (since $f(U) \subseteq f(A)$). Now it follows easily that $gf \in \mathrm{E}(\mathbf{A})$, that $gf(A) = U$, and that $\langle gf(x), gf(y)\rangle \notin \alpha$.

Now let T be any β-equivalence class, let $a \in A$, and define

$$F_a = \{e \in \mathrm{E}(\mathbf{A}) : e(A) \in \mathrm{M}_\mathbf{A}(\alpha, \beta) \text{ and } e(x) = f(x, a) \text{ for some } f \in \mathrm{Clo}_2\mathbf{A}\}.$$

Notice that $|F_a| \leq k_2$. Using the claim above, we shall now prove that, modulo α, F_a separates the points of T.

To do this, let $\langle u, v\rangle \in T^2 - \alpha$. Let $e \in \mathrm{E}(\mathbf{A})$ satisfy $\langle e(u), e(v)\rangle \notin \alpha$, $e(A) \in \mathrm{M}_\mathbf{A}(\alpha, \beta)$. Choose $f(x, \bar{y}) \in \mathrm{Clo}_{n+1}\mathbf{A}$ for some n, and $\bar{c} \in A^n$ such that $e(x) = f(x, \bar{c})$. By Lemma 4.4, since $e^2 = e$, we can arrange that the equation

$$f(f(x, \bar{y}), \bar{y}) = f(x, \bar{y})$$

holds in $\mathbf{A}$. Since $\mathbf{A}$ is Abelian, the equation

$$f(f(x, \bar{y}), \bar{z}) = f(x, \bar{z})$$

holds also. For $\bar{r} \in A^n$, write $f^{\bar{r}}(x) = f(x, \bar{r})$; then we have $f^{\bar{r}} \circ f^{\bar{s}} = f^{\bar{r}}$ for all $\bar{r}, \bar{s}$. From this it follows that

$$f^{\bar{r}} \in \mathrm{E}(\mathbf{A}),\ f^{\bar{r}}(A) \simeq f^{\bar{c}}(A),\ \text{and } \langle f^{\bar{r}}(u), f^{\bar{r}}(v)\rangle \notin \alpha$$

for each $\bar{r} \in A^n$. Clearly, then, for $\bar{r} = \langle a, \ldots, a\rangle$, we have $f^{\bar{r}} \in F_a$ and $\langle f^{\bar{r}}(u), f^{\bar{r}}(v)\rangle \notin \alpha$.

From what we have shown, the mapping $\pi(x/\alpha) = \langle e(x)/\alpha : e \in F_a \rangle$ embeds T/α into $\Pi\{e(T)/\alpha : e \in F_a\}$. To see that $|T/\alpha| \leq \max(2, k_1)^{k_2}$, as desired, it only remains to see that $|e(T)/\alpha| \leq \max(2, k_1)$ for each $e \in F_a$.

To see this, let $e \in F_a$, $e(A) = U$. We can assume that $|e(T)/\alpha| > 2$; thus $e(T)$ is included in one $\langle \alpha, \beta \rangle$-trace N in U, and $|N/\alpha| > 2$. Define

$$\Pi = \{ef|_U : f \in \mathrm{Clo}_1\mathbf{A}\} \cap \mathrm{Sym}\, U.$$

Obviously, $|\Pi| \leq k_1$. We claim that $\Pi = (\mathrm{Pol}_1\mathbf{A}|_U) \cap (\mathrm{Sym}\, U)$. To verify this claim, let $g \in (\mathrm{Pol}_1\mathbf{A}|_U) \cap (\mathrm{Sym}\, U)$. For some $h(x, \bar{y}) \in \mathrm{Clo}_{n+1}\mathbf{A}$ (for some n) and $\bar{a} \in A^n$ we have $g(x) = h(x, \bar{a}) = eh(x, \bar{a})$ for all $x \in U$. Let $f(x) = h(x, x, \ldots, x)$. For any $u \in U$, we can pick $v \in U$ such that

$$eh(u, \ldots, u) = g(v) = eh(v, a_1, \ldots, a_n).$$

Since $\mathbf{A}$ is strongly Abelian, this equation implies that $eh(u, \ldots, u) = eh(u, a_1, \ldots, a_n)$. Thus $g(u) = ef(u)$ for all $u \in U$, consequently, $g \in \Pi$.

Now $\mathbf{A}|_U$ is minimal relative to $\langle \alpha|_U, \beta|_U \rangle$, and every $f \in \mathrm{Pol}_1\mathbf{A}|_U$ either belongs to Π or satisfies $f(N) \times f(N) \subseteq \alpha$. Thus the simple minimal algebra $(\mathbf{A}|_N)/(\alpha|_N)$ of type **1** has for unary polynomials just the constants and the functions $(f|_N)_\alpha$ (such that $f \in \Pi$ and $f(N) = N$), which are permutations of $N/(\alpha|_N)$. Since the algebra is simple and has ≥ 3 elements, this set of $\leq k_1$ permutations must be transitive on $N/(\alpha|_N)$; hence $|e(T)/\alpha| \leq |N/(\alpha|_N)| \leq k_1$. □

THEOREM 14.3. *Let $\mathcal{V}$ be a locally finite variety. Every simple Abelian algebra in $\mathcal{V}$ has cardinality not greater than k^k where $k = |\mathbf{F}_\mathcal{V}(x, y)|$.*

PROOF. Suppose that $\mathbf{A}$ is a simple Abelian algebra in $\mathcal{V}$, and put $\mathcal{V}' = \boldsymbol{V}(\mathbf{A})$, and $\langle \alpha, \beta \rangle = \langle 0_A, 1_A \rangle$. Notice that $\mathcal{V}'$ is locally finite and $|\mathbf{F}_{\mathcal{V}'}(x, y)| \leq |\mathbf{F}_\mathcal{V}(x, y)|$. Thus Lemma 14.2 gives the desired conclusion if $\mathbf{A}$ is strongly Abelian, and otherwise Lemma 14.1 gives the conclusion. □

The next lemma is related to Corollary 5.17.

LEMMA 14.4. *Let $\mathbf{A}$ and $\mathbf{B}$ be finite algebras, $\mathbf{A} \in \boldsymbol{V}(\mathbf{B})$, and let β be a minimal congruence of $\mathbf{A}$ such that $\mathrm{typ}(0, \beta) \in \{\mathbf{3}, \mathbf{4}\}$. Then $\sharp(\beta/0) \leq |\mathbf{B}|$. If $\mathbf{A}$ is subdirectly irreducible and the $\langle 0, \beta \rangle$-minimal sets have empty tails, then $\mathbf{A} \in \boldsymbol{HS}(\mathbf{B})$.*

PROOF. We assume the hypotheses. For some finite m there is an algebra $\mathbf{S} \subseteq \mathbf{B}^m$ and a homomorphism π of $\mathbf{S}$ onto $\mathbf{A}$. Let $\delta = \pi^{-1}(0_A)$ and $\gamma = \pi^{-1}(\beta)$. For $i < m$, let η_i be the kernel of the ith projection of $\mathbf{S}$ into $\mathbf{B}$. We have that $\delta \prec \gamma$ and (by 5.3) $\mathrm{typ}(\delta, \gamma) = \mathrm{typ}(0, \beta)$. Let μ be the pseudo-complement of δ under γ (Remark 5.16). For each i such that $\gamma \wedge \eta_i \not\leq \delta$, we must have $\gamma \wedge \eta_i \geq \mu$. Since $\mu \neq 0_S$ and

$\eta_0 \wedge \cdots \wedge \eta_{m-1} = 0_S$, there is an i such that $\gamma \wedge \eta_i \leq \delta$. This inclusion directly implies that

$$\sharp(\beta/0) = \sharp(\gamma/\delta) \leq \sharp(\gamma/\gamma \wedge \eta_i) \leq \sharp(1_S/\eta_i) \leq |\mathbf{B}|.$$

Now let $\mathbf{A}$ be subdirectly irreducible and assume that the $\langle 0, \beta\rangle$-minimal sets have no tails. By Lemma 2.18, the $\langle \delta, \gamma\rangle$-minimal sets in S have no tails. Let $U \in \mathrm{M}_{\mathbf{S}}(\delta, \gamma)$. By Lemma 4.17 (applied to $\mathbf{S}|_U$), $|U| = 2$, say $U = \{0, 1\}$ where $\langle 0, 1\rangle \in \gamma - \delta$. Now again choose i such that $\gamma \wedge \eta_i \leq \delta$. Then clearly $\delta|_U \vee \eta_i|_U = \mathrm{id}_U$. Since $|_U$ is a lattice homomorphism, it follows that $\langle 0, 1\rangle \notin \delta \vee \eta_i$. Thus $\gamma \not\leq \delta \vee \eta_i$, implying that $\eta_i \leq \delta$ since $\mathbf{A}$ is subdirectly irreducible. (If $\chi > \delta$, $\chi \in \mathrm{Con}\,\mathbf{S}$, then $\chi \geq \gamma$.) Finally, $\eta_i \leq \delta$ implies that $\mathbf{A} \cong \mathbf{S}/\delta$ is a homomorphic image of $\mathbf{S}/\eta_i$, where $\mathbf{S}/\eta_i$ is isomorphic to a subalgebra of $\mathbf{B}$. □

THEOREM 14.5. *Let $\mathcal{V} = \boldsymbol{V}(\mathbf{B})$ where $\mathbf{B}$ is a finite algebra.*

(1) *$\mathcal{V}$ has, up to isomorphism, only a finite set of finite simple algebras of types $\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}$.*

(2) *If $\mathbf{5} \notin \mathrm{typ}\{\mathcal{V}\}$, then every simple non-Abelian algebra in $\mathcal{V}$ belongs to $\boldsymbol{HS}(\mathbf{B})$, and every simple Abelian algebra in $\mathcal{V}$ is a homomorphic image of $\mathbf{F}_{\mathcal{V}}(k^k)$ where $k = |\mathbf{F}_{\mathcal{V}}(2)|$.*

PROOF. Almost every assertion in this theorem is already covered by Theorem 14.3 or Corollary 5.17. All that remains to be shown is that if $\mathcal{V}$ has an infinite simple algebra then $\mathbf{5} \in \mathrm{typ}\{\mathcal{V}\}$.

Suppose that $\mathbf{S}$ is an infinite simple algebra in $\mathcal{V}$. By Theorem 14.3, $\mathbf{S}$ is non-Abelian. Choose any finite non-Abelian subalgebra $\mathbf{S}_1$ in $\mathbf{S}$ with $|\mathbf{S}_1| > |\mathbf{B}|$. ($\mathcal{V}$ is locally finite.) There must exist a finite algebra $\mathbf{S}_2$, $\mathbf{S}_1 \subseteq \mathbf{S}_2 \subset \mathbf{S}$, such that for all $\{x, y, u, v\} \subseteq S_1$, $u \neq v$ implies $\langle x, y\rangle \in \Theta_{\mathbf{S}_2}(u, v)$ (since $\mathbf{S}$ is simple). Let α be any maximal member of the set $\{\delta \in \mathrm{Con}\,\mathbf{S}_2 : \delta|_{S_1} = 0_{S_1}\}$; and choose a cover $\beta \succ \alpha$ in $\mathrm{Con}\,\mathbf{S}_2$. Now S_1 is contained in one β-equivalence class, and $\alpha|_{S_1} = 0_{S_1}$, implying that $\sharp(\beta/\alpha) \geq |S_1| > |\mathbf{B}|$ and $\langle \alpha, \beta\rangle$ is non-Abelian. It follows now from Lemma 14.4 (applied to $\mathbf{A} = \mathbf{S}_2/\alpha$ and its minimal congruence β/α) that $\mathrm{typ}(\alpha, \beta) = \mathrm{typ}(0, \beta/\alpha) \notin \{\mathbf{3}, \mathbf{4}\}$. Since $\langle \alpha, \beta\rangle$ is non-Abelian, its type can only be $\mathbf{5}$. □

In varieties omitting both the unary and the semilattice type, we have a strong result virtually identical to what was known for congruence modular varieties.

THEOREM 14.6. *Suppose that $\mathrm{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{5}\} = \emptyset$ and that $\mathbf{B}$ is a finite algebra in $\mathcal{V}$, where $\mathcal{V}$ is locally finite.*

(1) *For every $\mathbf{A} \in \boldsymbol{V}(\mathbf{B})$ and $\alpha \prec \beta$ in $\mathrm{Con}\,\mathbf{A}$ we have $\sharp(\beta/\alpha) \leq |\mathbf{B}|$.*

(2) *If $\mathbf{A}_1$ and $\mathbf{A}_2$ are finite simple algebras in $\mathcal{V}$ then*

$$\boldsymbol{V}(\mathbf{A}_1) = \boldsymbol{V}(\mathbf{A}_2) \text{ implies } \mathbf{A}_1 \cong \mathbf{A}_2.$$

PROOF. As we have seen in the proof of 14.1, to prove (1), it will suffice to prove it for finite algebras in $\boldsymbol{V}(\mathbf{B})$. By Theorem 0.2, we need only consider subalgebras of finite powers of $\mathbf{B}$, since every finite algebra in $\boldsymbol{V}(\mathbf{B})$ is a homomorphic image of such an algebra. So let $\mathbf{A} \subseteq \mathbf{B}^n$ and $\alpha \prec \beta$ in Con $\mathbf{A}$. If $\langle \alpha, \beta \rangle$ is non-Abelian, then we have the desired result from Lemma 14.4 (after passing to the algebra $\mathbf{A}/\alpha$). Assume now that $\langle \alpha, \beta \rangle$ is Abelian. Let T be any β-equivalence class. By Theorem 7.12, there is a term operation $p(x, y, z)$ of $\mathbf{A}$ such that T is closed under this operation and for all $x, y \in T$, we have $p(x, y, y) \equiv x \equiv p(y, y, x) \pmod{\alpha}$ and $p(x, x, x) = x$.

Now let K be the set of all sets of the form $e(T)$ where $e \in \mathrm{E}(\mathbf{A})$, $e(T) \subseteq T$, and $e(x) \equiv x \pmod{\alpha}$ for all $x \in T$. Let $S = e(T)$ be a minimal member of K, where e satisfies the conditions just laid down.

Claim. $\mathbf{A}|_S$ is Mal'cev.

To prove this claim, let $f(x, y, z) = ep(ex, ey, ez)$. Notice that $f(T^3) \subseteq S$ and $f(x, y, y) \equiv f(y, y, x) \equiv x \pmod{\alpha}$ for all $x, y \in T$. For every $a \in S$, the function $h(x) = f(a, a, x)$ has a power h^m which is idempotent, and $h^m(x) \equiv h(x) \equiv x \pmod{\alpha}$ for all $x \in T$ while $h^m = eh^m e$. By the minimality of S, we have $h^m(T) = S$ and so $h^m(x) = x$ for $x \in S$. Proceeding as in the proof of 4.20 (Claim 3 there), we can construct a polynomial f' of $\mathbf{A}$ such that $f'(T^3) \subseteq S$ and $f'(x, x, y) = y$ for all $x, y \in S$ while $f'(x, y, y) \equiv x \pmod{\alpha}$ for all $x, y \in T$. Finally, proceeding through the proof of Claim 4 in 4.20, we can construct a polynomial $d(x, y, z)$ such that $d(T^3) = S$ and $d|_S$ is Mal'cev. Thus our claim is true.

Now let $\mathbf{S} = \mathbf{A}|_S$ and let $\eta_0, \ldots, \eta_{n-1}$ be the restrictions to S of the kernels of the projections of $\mathbf{B}^n$ onto $\mathbf{B}$. Henceforth, we consider only congruences in $\mathbf{S}$. Letting $\alpha' = \alpha|_S$, we have $|S/\alpha'| = |T/\alpha|$, and we wish to prove that this number is $\leq |\mathbf{B}|$. Notice that $\alpha' \prec 1_S$ in Con $\mathbf{S}$, $\sharp(1_S/\eta_i) \leq |\mathbf{B}|$ for all i, and $\bigwedge\{\eta_i : i < n\} = 0_S$. The argument from this point is the same as the one that was used in [10].

Namely, we find a system $\{\eta_i'\} = \{\eta_0', \eta_1', \ldots, \eta_{n-1}'\}$ such that $\eta_i' \geq \eta_i$ for all i, $\bigwedge \eta_i' \leq \alpha'$, and where this fails to be true for any $\{\eta_i''\}$ that has $\eta_i'' > \eta_i'$ for some i and $\eta_i'' \geq \eta_i'$ for all $i < n$. We can assume that $\eta_0' \neq 1_S$. Then $\bar{\eta}' = \eta_1' \wedge \cdots \wedge \eta_{n-1}'$ is not $\leq \alpha'$ (else η_0' could have been replaced by 1_S). If $\eta_0' \leq \alpha'$ we are done, $\sharp(1_S/\alpha') \leq \sharp(1_S/\eta_0') \leq |\mathbf{B}|$; so we assume $\eta_0' \not\leq \alpha'$, $\bar{\eta}' \not\leq \alpha'$. Now $(\eta_0' \vee (\alpha' \wedge \bar{\eta}')) \wedge \eta_1' \wedge \cdots \wedge \eta_{n-1}' \leq \alpha'$, by the modularity of **Con S**; hence $\alpha' \wedge \bar{\eta}' \leq \eta_0'$ by the choice of the system $\{\eta_i'\}$. We now have the picture in Figure 36 (which is *not* claimed to represent a *sublattice* of **Con S**). Note that $\alpha' \vee \bar{\eta}' = 1_S$ because $\alpha' \prec 1_S$.

The algebra $\mathbf{S}$ is Mal'cev, so its congruences permute. Thus by Exercise 14.9 (7), $\sharp(\gamma/\lambda) = \sharp(\varepsilon/\delta)$ whenever $I[\lambda, \gamma]$ and $I[\delta, \varepsilon]$ are projective intervals in **Con S**. So we have $\sharp(1_S/\alpha') = \sharp(\bar{\eta}'/\bar{\eta}' \wedge \eta_0') = \sharp(\bar{\eta}' \vee \eta_0'/\eta_0') \leq \sharp(1_S/\eta_0')$, and this finishes our proof of (1).

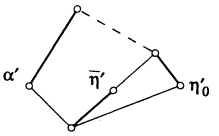


Figure 36

To prove (2), let $\mathbf{A}_1$ and $\mathbf{A}_2$ be finite simple algebras in $\mathcal{V}$ such that $\boldsymbol{V}(\mathbf{A}_1) = \boldsymbol{V}(\mathbf{A}_2)$. In Theorem 14.8, we prove that $\mathbf{A}_1$ and $\mathbf{A}_2$ have the same type, and are isomorphic unless the type is **1**, **2**, or **5**. Using that, we can assume that $\text{typ}(\mathbf{A}_1) = \text{typ}(\mathbf{A}_2) = \mathbf{2}$. Now by Theorems 7.6 and 7.11, $\mathbf{A}_1$ and $\mathbf{A}_2$ belong to the variety of locally solvable algebras in $\mathcal{V}$, which is a congruence permutable variety. Hence they are isomorphic, by [11, Theorem 10.10]. □

Before continuing to our last theorem, we note one further result along the lines of 14.1, 14.2, 14.4. Since it remains in the nature of an isolated curiosity, we shall merely outline the proof.

THEOREM 14.7. *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be finite algebras,* $\mathbf{A} \in \boldsymbol{V}(\mathbf{B})$, *and let* $0 \prec \beta$ *in* Con $\mathbf{A}$ *and* N *be any* $\langle 0, \beta\rangle$*-trace. The cardinality of* N *is no greater than the maximum cardinality of a subgroup of the semigroup* $\langle \text{Pol}_1\mathbf{B}, \circ\rangle$ *(or* 2, *whichever is greater).*

PROOF. We consider the group $\mathbf{P} = \langle \Pi, \circ\rangle$ of non-constant unary polynomials of $\mathbf{A}|_N$. This group is in $\boldsymbol{HS}(\langle \text{Pol}_1\mathbf{A}, \circ\rangle)$; and it is easy to see that $\langle \text{Pol}_1\mathbf{A}, \circ\rangle$ is in the variety of semigroups generated by $\langle \text{Pol}_1\mathbf{B}, \circ\rangle$. (Consider any equation that fails to hold in the first semigroup.) It can be proved that when $\mathbf{C}$ and $\mathbf{D}$ are finite semigroups, and $\mathbf{C} \in \boldsymbol{V}(\mathbf{D})$, then every *subgroup* of $\mathbf{C}$ lies in the variety generated by the subgroups of $\mathbf{D}$. Let $\mathbf{G}_1, \ldots, \mathbf{G}_n$ be the subgroups of $\langle \text{Pol}_1\mathbf{B}, \circ\rangle$, and let Π' be a minimal normal subgroup of $\mathbf{P}$. Since $\mathbf{P} \in \boldsymbol{V}(\mathbf{G}_1, \ldots, \mathbf{G}_n)$, it follows from a refined version of Theorem 14.6 that $|\Pi'| \leq \max(|\mathbf{G}_1|, \ldots, |\mathbf{G}_n|)$.

Now the relation

$$\{\langle x, y\rangle \in N^2 : y = f(x) \text{ for some } f \in \Pi'\} = \theta$$

is easily seen to be a non-zero congruence of the algebra $\langle N, \Pi\rangle$. Since $\langle N, \Pi\rangle$ is simple (polynomially equivalent to $\mathbf{A}|_N$), we have $\theta = N^2$. Thus Π' is transitive on N and $|N| \leq |\Pi'|$. (We ignored the case $\Pi = \{\text{id}\}$, where $|N| = 2$.) □

THEOREM 14.8. *Suppose that* $\mathbf{A}$ *and* $\mathbf{B}$ *are finite simple algebras and* $\boldsymbol{V}(\mathbf{A}) = \boldsymbol{V}(\mathbf{B})$. *Then* $\text{typ}(\mathbf{A}) = \text{typ}(\mathbf{B})$; *and* $\mathbf{A} \cong \mathbf{B}$ *if this type is* **3** *or* **4**.

PROOF. If either of $\mathbf{A}$ or $\mathbf{B}$ has type **1**, then $\mathcal{V} = \boldsymbol{V}(\mathbf{A}) = \boldsymbol{V}(\mathbf{B})$ is locally strongly solvable (Corollary 7.6); then $\text{typ}\{\mathcal{V}\} = \{\mathbf{1}\}$ and both simple algebras have type **1**.

If one of them has type **2**, then $\mathcal{V}$ is locally solvable, $\text{typ}\{\mathcal{V}\} \subseteq \{\mathbf{1}, \mathbf{2}\}$, and so both have type **2** since neither has type **1**. If $\{\text{typ}(\mathbf{A}), \text{typ}(\mathbf{B})\} \subseteq \{\mathbf{3}, \mathbf{4}\}$, then $\mathbf{A} \in \boldsymbol{HS}(\mathbf{B})$ and $\mathbf{B} \in \boldsymbol{HS}(\mathbf{A})$ by 5.17, hence $\mathbf{A} \cong \mathbf{B}$.

It remains only to reject the possibility that one of the types is **5** and the other is **3** or **4**. So assume that $\text{typ}(\mathbf{A}) = \mathbf{5}$ and $\text{typ}(\mathbf{B}) \in \{\mathbf{3}, \mathbf{4}\}$. There is an integer m, an algebra $\mathbf{S} \subseteq \mathbf{B}^m$, and a congruence θ on $\mathbf{S}$ with $\mathbf{S}/\theta \cong \mathbf{A}$. We assume that m is minimal. By 5.17, $\mathbf{B} \in \boldsymbol{HS}(\mathbf{A})$, leading to an algebra $\mathbf{S}_1 \subseteq \mathbf{S}$ with a congruence $\delta \geq \theta|_{S_1}$ such that $\mathbf{S}_1/\delta \cong \mathbf{B}$. Now $\delta \prec 1_{S_1}$ and $\text{typ}(\delta, 1_{S_1}) = \text{typ}(\mathbf{B})$; hence, as in the proof of 5.17, there is $i < m$ such that $\eta_i|_{S_1} \leq \delta$, where η_i is the kernel of the ith projection of $\mathbf{B}^m$ to $\mathbf{B}$. We shall assume that $i = 0$.

Now $\mathbf{S}_1/(\eta_0|_{S_1})$ is isomorphic to a subalgebra of $\mathbf{B}^m/\eta_0 \cong \mathbf{B}$, and $\mathbf{S}_1/\delta \cong \mathbf{B}$, while $\eta_0|_{S_1} \leq \delta$; so we have $\delta = \eta_0|_{S_1}$ since $\mathbf{B}$ is finite. Since $|\mathbf{B}^m/\eta_0| = |\mathbf{S}_1/(\eta_0|_{S_1})|$, we have that for all $x \in B^m$, $x/\eta_0 \cap S_1 \neq \emptyset$. Thus $\mathbf{S}/(\eta_0|_S) \cong \mathbf{S}_1/(\eta_0|_{S_1}) \cong \mathbf{B}$. Let us summarize and reformulate what we have learned.

(14.8.1) $\theta \prec 1_S$, $\text{typ}(\theta, 1_S) = \mathbf{5}$ $(= \text{typ}(\mathbf{A}))$;
$\mathbf{S}_1 \subseteq \mathbf{S}$, $\theta|_{S_1} \leq \eta_0|_{S_1} \prec 1_{S_1}$, $\text{typ}(\eta_0|_{S_1}, 1_{S_1}) = \text{typ}(\mathbf{B}) \in \{\mathbf{3}, \mathbf{4}\}$;
$x/\eta_0 \cap S_1 \neq \emptyset$ for each $x \in S$.

We denote $\bigwedge\{\eta_i : i > 0\}$ by $\bar{\eta}_0$. Since m was minimal, $\bar{\eta}_0|_S \not\leq \theta$. Then by 2.8 (4) we deduce

(14.8.2) every $U \in \text{M}_{\mathbf{S}}(\theta, 1_S)$, satisfies $\bar{\eta}_0|_U \not\leq \theta|_U$.

Now we choose any $U_1 \in \text{M}_{\mathbf{S}_1}(\eta_0|_{S_1}, 1_{S_1})$. It is easy to see that there is $e \in \text{E}(\mathbf{S})$ with $e(S_1) = U_1$ and $e|_{S_1} \in \text{E}(\mathbf{S}_1)$. We choose such an e with $e(S)$ minimal (under inclusion) among all sets $f(S)$ where $f \in \text{E}(\mathbf{S})$, $f|_{S_1} \in \text{E}(\mathbf{S}_1)$, and $f(S_1) = U_1$. Since $\theta|_{S_1} \leq \eta_0|_{S_1}$, we have $e(1_S) \not\subseteq \theta$; hence by 2.8 (6) and 2.8 (3), $e(S)$ contains some member U of $\text{M}_{\mathbf{S}}(\theta, 1_S)$; and from (14.8.2) we get that there is $\langle u, v\rangle \in (\bar{\eta}_0 - \theta) \cap U^2$. By (14.8.1) there is $u_1 \in S_1$, $u_1 \equiv u \pmod{\eta_0}$. Then $u = e(u) \equiv e(u_1) \pmod{\eta_0}$. Thus, changing notation, $\langle u, u_1\rangle \in \eta_0$, $u_1 \in U_1$. Similarly, we have some $v_1 \in U_1$, $\langle v, v_1\rangle \in \eta_0$. Now by 4.17, U_1 is a two-element set, say $U_1 = \{0, 1\}$. Since $\langle u, v\rangle \in \bar{\eta}_0 - 0_S$, $\langle u, v\rangle \notin \eta_0$; hence $\{u_1, v_1\} = \{0, 1\}$. Changing notation, (exchanging u, v if necessary) we now have

(14.8.3) $e \in \text{E}(\mathbf{S})$, $e|_{S_1} \in \text{E}(\mathbf{S}_1)$, $e(S_1) = U_1 = \{0, 1\} \in \text{M}_{\mathbf{S}_1}(\eta_0|_{S_1}, 1_{S_1})$;
$e(S) \supseteq U \in \text{M}_{\mathbf{S}}(\theta, 1_S)$, $\langle u, v\rangle \in \bar{\eta}_0|_U - \theta|_U$, $\langle u, 0\rangle \in \eta_0$ and $\langle v, 1\rangle \in \eta_0$.

Since $\text{typ}(\eta_0|_{S_1}, 1_{S_1}) \in \{\mathbf{3}, \mathbf{4}\}$, there is $q_1 \in \text{Pol}_2\mathbf{S}_1$, and hence $q \in \text{Pol}_2\mathbf{S}$, such that $q|_{S_1} \in \text{Pol}_2\mathbf{S}_1$ and $q(0, 1) = q(1, 0) = q(1, 1) = 1$, $q(0, 0) = 0$. Letting $h(x) = eq(x, x)$, and taking $q'(x, y) = h^{n-1}q(x, y)$ where $h^n = h^{2n}$, then q' has the properties assumed of q; and moreover, the minimality of e implies that $h^n(S) = e(S)$, and hence that

$q'(u,u) = h^n(u) = u$ and $q'(v,v) = v$. Furthermore,

$$q'(u,v) \equiv q'(v,v) = v \pmod{\bar{\eta}_0},$$

$$q'(u,v) \equiv q'(0,1) = 1 \equiv v \pmod{\eta_0}.$$

Since $\eta_0 \cap \bar{\eta}_0 = \mathrm{id}$, we have $q'(u,v) = v$. Likewise, we have $q'(v,u) = v$. A similar argument applied to a meet operation on $\{0,1\}$ completes the derivation of the following assertion.

(14.8.4) $\quad \mathbf{S}|_{\{u,v\}}$ has the operations of a two-element lattice.

Now by 4.15, since $\mathrm{typ}(\theta, 1_S) = \mathbf{5}$, U is the disjoint union of $u/(\theta|_U)$ and $v/(\theta|_U)$. Since U is the range of some member of $\mathrm{E}(\mathbf{S})$, we easily conclude from (14.8.4) that $(\mathbf{S}|_U)/(\theta|_U)$ is a two-element algebra having at least the operations of a lattice. This contradicts our assumption that $\mathrm{typ}(\theta, 1_S) = \mathbf{5}$. The proof is finished. □

Exercises 14.9

(1) Suppose that $\mathcal{V}$ is a locally finite variety and that $\mathbf{A}$ is a finite simple algebra of type **3** or **4** belonging to $\mathcal{V}$. Show that there is an equation ε satisfying $\mathbf{B} \models \varepsilon \Leftrightarrow \mathbf{A} \notin \boldsymbol{HS}(\mathbf{B}) \Leftrightarrow \mathbf{A} \notin \boldsymbol{V}(\mathbf{B})$ for all $\mathbf{B} \in \mathcal{V}$.

(2) Let $\mathcal{V} = \boldsymbol{V}(\mathbf{B}_1, \ldots, \mathbf{B}_n)$ and assume that $\mathcal{V}$ is congruence modular and $\mathbf{B}_1, \ldots, \mathbf{B}_n$ are finite. Let k be the maximum of $\sharp(\gamma/\delta)$ with $\langle \delta, \gamma \rangle$ ranging over prime quotients of the $\mathbf{B}_i$. Show that $\sharp(\beta/\alpha) \leq k$ whenever $\mathbf{A} \in \mathcal{V}$ and $\alpha \prec \beta$ in $\mathrm{Con}\,\mathbf{A}$. (Can congruence modularity be relaxed to: $\mathrm{typ}\{\mathcal{V}\} \cap \{\mathbf{1}, \mathbf{5}\} = \emptyset$? We do not know the answer to this.)

(3) Let $\mathbf{G}$ be a finite simple group with maximal subgroups $\mathbf{H}_0, \mathbf{H}_1$. Show that $\langle \{xH_i : x \in G\},\ f_\lambda(\lambda \in G) \rangle = \mathbf{A}_i$ are simple algebras of type **1**, where $f_\lambda(xH_i) = \lambda x H_i$. Show also that $\mathbf{A}_0 \cong \mathbf{A}_1$ iff H_0 and H_1 are conjugate subgroups. Taking $\mathbf{G}$ to be the alternating group on five letters, prove in this way that there are two non-isomorphic simple algebras of type **1** which generate the same variety. (Do there exist examples like this one, except that the algebras have type **2**? We do not know.)

(4) Here is an example due to C. Shallon of a four-element simple algebra whose variety has simple algebras of every cardinality ≥ 4 (finite and infinite). For finite $n \geq 4$, let $\mathbf{S}_n = \langle \{0, \ldots, n-1\},\ \cdot \rangle$ where $x \cdot y = x$ if $x \neq 0 \neq y$ and $|x - y| \leq 1$, and $x \cdot y = 0$ otherwise. These algebras are simple, and $\mathbf{S}_i$ is a subalgebra of $\mathbf{S}_j$ when $i \leq j$. Show that $\mathbf{S}_n \in \boldsymbol{HS}(\mathbf{S}_4^n)$ for each n, and conclude that $\boldsymbol{V}(\mathbf{S}_4) = \boldsymbol{V}(\mathbf{S}_n)$ for all n.

(5) Let R be a symmetric, irreflexive relation on a set X (so that $\langle X\ ,\ R \rangle$ is a graph), and put $\mathbf{A} = \langle X \cup \{e\}, \cdot \rangle$ where $e \notin X$ and $x \cdot y = x$ if $\langle x, y \rangle \in R$ or $x = y$, and $= e$ otherwise. Show that $\mathbf{A}$ belongs to the variety generated by $\mathbf{S}_4$

(from the last exercise). Show that $\mathbf{A}$ is simple iff $X \neq \emptyset$, R is connected on X, and for every $x \neq y$ in X there is $z \in X$ such that $\langle x, z\rangle \in R \leftrightarrow \langle y, z\rangle \notin R$.

(6) By Theorems 14.3 and 14.8, the algebras $\mathbf{S}_n$ of the last Exercise must be of type **5**. By Theorem 13.6, they must be "orderable". Verify both of these properties; and find the minimal, non-trivial, admissible orderings of $\mathbf{S}_n$.

(7) Let $\mathbf{A}$ be an algebra with congruences α, β, γ and δ, where α and δ permute. Suppose that $I[\alpha, \beta]$ projects down to $I[\gamma, \delta]$ (i.e., $\alpha \wedge \delta = \gamma$ and $\alpha \vee \delta = \beta$). Prove that $\sharp(\beta/\alpha) = \sharp(\delta/\gamma)$.

PROBLEMS

1. Is it true that if $\mathbf{A}$ is an Abelian algebra and there is an equation in the language of lattices that is valid in the congruence lattice of every algebra in $\boldsymbol{V}(\mathbf{A})$, and fails to be valid in some lattice, then $\mathbf{A}$ must be polynomially equivalent to a module? (Yes, if $\boldsymbol{V}(\mathbf{A})$ is locally finite.)

2. A variety $\mathcal{V}$ is called Abelian iff all its algebras are Abelian, and Hamiltonian iff every subalgebra of an algebra $\mathbf{A}$ in $\mathcal{V}$ is a full equivalence class of a congruence on $\mathbf{A}$. Is every locally finite Abelian variety Hamiltonian? (It is known that every Hamiltonian variety is Abelian.)

3. If $\mathbf{A}$ is a finite Abelian algebra of finite type, is $\boldsymbol{V}(\mathbf{A})$ finitely axiomatizable?

4. Let $\mathbf{A}$ be a finite algebra with congruence lattice $\mathbf{L}$. Suppose that $\mathbf{L}$ has an $\mathbf{M}_n$ ($n \geq 3$) as a sublattice in which the 0 and 1 are the same as in $\mathbf{L}$. Is $\mathbf{A}$ Abelian? [This problem has been solved by Ross Willard at the University of Waterloo, Ontario. The answer is "not necessarily".]

5. If $\mathbf{A}$ is a finite algebra, must there exist an integer n such that if θ is a minimal congruence in an algebra of $\boldsymbol{V}(\mathbf{A})$, and if θ is Abelian but not strongly Abelian, then every θ-equivalence class has at most n elements?

6. Suppose that $\mathbf{L}$ is a finitely projective finite lattice. Does there exist a (locally finite) variety $\mathcal{W}$ with the property that for every locally finite variety $\mathcal{V}$ we have: $\mathcal{V}$ satisfies some idempotent Mal'cev condition not satisfied by $\mathcal{W}$ iff $\mathbf{L}$ is not isomorphic to a sublattice of the congruence lattice of any algebra in $\mathcal{V}$? (If congruence modularity turns out to be a "prime" Mal'cev condition, then this is true for $\mathbf{L} = \mathbf{N}_5$, although it may be that the variety $\mathcal{W}$ cannot be locally finite.)

7. Let $\mathbf{L}$ be the congruence lattice of a finite algebra. Find interesting conditions under which the maximal intervals in $\mathbf{L}$ that omit type **4** are the equivalence classes of a congruence on $\mathbf{L}$. (Consider, for instance, these conditions: (1) The algebra belongs to a variety that omits types **1** and **5**. (2) The algebra belongs to a variety in which type **4** minimal sets have empty tails.)

8. Investigate minimal tolerances in finite algebras.

9. Apply tame congruence theory to the study of minimal locally finite varieties. (Note that the finite free algebras in these varieties, when all endomorphisms are adjoined as operations, become simple algebras.)

10. Describe all finite simple algebras that generate minimal varieties and possess no nontrivial subalgebras.

11. Prove or disprove: If $\mathbf{A}$ is a finite algebra such that $\boldsymbol{V}(\mathbf{A})$ admits no finite bound for the cardinals of its simple algebras, then this class of cardinals is not bounded by any cardinal.

12. The same problem as the above, for subdirectly irreducible algebras in place of simple algebras.

13. Does there exist a locally finite variety that omits types **1** and **5** and whose class of congruence lattices obeys no nontrivial lattice equation?

14. Prove or disprove: If $\mathcal{V}$ is a locally finite variety, the class of congruence lattices of algebras in $\mathcal{V}$ obeys some nontrivial lattice equation iff $\mathcal{V}$ omits types **1** and **5**, and also the type **4** minimal sets in $\mathcal{V}$ have empty tails.

15. Investigate $\langle 0, \alpha \rangle$-minimal sets for Abelian minimal congruences α of finite groups. Do the same for rings.

16. Let $\mathbf{A}$ be an E-minimal algebra with congruence lattice $\mathbf{L}$. Is it true that $\mathbf{L}$ obeys every lattice equation that holds in all subgroup lattices of finite Abelian groups? The question is open for finite groups in place of E-minimal algebras, and more generally, it is open for finite algebras in congruence-modular varieties. (If the answer is yes for E-minimal algebras, then the other questions have positive answers.) Concerning this question for finite groups, see Exercise 8.8 (4).

17. Explain why it happens that Mal'cev properties involving congruences almost invariably are expressible with operations of just three variables.

An appendix added in July, 1996

In this second printing of this book, the bibliography has been expanded to include fifty-one new items, numbered [35]-[85]. With only a few exceptions, each of these papers applies, or extends, the theory presented in this book, or makes a contribution toward the solution of one of the open problems listed on the preceeding pages. Many of the papers manage to extend results of this book, in some fashion, to algebras and varieties that are not assumed to be locally finite. What follows is a brief commentary on some of these papers.

Among the seventeen open problems listed on the preceeding pages, Problems 1, 2, 3, 4, 9, 10, 11, 12, 14 and 16 have now been solved.

Problem 1 was solved by K. Kearnes and Á. Szendrei [57]. They proved that every Abelian algebra in a variety which satisfies some idempotent Maltsev condition that fails to hold in the variety of semilattices, is an affine algebra.

Problem 2 asked if every locally finite variety of Abelian algebras is Hamiltonian. E. W. Kiss and M. Valeriote [60] have shown that this is indeed the case, and the result has been extended in [54] and [64]. Very recently, K. Kearnes and R. Willard (unpublished) have shown that every locally finite variety of Abelian algebras is generated by one finite algebra and they produced a negative answer to Problem 3.

Problem 4 was solved by R. Willard [83]. He constructed, for every $n > 2$, a finite, non-Abelian algebra $\mathbf{A}_n$ having a copy of $\mathbf{M}_n$ as a $\{0,1\}$-sublattice of its congruence lattice. He proved also that if **Con A** contains a $\{0,1\}$-sublattice isomorphic to $\mathbf{M}_n$ where $n > 2$ and if $\mathbf{A}$ belongs to a variety that omits type **1** then $\mathbf{A}$ is Abelian. K. Kearnes [50] improved the latter result. He proved that if $\mathbf{A}$ is a finite algebra and **Con A** contains a $\{0,1\}$-sublattice isomorphic to $\mathbf{M}_n$ where $n > 2$ then $\mathbf{A}$ is left-nilpotent; and if in addition, $\mathbf{A}$ omits type **1**, then $\mathbf{A}$ is Abelian.

Problems 9 and 10 have been largely solved, through the combined efforts of K. Kearnes, E. W. Kiss, Á. Szendrei and M. Valeriote. These problems basically ask for a characterization or classification of all minimal locally finite varieties via the classification of the strictly simple algebras that generate them. (An algebra is "strictly simple" if it is finite, simple, and has no subalgbras besides itself and possibly some one-element subalgebras.) K. Kearnes, Á. Szendrei [56] contains this result: A strictly simple algebra generates a minimal variety iff it is either non-Abelian or has a one-element subalgebra, and in addition, satisfies a certain Maltsev condition. Their result leaves room for improvement but, for Abelian algebras, it refines to the following: A strictly simple algebra of type **1** generates a minimal variety iff it is term-equivalent to a matrix power of a two-element algebra with no operations except possibly one constant; a strictly simple algebra of type **2** generates a minimal variety iff it has a one-element subalgebra and is polynomially equivalent to a cyclic module over a finite simple ring with unit.

In Á. Szendrei's papers [73]–[76] can be found results determining all the finite strictly simple algebras whose operations are idempotent, all the finite simple Abelian algebras whose basic operations are surjective, all the finite simple algebras having just one basic operation, and all the finite term-minimal algebras.

Problem 12 was solved by R. McKenzie [66]. He exhibited varieties, each of them generated by a four-element algebra, which are precisely residually $< \lambda$ where λ is any finite cardinal > 4, or any of ω, ω_1, $(2^\omega)^+$. M. Valeriote [82] adapted

the constructions of [66] to produce an eight-element algebra of finite type which generates a semi-simple variety whose largest simple (or equivalently, subdirectly irreducible) algebra is denumerably infinite. This solved Problem 11.

Problem 14 was solved by M. Valeriote in collaboration with K. Kearnes (unpublished). They disproved the statement by exhibiting a counter-example which is a reduct of Polin's variety.

Problem 16 was solved by P. P. Pálfy and Cs. Szabo [71]. They exhibited an equation which is valid in the lattice of subgroups of every Abelian group, but is not valid in the lattice of normal subgroups of a certain finite group of order 2^{10}. The equation has eight variables and the group that falsifies it is the free group on five generators in the variety generated by the eight-element quaternion group.

J. Berman [39] shows that, where $\mathbf{A}$ is any finite simple algebra, the system of cardinalities of the free algebras in $V(\mathbf{A})$ almost determines the type of $\mathbf{A}$.

How difficult is it to determine the type set of a finite algebra $\mathbf{A}$, or of the variety generated by $\mathbf{A}$? These questions are addressed in [37], [42] and [70]. R. McKenzie [70] proved that there is no algorithm (that could be expressed by a recursive function) to determine if the Boolean type appears in the type-set of $V(\mathbf{A})$, where $\mathbf{A}$ is an arbitrary finite algebra of finite similarity type. This result—as well as other undecidability results for finite algebras appearing in [67] – [70], [84] and [85] and proved by the same method—was a serendipitous byproduct of the resolution of Problem 12. Tame-congruence theoretic ideas lie behind these discoveries, although the results and their proofs do not easily reveal that fact.

The papers [38], [46] and [77] contain an alternative development of tame congruence theory based on "subtraces". Those papers and [61] provide shorter routes to many of the results in Chapters 4, 5 and 6.

Theorem 9.19 in this book has been generalized by P. Lipparini [63]. He proved that for each integer $n \geq 2$, any variety with n-permuting congruences is congruence-ε for some nontrivial lattice equation ε. The open problem in Exercise 8.8.1 has been solved by M. Valeriote and R. Willard [81]. They proved that a locally finite variety has permuting congruences iff its finite algebras satisfy the conditions (i) and (ii) of the exercise. K. Kearnes [49] found a tame-congruence theoretic criterion for a locally finite variety to have 3-permuting congruences and indicated that in a certain sense, no such criterion can exist for n-permuting congruences for any fixed $n > 3$.

Theorem 7.7 in this book has been strengthened by R. Freese, J. B. Nation and K. Kearnes [40]. They proved that for any finite algebra $\mathbf{A}$, the lattice $(\mathbf{Con}\,\mathbf{A})/\overset{s}{\sim}$ is an upper-bounded homomorphic image of a free lattice.

Our theory has become the essential tool for the investigation of decidable locally finite varieties and quasi-varieties. R. McKenzie, M. Valeriote [65] proved that every decidable locally finite variety decomposes as the varietal product of three very special decidable varieties: $\mathcal{S}$, a variety of strongly Abelian algebras; $\mathcal{A}$, an affine variety; and $\mathcal{D}$, a discriminator variety. This result was a precursor to a beautiful result of B. Hart, S. Starchenko, M. Valeriote [41] according to which any variety of countable type that has fewer than continuum many non-isomorphic countable members decomposes as the varietal product of a strongly Abelian and an affine variety. Following the path pioneered in [65], several researchers are currently studying the characteristic algebraic properties of locally finite varieties for which the theory of their finite members is decidable. Current work in this area is represented by the papers [43], [44], [45], [80].

Several commutator theories for varieties that are not assumed to be congruence modular have been studied in [52], [53], [57] and [62] and some impressive results have been obtained.

BIBLIOGRAPHY

1. Ágoston, I., Demetrovics, L. and Hannák, L., *On the number of clones containing all constants*, in "Lectures in Universal Algebra", Coll. Math. Soc. János Bolyai, No. 43, 1983.
2. Berman, J., *Varieties with log-linear free spectra*, (preprint).
3. Berman, J. and McKenzie, R., *Clones satisfying the term condition*, Discrete Math. **52** (1984), 7–29.
4. Burris, S. and Sankappanavar, H.P., "A Course in Universal Algebra," Springer Graduate Texts in Mathematics, 1981.
5. Burris, S. and McKenzie, R., "Decidability and Boolean representations," Amer. Math. Soc. Memoirs No. 246, 1981.
6. Czedli, G., *A Mal'cev type characterization for the semi-distributivity of congruence lattices*, Acta Sci. Math. **43** (1981), 267–272.
7. _____, *A characterization of congruence semi-distributivity*, in "Universal Algebra and Lattice Theory", Springer Lecture Notes No. 1004, 1983.
8. Davey, B.A. and Sands, B., *An application of Whitman's condition to lattices with no infinite chains*, Algebra Universalis **7** (1977), 171–178.
9. Day, A. and Freese, R., *A characterization of identities implying congruence modularity. I*, Canadian J. Math **32** (1980), 1140–1167.
10. Freese, R. and McKenzie, R., *Residually small varieties with modular congruence lattices*, Trans. Amer. Math. Soc. **246** (1981), 419–430.
11. _____, "Commutator theory for congruence modular varieties," London Math. Soc. Lecture Note No. 125, 1987.
12. Freese, R. and Nation, J.B., *Congruence lattices of semilattices*, Pacific J. Math. **49** (1973), 51–58.
13. Garcia, O.C. and Taylor, W., "The lattice of interpretability types of varieties," Amer. Math. Soc. Memoirs No. 305, 1984.
14. Grätzer, G., "Universal Algebra," Springer (2nd Edition), 1979.
15. _____, "General Lattice Theory," Academic Press, 1978.
16. Gumm, H.P., "Geometrical methods in congruence modular algebras," Amer. Math. Soc. Memoirs No. 286, 1983.
17. Hagemann, J. and Mitschke, A., *On n-permutable congruences*, Algebra Universalis **3** (1973), 8–12.

18. Hobby, D., *Congruence lattices of finite algebras*, Algebra Universalis **23** (1986), 44–57.
19. Jónsson, B., *Algebras whose congruence lattices are distributive*, Math. Scand. **21** (1967), 110–121.
20. Jónsson, B. and Rival, I., *Lattice varieties covering the smallest non-modular variety*, Pacific J. Math. **82** (1979), 463–478.
21. Lavrov, I.A., *Effective inseparability of the sets of identically true formulae and finitely refutable formulae for certain elementary theories*, Algebra i Logika, Seminar 2, Vol. 1 (1963), 5–18.
22. McKenzie, R., *Finite forbidden lattices*, in "Universal Algebra and Lattice Theory", Springer Lecture Notes No. 1004, 1983.
23. ———, *Residually small varieties of semigroups*, Algebra Universalis **13** (1981), 171–201.
24. Nation, J.B., *Finite sublattices of a free lattice*, Trans. Amer. Math. Soc. **269** (1982), 311–337.
25. Neumann, H., "Varieties of Groups," Ergebnisse der Math. und ihrer Grenzgebiete, ns. 37, Springer–Verlag, 1967.
26. Pálfy, P.P., *Unary polynomials in algebras I*, Algebra Universalis **18** (1984), 262–273.
27. Pálfy, P.P. and Pudlák, P., *Congruence lattices of finite algebras and intervals in subgroup lattices of finite groups*, Algebra Universalis **11** (1980), 22–27.
28. Pixley, A., *Local Mal'cev conditions*, Canad. Math. Bull. **15** (1972), 559–568.
29. Post, E.L., "The two-valued iterative systems of mathematical logic," Annals of Math. Studies No. 5, Princeton University Press, 1941.
30. Pudlák, P. and Tuma, J., *Every finite lattice can be embedded into a finite partition lattice*, Algebra Universalis **10** (1980), 74–95.
31. Salomaa, A., *On essential variables of functions, especially in the algebra of logic*, Ann. Acad. Sci. Fenn. Ser. AI, No. 339, 1963.
32. Taylor, W., *Varieties obeying homotopy laws*, Canadian J. Math. **29** (1977), 498–527.
33. Wille, R., "Kongruenzklassengeometrien," Springer Lecture Notes No. 113, 1970.
34. Zamyatin, A.P., *A non-Abelian variety of groups has an undecidable elementary theory*, Algebra and Logic **17** (1978), 13–17.

ADDED IN JULY, 1996

35. P. Agliano, K. Kearnes, *Congruence semimodular varieties I: locally finite varieties*, Algebra Universalis **32** (1994), 224-269.

36. P. Agliano, K. Kearnes, *Congruence semimodular varieties II: regular varieties*, Algebra Universalis **32** (1994), 270–296.

37. J. Berman, E.W. Kiss, P. Pröhle, Á. Szendrei, *The set of types of a finitely generated variety*, Discrete Math. **112** (1993), 1–20.

38. J. Berman, S. Seif, *An approach to tame congruence theory via subtraces*, Algebra Universalis **30** (1993), 479–520.

39. J. Berman, *Free spectra gaps and tame congruence types*, International Journal of Algebra and Computation **5** (1995), 651–672.

40. R. Freese, J.B. Nation, K. Kearnes, *Congruence lattices of congruence semidistributive algebras*, in: Lattice Theory and its Applications, Heldermann Verlag Berlin, 1995, pp. 63–78.

41. B. Hart, S. Starchenko, M. Valeriote, *Vaught's conjecture for varieties*, Trans. Amer. Math. Soc. **342** (1994), 173–196.

42. D. Hobby, *Finding type sets is NP-hard*, International Journal of Algebra and Computation **1** (1991), 437–444.

43. P. Idziak, *A characterization of finitely decidable congruence modular varieties*, Transactions Amer. Math. Soc. (to appear).

44. P. Idziak, M. Valeriote, *A property of the solvable radical in finitely decidable varieties*, (manuscript, 1992).

45. J. Jeong, *Type* **2** *subdirectly irreducible algebras in finitely decidable varieties*, (manuscript, 1991).

46. P. M. Johnson, S. Seif, *Generalizations of tame congruence theory*, (manuscript, 1992).

47. K. Kearnes, *Type preservation in locally finite varieties with the CEP*, Canadian Journal of Mathematics **43** (1991), 748–769.

48. K. Kearnes, *Congruence lower semimodularity and 2-finiteness imply congruence modularity*, Algebra Universalis **28** (1991), 1–11.

49. K. Kearnes, *Congruence permutability and congruence 3-permutability in locally finite varieties*, Journal of Algebra **156** (1993), 36-49.

50. K. Kearnes, *An order-theoretic property of the commutator*, International Journal of Algebra and Computation **3** (1993), 491–533.

51. K. Kearnes, *Idempotent simple algebras*, in: Logic and Algebra, Proc. of the Magari Memorial Conference, Siena, 1994, Marcel Dekker, New York.

52. K. Kearnes, *Varieties with a difference term*, Journal of Algebra **177** (1995), 926–960.

53. K. Kearnes, *A quasi-affine representation*, International Journal of Algebra and Computation **5** (1995), 673–702.

54. K. Kearnes, *A Hamiltonian property for nilpotent algebras*, Algebra Universalis (to appear).

55. K. Kearnes, E. W. Kiss, M. Valeriote, *Minimal sets and varieties*, Transactions Amer. Math. Soc. (to appear).

56. K. Kearnes, Á. Szendrei, *A characterization of minimal locally finite varieties*, Trans. Amer. Math. Soc. (to appear).

57. K. Kearnes, Á. Szendrei, *The relationship between two commutators*, (manuscript, 1996).

58. K. Kearnes, R. Willard, *Inherently nonfinitely based solvable algebras*, Canad. Math. Bull. **37** (1994), 514–521.

59. E.W. Kiss, P. Pröhle, *Problems and results in tame congruence theory. A survey of the '88 Budapest Workshop*, Algebra Universalis **29** (1992), 151–171.

60. E.W. Kiss, M. Valeriote, *Abelian algebras and the Hamiltonian property*, Journal of Pure and Applied Algebra **87** (1993), 37–49.

61. E.W. Kiss, *An easy way to minimal algebras*, International Journal of Algebra and Computation (to appear).

62. P. Lipparini, *Commutator theory without join-distributivity*, Transactions Amer. Math. Soc. (to appear).

63. P. Lipparini, *n-permutable varieties satisfy non-trivial congruence identities*, Algebra Universalis **33** (1995), 159–168.

64. R. McKenzie, *Congruence extension, Hamiltonian and Abelian properties in locally finite varieties*, Algebra Universalis **28** (1991), 589–603.

65. R. McKenzie, M. Valeriote, *The Structure of Decidable Locally Finite Varieties* , Birkhauser, Progress in Mathematics, Vol. 79, 1989.

66. R. McKenzie, *The residual bounds of finite algebras*, International Journal of Algebra and Computation **6** (1996), 1–28.

67. R. McKenzie, *The residual bound of a finite algebra is not computable*, International Journal of Algebra and Computation **6** (1996), 29–48.

68. R. McKenzie, *Tarski's finite basis problem is undecidable*, International Journal of Algebra and Computation **6** (1996), 49–104.

69. R. McKenzie, *Recursive inseparability for residual bounds of finite algebras*, (manuscript, 1995).

70. R. McKenzie, *The type-set of a variety is not computable*, (manuscript, 1995).

71. P.P. Pálfy, Cs. Szabo, *An identity for subgroup lattices of Abelian groups*, Algebra Universalis **33** (1995), 191–195.

72. R. W. Quackenbush, *Quasi-affine algebras*, Algebra Universalis **20** (1985), 318–327.

73. Á. Szendrei, *Every idempotent plain algebra generates a minimal variety*, J. Australian Math. Soc. **25** (1988), 36–39.

74. Á. Szendrei, *Simple surjective algebras having no proper subalgebras*, J. Australian Math. Soc. **48** (1990), 434–454.

75. Á. Szendrei, *A survey on strictly simple algebras and minimal varieties*, in: Universal Algebra and Quasigroup Theory, A. Romanowska and J.D.H Smith (eds.), Heldermann Verlag Berlin, 1992, pp. 209–239.

76. Á. Szendrei, *Term minimal algebras*, Algebra Universalis **32** (1994), 439–477.

77. S. Seif, *Congruence lattices of algebras —the signed labelling*, Proc. Amer. Math. Soc. **124** (1996).

78. S. Seif, *Tame congruence theory on semigroups through the J labelling*, Semigroup Forum (to appear).

79. S. Seif, *Congruence Semimodular and Congruence Jordan-Dedekind Chain Condition Algebras Characterized*, (manuscript, 1992).

80. M. Valeriote, R. Willard, *Some properties of finitely decidable varieties*, International Journal of Algebra and Computation **2** (1992), 89–101.

81. M. Valeriote, R. Willard, *A characterization of locally finite congruence permutable varieties*, J. Algebra **140** (1991), 362–369.

82. M. Valeriote, *A residually small, finitely generated, semi-simple variety which is not residually finite*, International Journal of Algebra and Computation (to appear).

83. R. Willard, $\mathbf{M}_n$ *as a* $\{0,1\}$*-sublattice of* $\mathbf{Con}\,\mathbf{A}$ *does not force the term condition*, Proc. Amer. Math. Soc. **104** (1988), 349–356.

84. R. Willard, *Tarski's finite basis problem via* $\mathbf{A}(T)$, Trans. Amer. Math. Soc. (to appear).

85. R. Willard, *Determining whether* $V(\mathbf{A})$ *has a model-companion is undecidable*, (manuscript, 1995).

INDEX OF TERMS

INDEX OF NOTATION

$f^k_{(i)}$	f iterated k times on its $i+1$-st variable, 46
f_α	operation on A/α corresponding to f, 8
$f(\alpha)$	$\{\langle f(x), f(y)\rangle : \langle x, y\rangle \in \alpha\}$, 25
$f\|_U$	f restricted to U^n (f is n-ary), 26
$f\|_{(U_0\times\cdots\times U_{n-1})}$	f restricted to $U_0 \times \cdots \times U_{n-1}$, 26
$f : B \simeq C$	f is a polynomial isomorphism between B and C, 28
$f : \mathbf{A} \to \mathbf{B}$	f is a homomorphism from $\mathbf{A}$ into $\mathbf{B}$, 7
$f : \mathbf{A} \twoheadrightarrow \mathbf{B}$	f is a homomorphism from $\mathbf{A}$ onto $\mathbf{B}$
$f : \mathbf{L} \overset{0,1-\mathrm{sep}}{\longrightarrow} \mathbf{L}'$	f is a 0, 1-separating homomorphism, 20
$\mathbf{F}_L(X)$	L-free algebra generated by X, 12
$\mathbf{F}_\mathcal{K}(X)$	free algebra for $\mathcal{K}$ generated by X, 13
$\mathbf{F}_\mathcal{V}(k)$	$\mathcal{V}$-free algebra on k generators, 14
$\mathbf{GF}(q)$	finite (Galois) field with q elements, 173
$\boldsymbol{H}\mathcal{K}$	class of homomorphic images of algebras in $\mathcal{K}$, 13
$I[a, b]$	interval sublattice, 11
id_A	identity function on A, 8
$\mathcal{K}_{fin}$	class of finite members of $\mathcal{K}$, 100
$\mathcal{K}_1/\mathcal{K}_0$	(e.g., SD($\wedge$)/$\mathcal{M}odular$), 117
$\ker \pi$	kernel of π, 9
$\mathrm{M}_\mathbf{A}(\alpha, \beta)$	set of $\langle\alpha, \beta\rangle$-minimal sets, 28
$\mathrm{M}(\mathbf{A})$	$\mathrm{M}_\mathbf{A}(0_A, 1_A)$, 168
$\mathbf{M}_n$	projective line with n points (a lattice), 21
$\mathbf{M}_{3,3}$	an eight-element lattice, 21
$\mathrm{Mod}(\Sigma)$	class of models of a set Σ of equations, 13
$\mathbf{N}_5$	smallest non-modular lattice, 9, 10
p^n_i	$i+1$-st n-ary projection, 6
$\boldsymbol{P}\mathcal{K}$	class of products of members of $\mathcal{K}$, 13
$\boldsymbol{P}_{fin}\mathcal{K}$	class of finite products of members of $\mathcal{K}$, 14
$\mathrm{Pol}\,\mathbf{A}$	clone of polynomial operations of $\mathbf{A}$, 6
$\mathrm{Pol}_n\mathbf{A}$	set of n-ary members of Pol $\mathbf{A}$, 6
$(\mathrm{Pol}\,\mathbf{A})\|_U$	clone of derived polynomial operations on U, 6, 26

Department of Mathematics
State University of New York
New Paltz, New York 12561

Department of Mathematics
University of California
Berkeley, California 94720