Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

1004

Universal Algebra and Lattice Theory

Proceedings of the Fourth International Conference
Held at Puebla, Mexico, 1982

Edited by R. S. Freese and O. C. Garcia

Springer-Verlag
Berlin Heidelberg New York Tokyo 1983

Editors

Ralph S. Freese
University of Hawaii at Manoa, Department of Mathematics
2565 The Mall, Honolulu, Hawai 96822, USA

Octavio C. Garcia
Instituto de Matemáticas-UNAM
Area de la Investigación Científica Circuito Exterior
Cd. Universitaria Mexico 20, D.F. México

AMS Subject Classifications (1980): 06C05, 06D05, 06F15, 08A05, 08A40, 08B05, 08B15, 08B20

ISBN 3-540-12329-6 Springer-Verlag Berlin Heidelberg New York Tokyo
ISBN 0-387-12329-6 Springer-Verlag New York Heidelberg Berlin Tokyo

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2146/3140-543210

FOREWORD

These Proceedings contain papers based on lectures given at the Fourth International Conference on Universal Algebra and Lattice Theory held January 11-22, 1982 in Puebla, Mexico. This volume offers the reader a good sample of the recent advances and current trends in this active field.

We would like to thank the authors for contributing very high quality papers and the referees for their careful job on each paper. We would also like to acknowledge the support of the Instituto de Mathemáticas de la Universidad Nacional Autónoma de Mexico and the Instituto de Ciencias de la Universidad Autónoma de Puebla. We wish to thank the organizing committee: Bernhard Banachewski, Octavio C. Garcia, Ralph McKenzie, George McNulty, Don Pigozzi, and Walter Taylor, and the local organizing committee: Raymundo Bautista, Humberto Cardenas, Octavio C. Garcia, Emilio Lluis, and Jose Antonio de la Peña. We would especially like to thank Ms. Lourdes Arceo for her continuous help and Springer-Verlag for its help in publishing these Proceedings.

Ralph Freese
Honolulu

Octavio C. Garcia
Mexico, D.F.

TABLE OF CONTENTS

THE AMALGAMATION CLASS OF A DISCRIMINATOR VARIETY IS FINITELY AXIOMATIZABLE

Clifford Bergman

Discriminator varieties have been extensively studied since their introduction by Pixley in 1970. Among their attributes, discriminator varieties exhibit a strong relationship between the quantifier-free formulas and certain terms in the language of the variety. This paper exploits that relationship in order to prove that some important classes of algebras, generally defined using algebraic properties, can be described by a finite set of first-order sentences.

If K is a class of algebras, define $Ps(K)$ to be the class of all algebras isomorphic to a subdirect product of members of K. An algebra A of K is an *amalgamation base* of K if, for every $B_0, B_1 \in K$ and α_0, α_1 embedding A into B_0 and B_1 respectively, there is an algebra C of K and embeddings β_0 of B_0 into C and β_1 of B_1 into C such that $\beta_1 \circ \alpha_1 = \beta_0 \circ \alpha_0$. The collection of all amalgamation bases is called the *amalgamation class*, $AMAL(K)$.

Let V be a finitely generated discriminator variety of finite type. In this paper, the following classes will be shown to be finitely axiomatizable:

(i) $Ps(S)$, where S is a set of simple algebras of V

(ii) $AMAL(V)$.

These results are taken from the author's doctoral thesis written under Ralph McKenzie. The author is greatly indebted to him for his guidance and suggestion of this problem.

Notation. For a class K of algebras, K_{SI} denotes the class of subdirectly irreducible algebras of K. Terms in the language of K will be denoted by lower case Greek letters. If α is a term and $A \in K$ then α^A denotes the term function of A corresponding to α. For convenience, the sequence of letters $x_0, x_1, \ldots, x_{n-1}$ will often be abbreviated $\overline{x}$.

The lattice of congruences of an algebra A is denoted by $\mathrm{Con}(A)$ and has smallest element Δ and largest element ∇. If B is a subalgebra of A and $\Theta \in \mathrm{Con}(A)$, then $\Theta|B$ denotes the congruence $\Theta \cap B^2$ of B. For definitions and basic facts not explained here, the reader can consult [2] or [3].

DEFINITION 1. A variety V is a *discriminator variety* if there is a term $\sigma(x,y,z)$ in the language of V (called the *discriminator term*) such that an algebra $A \in V$ is subdirectly irreducible or trivial if and only if $A \models (\sigma(x,x,z) \approx z \wedge x \not\approx y \rightarrow \sigma(x,y,z) \approx x)$.

In [6] Pixley showed that a finitely generated variety is a discriminator variety if and only if it is arithmetical and every subalgebra of a subdirectly irreducible algebra is either simple or trivial.

Suppose $(A_i : i \in I)$ is a family of algebras and D is an ultrafitler on the set I. Then D induces a congruence (also denoted D) on $\Pi(A_i : i \in I)$ by: $a \equiv b(D)$ if and only if $\{i \in I : a_i = b_i\} \in D$.

To build a set of sentences describing $Ps(S)$, we first need sentences to insure that the discriminator term has the desired properties. These were discovered by R. McKenzie [5].

THEOREM 2. *Let* $\underline{L}$ *be a first-order language with no non-logical relation symbols and with function symbols* $\{f_i : i < k\}$, k *a cardinal. Suppose* $\sigma(x,y,z)$ *is a term of* $\underline{L}$ *and let* Σ *be the set consisting of the following identities:*

(e0) $\sigma(x,x,y) \approx y$

(e1) $\sigma(x,y,x) \approx x$

(e2) $\sigma(x,y,y) \approx x$

(e3) $\sigma(x,\sigma(x,y,z),y) \approx y$

(e4)$_i$ $\sigma(x,y,f_i(v_0,v_1,\ldots,v_{n_i-1})) \approx \sigma(x,y,f_i[\sigma(x,y,v_0),\ldots,\sigma(x,y,v_{n_i-1})])$

for $i < k$, *where* f_i *is* n_i*-ary.*

(1) *The variety* V *determined by the equations* Σ *is a discriminator variety with discriminator term* σ.

(2) *Every finite algebra of* V *is a direct product of simple algebras.*

(3) *For every* $A \in V$ *and* $a,b \in A$, *the binary relation*

$$\Theta(a,b) = \{(x,y) \in A^2 : \sigma^A(a,b,x) = \sigma^A(a,b,y)\}$$

is the smallest congruence of A *containing* (a,b).

(4) *For every quantifier free formula* ϕ *of* $\underline{L}$ *there are terms* α *and* β *of* $\underline{L}$ *such that for every* $B \in V_{SI}$ *and* $b_0,\ldots,b_{m-1} \in B$, $B \models \phi(\overline{b}) \leftrightarrow (\exists y)\alpha(\overline{b},y) \not\approx \beta(\overline{b},y)$.

COROLLARY 3. *Let* V *be a discriminator variety with discriminator term* σ. *Then the equations of* Σ *hold in* V. *Let* ϕ, α *and* β *be as in theorem 2(4). For any* $A \in V$ *and* $a_0,\ldots,a_{m-1} \in A$, *the following are equivalent:*

(i) there exists a coatom Ψ *of* Con(A) *such that*

$$A/\Psi \models \phi(a_0/\Psi,\ldots,a_{m-1}/\Psi)$$

(ii) $A \models (\exists y)\alpha(a_0,\ldots,a_{m-1},y) \not\approx \beta(a_0,\ldots,a_{m-1},y)$.

Proof. Let $A \in V$ and suppose (i) holds. Take $B = A/\Psi$ and $b_i = a_i/\Psi$ for $i < m$. Then $B \models \phi(b_0,\ldots,b_{m-1})$ implies by theorem 2 that there is $z \in B$ with $\alpha^B(b_0,\ldots,b_{m-1},z) \neq \beta^B(b_0,\ldots,b_{m-1},z)$. Choose $y \in A$ with $y/\Psi = z$. Since $\alpha^A(\overline{a},y)/\Psi = \alpha^B(\overline{b},z) \neq \beta^B(\overline{b},z) = \alpha^B(\overline{a},y)/\Psi$ we conclude (ii).

Conversely, if α and β disagree for some $y \in A$, then they are separated by a completely meet-irreducible congruence Ψ. By semi-simplicity, $B = A/\Psi$ is simple, and we reverse the implication above to derive (i).

For the remainder of this paper, suppose V is a finitely generated discriminator of finite type, that is the language of V has only finitely many basic operation and constant symbols. If B is a finite structure of this language, then there is a quantifier-free formula $Dg_B(x_0,\ldots,x_{n-1})$ (the "diagram of B") such that, for every structure A and $a_0,\ldots,a_{n-1} \in A$, $A \models Dg_B(\overline{a})$ if and only if $\{a_0,\ldots,a_{n-1}\}$ is the universe of a subalgebra of A isomorphic to B. Applying the corollary to this formula, we obtain terms α and β such that there are elements $a_0,\ldots,a_{n-1},b$ of A with $\alpha^A(\overline{a},b) \neq \beta^A(\overline{a},b)$ if and only if, for some coatom Ψ of Con(A), A/Ψ contains a copy of B as a subalgebra. What is more surprising, we can strengthen the inequation in such a way that A/Ψ will be isomorphic to B.

THEOREM 4. *Let* V *be a finitely generated discriminator variety of finite type. Let* $S \subseteq V_{SI}$. *Then* Ps(S) *is a finitely axiomatizable class.*

<u>Proof</u>. Since V is finitely generated, we may assume that S is a finite set of finite algebras, $S = \{L_0,\dots,L_{m-1}\}$. Since the language is of finite type, the set Σ of theorem 2 is finite. Informally, we need to add to Σ a sentence saying that for any pair of distinct elements c and d, there is a completely meet-irreducible congruence Ψ separating c and d so that the quotient algebra modulo Ψ is isomorphic to one of the L_j's.

Fix $j < m$. Let $L = L_j$ and $r = \mathrm{card}(L)$. By corollary 3, there are terms α and β such that for every $A \models \Sigma$ and $a_0,\dots,a_{r-1},c,d \in A$:

$$A \models (\exists y)\alpha(\overline{a},y,c,d) \not\approx \beta(\overline{a},y,c,d)$$

if and only if there is a coatom Ψ of $\mathrm{Con}(A)$ such that:

$$A/\Psi \models c/\psi \not\approx d/\Psi \wedge \mathrm{Dg}_L(a_0/\Psi,\dots,a_{r-1}/\Psi).$$

Now define the formula $\mathrm{Sep}_L(u,v)$ to be:

$$(\exists x_0,\dots,x_{r-1})(\exists y)(\forall z)[\alpha(\overline{x},y,u,v) \not\approx \beta(\overline{x},y,u,v) \wedge \bigvee_{i<r}(\sigma(x_i,z,\alpha(\overline{x},y,u,v)) \not\approx \sigma(x_i,z,\beta(\overline{x},y,u,v)))].$$

The key claim is that for any $A \models \Sigma$ and $c,d \in A$, $A \models \mathrm{Sep}_L(c,d)$ if and only if there is a coatom Ψ of $\mathrm{Con}(A)$ such that $c/\Psi \neq d/\Psi$ and $A/\Psi \cong L$. Once this is established, the members of Σ together with the sentence:

$$(\forall u)(\forall v)(u \not\approx v \rightarrow \bigvee_{j<m} \mathrm{Sep}_{L_j}(u,v))$$

will axiomatize $\mathrm{Ps}(S)$.

Suppose first that for $c,d \in A$, there is $\Psi \in \mathrm{Con}(A)$ such that $c/\Psi \neq d/\Psi$ and $A/\Psi \cong L$. Then A/Ψ satisfies Dg_L for some elements $g_0,\dots,g_{r-1}$. Choosing a_i in A to represent g_i modulo Ψ, there is a $b \in A$ such that $\alpha^A(\overline{a},b,c,d) \neq \beta^A(\overline{a},b,c,d)$. Now let e be any element of A. Since $A/\Psi = \{g_0,\dots,g_{r-1}\}$, there is $i < r$ such that $e \equiv a_i(\mathrm{mod}\,\Psi)$. For this i we clearly have $\sigma^A(a_i,e,\alpha^A(\overline{a},b,c,d)) \neq \sigma^A(a_i,e,\beta^A(\overline{a},b,c,d))$ since they are incongruent modulo Ψ. Thus A satisfies $\mathrm{Sep}_L(c,d)$.

Conversely, let $A \models \mathrm{Sep}_L(c,d)$. Let $a_0,\dots,a_{r-1},b$ be elements that witness the existential quantifiers. Denote the elements $\alpha^A(\overline{a},b,c,d)$ and $\beta^A(\overline{a},b,c,d)$ by α and β respectively. Write A as a subdirect product of subdirectly irreducible algebras, $A \leq \Pi(A_t : t \in T)$, and let Θ_t be the kernel of the projection $A \twoheadrightarrow A_t$. Set $U = \{t \in T : \alpha \not\equiv \beta(\mathrm{mod}\,\Theta_t)\}$ and for every $x \in A$, $V_x = \{t \in T : \text{for some } i < r,\ a_i \equiv x(\mathrm{mod}\,\Theta_t)\}$.

<u>Claim</u>. There is an ultrafilter D on T such that $U \in D$ and for every $x \in A$, $V_x \in D$.

Observe that once the claim is established the theorem will follow easily. For, take $\Psi = D|A$. Ψ is a coatom of $\mathrm{Con}(A)$ since A/Ψ can be embedded in the ultraproduct $(\Pi A_t)/D$ which is simple (V is finitely generated). Since $U \in D$, $\alpha \not\equiv \beta(\mathrm{mod}\,\Psi)$, hence by the construction of α and β, $c/\Psi \neq d/\Psi$ and $\{a_0/\Psi,\ldots,a_{r-1}/\Psi\}$ forms a subalgebra of A/Ψ isomorphic to L. But for every $x \in A$, $V_x \in D$ implies that $x \equiv a_i(\mathrm{mod}\,\Psi)$ some $i < r$. Therefore $L \cong \{a_0/\Psi,\ldots,a_{r-1}/\Psi\} = A/\Psi$ and the theorem follows.

To verify the claim, it suffices to show that the family $U \cup \{V_x : x \in A\}$ has the finite intersection property. For this choose $x_0,\ldots,x_k$ from A for some natural number k and let E be the subalgebra of A generated by all the elements $a_0,\ldots,a_{r-1},b,x_0,\ldots,x_k,\alpha$ and β. This is a finite set so, since V is finitely generated, E is finite. Therefore by theorem 2(2), E is a direct product of simple algebras, in fact $E \cong \Pi(E_t : t \in T_0)$ where T_0 is a finite subset of T and $E_t = E/(\Theta_t|E)$.

Now suppose $U \cap \bigcap(V_{x_j} : j \leq k) = \emptyset$. Then for every $t \in U$, there is an integer $t^* \leq k$ with $t \notin V_{x_{t^*}}$. Since E is a direct product, there is an element $e \in E$ such that for every $t \in T_0 \cap U$, $e \equiv x_{t^*}(\mathrm{mod}\,\Theta_t)$. Recall that A is assumed to satisfy $\mathrm{Sep}_L(c,d)$ with $a_0,\ldots,a_{r-1},b$ as witnesses. Since $e \in A$, this insures that for some $i < r$, $\sigma^A(a_i,e,\alpha) \neq \sigma^A(a_i,e,\beta)$. Since every a_i, e, α and β is a member of E this can be computed in E as well, thus: $\sigma^E(a_i,e,\alpha) \neq \sigma^E(a_i,e,\beta)$. However terms of E are computed coordinatewise, so for any $i < r$: if $t \in T_0 \cap U$ then $e \equiv x_{t^*} \not\equiv a_i(\mathrm{mod}\,\Theta_t)$ (since $t \notin V_{x_{t^*}}$), and for $t \in T_0 - U$, $\alpha \equiv \beta(\mathrm{mod}\,\Theta_t)$. Therefore the elements $\sigma^E(a_i,e,\alpha)$ and $\sigma^E(a_i,e,\beta)$ agree in every coordinate of E, so must be equal. This is a contradiction and concludes the proof.

Let us now turn to the amalgamation class. $\mathrm{AMAL}(V)$ has proved to be a difficult class to characterize, even for very well-behaved varieties. The aim of this paper is to show that, at least for discriminator varieties, the class has a very satisfactory description, namely by a finite set of first order sentences. [1] is an in-depth study of the subject and contains the characterization of $\mathrm{AMAL}(V)$

that will serve as the starting point here.

DEFINITION 5. Let V be a variety, $A \in V$:

(1) $V_{ASI} = AMAL(V) \cap V_{SI}$

(2) $A^{\$} = \Pi(A/\Psi : \Psi \in Con(A)$ and $A/\Psi \in V_{ASI})$

(3) μ_A is the canonical homomorphism from A to $A^{\$}$.

Werner proved [7, theorem 2.2(11)] that every discriminator variety is filtral, hence has the congruence extension property. A *maximal simple algebra* of V is a simple algebra of V with no proper, simple extensions in V.

THEOREM 6 [1, 3.5 and 4.10]: *Let* V *be a finitely generated discriminator variety.*

(1) *For* $A \in V_{SI}$: $A \in V_{ASI}$ *if and only if for every pair of maximal simple algebras* B_0, B_1 *extending* A, *there is an isomorphism of* B_0 *with* B_1 *which is the identity on* A.

(2) *For* $A \in V$: $A \in AMAL(V)$ *if and only if for every maximal simple algebra* M *and homomorphism* $\lambda : A \to M$ *there is a homomorphism* $\overline{\lambda} : A^{\$} \to M$ *such that* $\overline{\lambda} \circ \mu_A = \lambda$.

COROLLARY 7. *Let* V *be a finitely generated discriminator variety,* $A \in V$. *Then* $A \in AMAL(V)$ *if and only if:*

(i) μ_A *is one-to-one and*

(ii) *For every maximal simple* M, *every* $\Theta \in Con(A)$ *and* η *embedding* A/Θ *into* M, *there exists* $\overline{\Theta} \in Con(A^{\$})$ *and* $\overline{\eta}$ *embedding* $A^{\$}/\overline{\Theta}$ *into* M *such that* $\overline{\Theta}|A = \Theta$ *and* $\overline{\eta} \circ (\mu/\overline{\Theta}) = \eta$. *(Here* $\mu/\overline{\Theta} : A/\Theta \to A^{\$}/\overline{\Theta}$ *takes* a/Θ *to* $\mu(a)/\overline{\Theta}$.*)*

<u>Proof</u>. The following diagram should suggest the proof with $\Theta = \ker \lambda$.

$$\begin{tikzcd}
A^{\$} \arrow[dr, two heads] & & \\
 & A^{\$}/\overline{\Theta} \arrow[dr, "\overline{\eta}"] & \\
A \arrow[uu, tail, "\mu_A"] \arrow[r, two heads] & A/\Theta \arrow[u, tail, "\mu/\overline{\Theta}"] \arrow[r, tail, "\eta"'] & M
\end{tikzcd}$$

Suppose V is of finite type, K, L are simple algebras of V and ν is an embedding of K into L. Write $K = \{k_0,\ldots,k_{r-1}\}$. By an argument almost identical to the one preceding theorem 4, there are terms γ and δ so that the formula $\mathrm{Fac}_K(x_0,\ldots,x_{r-1},u,v)$ given by

$$(\exists y)(\forall z)[\gamma(\overline{x},y,u,v) \not\approx \delta(\overline{x},y,u,v) \wedge \bigvee_{i<r}(\sigma[x_i,z,\gamma(\overline{x},y,u,v)] \not\approx \sigma[x_i,z,\delta(\overline{x},y,u,v)])]$$

is such that

$A \models \mathrm{Fac}_K(\overline{a},c,d)$ if and only if there is a coatom Ψ of $\mathrm{Con}(A)$ such that $c \equiv d(\mathrm{mod}\,\Psi)$ and $\{a_0/\Psi,\ldots,a_{r-1}/\Psi\} \cong K$ with a_j/Ψ is mapped to k_j for $j < r$.

Similarly, there is a formula $\mathrm{Ext}_{L,\nu,K}(\overline{x},\overline{y},u,v)$ such that

$A \models \mathrm{Ext}_{L,\nu,K}(\overline{a},\overline{b},c,d)$ if and only if there is a coatom Ψ of $\mathrm{Con}(A)$ such that $c \equiv d(\Psi)$, $A/\Psi = \{a_0/\Psi,\ldots,a_{r-1}/\Psi,b_0/\Psi,\ldots,b_{s-1}/\Psi\}$ and there is an isomorphism of A/Ψ with L which carries a_j/Ψ to $\nu(k_j)$ for $j < r$.

THEOREM 8. *Let* V *be a finitely generated discriminator variety of finite type. Then* $\mathrm{AMAL}(V)$ *is finitely axiomatizable.*

Proof. Begin with the set Σ' axiomatizing $\mathrm{Ps}(V_{ASI})$ produced by theorem 5. Then $A \models \Sigma'$ if and only if μ_A is one-to-one. To apply corollary 7, let M be maximal simple, $\Theta \in \mathrm{Con}(A)$ and η an embedding of A/Θ into M. Since V has the congruence extension property, $K = A/\Theta$ is simple. We need a sentence equivalent to the existence (in the presence of Σ') of $\overline{\eta}$ and $\overline{\Theta}$ as in 7(ii).

Since V is finitely generated, there are only finitely many pairs (up to isomorphism) (L_i,ν_i) such that: (i) $L_i \in V_{ASI}$, (ii) ν_i is an embedding of K into L_i and (iii) there exists $\tau : L_i \to M$ such that $\tau \circ \nu_i = \eta$. Let $i = 0,\ldots,m-1$ enumerate those pairs and let $P_{K,\eta}$ be the sentence:

$$(\forall\overline{x})\bigvee_{i=0}^{m-1}(\forall u,v)[\mathrm{Fac}_K(\overline{x},u,v) \to (\exists\overline{y})\mathrm{Ext}_{L_i\nu_iK}(\overline{x},\overline{y},u,v)].$$

We verify that if $A \models \Sigma' \cup \{P_{K,\eta}\}$ then $\overline{\Theta}$ and $\overline{\eta}$ exist with the desired properties. The converse is left to the reader. Choose a sequence $a_0,a_1,\ldots,a_{r-1}$ of coset representatives for A by Θ. Since $A/\Theta = K$, for any $(c,d) \in \Theta$ we have $A \models \mathrm{Fac}_K(\overline{a},c,d)$. Therefore, by assumption, there is an $i < m$ such that

$A \models (\exists\bar{y})\mathrm{Ext}_{L_i,\nu_i,K}(\bar{a},\bar{y},c,d)$, whenever $(c,d) \in \Theta$.

Let $T = \{\Psi \in \mathrm{Con}(A) : A/\Psi \in V_{ASI}\}$ and consider the family $U \cup \{V(c,d) : (c,d) \in \Theta\}$ where:

$U = \{\Psi \in T$: there is an isomorphism of A/Ψ with L_i taking a_j/Ψ to $\nu_i(k_j)$ all $j < r\}$.

$V(c,d) = \{\Psi \in T : (c,d) \in \Psi\}$.

This family of subsets of T is contained in an ultrafilter over T. To show this, it suffices to check the finite intersection property. So, let $p < \omega$ and $(c_0,d_0),\ldots,(c_p,d_p)$ be pairs from Θ. In a discriminator variety, every compact congruence is principal (see [7,2.2.(8)]) so there exists $c,d \in A$ such that for every $\Psi \in \mathrm{Con}(A)$, $(c,d) \in \Psi$ if and only if $(c_j,d_j) \in \Psi$ all $j \leq p$. In particular, $(c,d) \in \Theta$ so $A \models (\exists\bar{y})\mathrm{Ext}_{L_i,\nu_i,K}(\bar{a},\bar{y},c,d)$. By the very construction of the formula $\mathrm{Ext}_{L_i,\nu_i,K}$, there is a congruence Ψ contained in $U \cap V(c,d)$ and hence in each $V(c_j,d_j)$, $j \leq p$. Since p as well as the (c_j,d_j)'s were arbitrary, the family has the finite intersection property.

$$
\begin{tikzcd}
A^{\$} \arrow[dr, two heads] & & & \\
 & A^{\$}/\bar{\Theta} \arrow[r, phantom, "\overset{\xi}{\cong}"] & L_i \arrow[dr, "\tau"] & \\
A \arrow[uu, tail, "\mu_A"] \arrow[r, two heads] & A/\Theta \arrow[u, tail, "\mu/\bar{\Theta}"] \arrow[r, phantom, "="] & K \arrow[u, tail, "\nu_i"'] \arrow[r, tail, "\eta"'] & M
\end{tikzcd}
$$

Thus there is an ultrafilter D over T containing these sets. Set $\overline{\Theta} = D$ as a congruence on $A^{\$}$. Since every $V(c,d) \in D$, $\overline{\Theta}|A \supseteq \Theta$. Since $U \in D$ we get the opposite inclusion as well as an isomorphism ξ of $A^{\$}/\overline{\Theta}$ with L_i whose composition with $\mu/\overline{\Theta}$ equals ν_i. Setting $\overline{\eta}$ to be $\tau \circ \xi$ (the map associated with (L_i,ν_i)) one verifies that $\overline{\eta} \circ (\mu/\overline{\Theta}) = \eta$ (see diagram).

Finally the proof can be completed by observing that there are only finitely many pairs (K,η) (up to isomorphism) such that η is an embedding of K into a maximal simple algebra. Define P to be the formula: $\bigwedge P_{K,\eta}$, the conjunction over all such pairs. Then the set $\Sigma' \cup \{P\}$ axiomatizes $AMAL(\mathcal{V})$.

Remark. A careful examination of the sentences involved will reveal that the characterizations in theorems 5 and 8 are $\forall\exists\forall$ in complexity. It is not hard to show that for any variety $\mathcal{V}$, $AMAL(\mathcal{V})$ is closed under unions of chains (take an ultraproduct). Thus, by the "Chang-Łos-Susko theorem", there is an axiomatization which is $\forall\exists$ in complexity. This can be achieved by omitting the subformulas "$(\forall z)\bigvee[\sigma(x,z,\alpha) \not\approx \sigma(x,z,\beta)]$" from Fac, Ext and Sep. Since the proofs are more complicated, we have not taken that tack. Is a similar reduction possible for $Ps(\mathcal{S})$?

REFERENCES

1. Bergman, C., Concerning the amalgamation bases of congruence distributive equational classes, Ph.D. thesis, University of California, 1981.

2. Burris, S. and H. P. Sankappanavar, A Course in Universal Algebra, Springer-Verlag, New York, 1981.

3. Grätzer, G., Universal Algebra, 2nd ed., Springer-Verlag, New York, 1979.

4. Jónsson, B., Algebras whose congruence lattices are distributive, Math. Scand., 21(1967), 110-121.

5. McKenzie, R., On spectra, and the negative solution of the decision problem for identities having a finite nontrivial model, J. Symbolic Logic, 40(1975), 186-195.

6. Pixley, A. F., Functionally complete algebras generating distributive and permutable classes, Math. Z., 114(1970), 361-372.

7. Werner, H., Discriminator Algebras, Studium zur Algebra und ihre Andwendungen 6, Akademie Verlag, Berlin (1978).

University of Hawaii at Manoa
Honolulu, HI 96822

FREE SPECTRA OF 3-ELEMENT ALGEBRAS

Joel Berman

If A is an algebraic system, then the free spectrum of A is the sequence s(n) of cardinalities of the free algebras on n free generators in the equational class generated by A. This paper is a catalog of such free spectra for several hundred different 3-element algebraic systems. The catalog is organized lexicographically by the sequences <s(0), s(1), s(2),...>.

1. USES OF FREE SPECTRA. Several points of view are possible in describing free spectra. In universal algebra the value s(n) is the number of distinct n-ary polynomials on an algebra A. If the algebra A is finite of size k, then a result of Birkhoff states that s(n) $\leq$ k**(k**n). (Here, and elsewhere in this paper, r**s means r rasied to the power s. Also, C(n,i) denotes the binomial coefficient n choose i.) Standard sources on universal algebra and free spectra include Birkhoff(1967) and Gratzer(1979).

Another place where the sequence s(n) occurs is in logic, especially many-valued logic. Given a system of propositional logic, s(n) counts the number of possible distinct truth tables that can be constructed in this system using the given connectives of the system. For classical logic this is of course 2**(2**n). For the nonclassical 3-valued systems of Post, Heyting, or Lukasiewicz the number of such truth tables is given by the entries #235#, #187#, or #201# respectively, in the catalog. In the logic literature the set of operation tables for the fundamental connectives is often called a matrix. Note that in computing the values of s(n) the so called designated elements of the matrix play no role. Another way of describing the free spectra in this setting is that the value s(n) is the cardinality of the Lindenbaum-Tarski algebra of n variable formulas in the given logical system. Rescher(1969) contains a very extensive presentation of the various many-valued logics and also has a detailed bibliography. Wolf(1977) contains an updating of this bibliography.

The theory of switching functions provides another place where free spectra occur. Here the numbers $s(n)$ can be interpreted as the number of inequivalent circuits that can be built using a specified family of components and n input signals. In the case where there are two possible choices for each input this corresponds to the usual Boolean valued switching theory. If instead the signals have three possible values, then the $s(n)$ sequences that arise correspond in a natural way to the free spectra of 3-element algebras. The Proceedings of the International Symposia on Multiple-valued Logic for the last ten years contain numerous papers on the theory of such switching functions. The book Moisil(1969) is devoted to this many-valued switching theory and the books Carvallo(1968) and Thielliez(1973) are devoted solely to the three-valued case. The paper Rosenberg(1977) has an extensive bibliography.

In Berman(1980) I considered the free spectra of 2-element algebras. In the 2-element case all the possible distinct equational classes that can be generated have been described by Post(1941). They form a countably infinite well-behaved family. Indeed, in my paper a description of all these equational classes, a list of their free spectra, and a tabulation of some other properties they possess all fit nicely onto one page.

The 3-element case is much more complicated. Firstly, there are an uncountable number of inequivalent equational classes that can be generated by 3-element algebras. Simple proofs of this are given in Janov and Mucnik (1959) and Hulanicki and Swierczkowski(1960). In fact, the equational classes they give have pairwise different free spectra. Also, many algebraic properties that hold for equational classes generated by 2-element algebras fail for the 3-element case. Berman(1980) contains about a half-dozen of such properties. The cause of this is not known except of course that 3 is bigger than 2. My motivation for writing this paper is in part an attempt to understand this.

Another motivation for this paper is that there appears to be a strong connection between the free spectrum, especially its rate of growth, and some important algebraic properties the equational class may possess. In Berman(1980) and Berman(1982) I investigated this and I felt that many more examples of free spectra would be needed in order to pursue this idea. So this catalog is a large collection of experimental results to be used, I hope, in suggesting theorems about algebras and their equational classes; theorems involving numerical conditions on the free spectrum.

Yet another motivation for compiling this list of free spectra is that the spectrum of an algebra is an important invariant for the algebra, and the first few terms of this invariant are easily computed (on a computer). This catalog is thus a bestiary of many known 3-element algebras, indexed by their free spectra. My experience with the extremely useful book, A Handbook of Integer Sequences by N. Sloane led me to compile the smaller, more specialized catalog given in this paper. As it turned out, the intersection of the sequences in Sloane's book and the free spectra listed below is a very small set.

2. THE CATALOG. The free spectra are arranged in lexicographic order. The values of $s(n)$ are obtained by the computer program described in Berman and Wolk(1980). Given the operation tables of an algebra A and an integer n, this program explicitly constructs the free algebra on n free generators for the equational class generated by A. That is, it produces a list of the distinct n-ary polynomials that can be built by composition from the fundamental operations of the algebra A. A detailed discussion of this program and an exact FORTRAN listing of it may be found in that paper.

In the catalog the values $s(0), s(1),\ldots,s(4)$ are explicitly listed. Following these first few values of the $s(n)$ is an explicit formula for $s(n)$ if such a formula is known. In some cases this formula for $s(n)$ only applies to $n > 0$. In a few cases such a formula is followed by a question mark; this indicates a conjectured closed form for evaluating $s(n)$. If fewer than five values of the $s(n)$

are given, and if no general formula for $s(n)$ is presented, then the missing values are not known. The value for $s(0)$ is defined to be the number of constant functions that are generated by the program when computing the free algebra on 1 free generator. Note that $s(0)$ can be positive even if there are no constants in the given similarity type of A.

The line following the values of $s(n)$ in the catalog is the set of functions of the algebra, unary operations written first. The algebra, A say, always has the same underlying set: {0,1,2}. Then a unary operation $g(x)$ is written as the 3-tuple (g(0) g(1) g(2)). Binary operations are written as 9-tuples, read across rows. Constants are treated as unary operations and appear as (ccc) for some c = 0,1, or 2. This catalog includes only algebras that have unary or binary operations.

The next lines for a given spectrum are a description of the algebra, logical system, set of switching functions, or clone or whatever. Most of the algebras etc. considered are taken from the literature. References are given whenever possible. An asterisk following a bibliographic item indicates that the article explicitly deals with the free algebras or the free spectra of the algebra A. Many of the closed forms for $s(n)$ presented here do not appear in the literature. Most, but not all, of these formulas are easy to derive. A paper describing general techniques for finding closed forms for free spectra is in preparation.

Two equational classes are called polynomially equivalent if there is a weak isomorphism between their countably generated free algebras that preserves free generators. See Goetz(1966) and Taylor(1973) for more details. In the catalog, algebras that have the same free spectra and generate polynomially inequivalent equational classes are distinguished by adding a suffix "1" or "2" etc. to the appropriate headings. The following procedure was used in deciding polynomial equivalence for algebras giving the same initial values for their free spectra. First the list of polynomials in the free algebra on two free generators was scanned to see if it contained the operations (or some isomorph) of the other system. This is relatively easy using the computer text editor. If this turns up nothing, then another computer program generates the principal congruences in the free algebra on one or two generators for each of the two algebras. Examination of this output usually provided conclusive proof of polynomial inequivalence, or else suggested the desired weak isomorphism.

In the description of the algebra the following terminology is used. Unary operations are frequently described by a phrase describing their diagram as a directed graph. Thus the unary function (100) is a 2-cycle with tail. The names for the other nonisomorphic unary functions are given in the index under "unary algebra". An algebra whose set of fundamental operations consists of a single binary operation is called a groupoid. A groupoid is a semigroup if the binary operation is associative. An algebra A is idempotent if $f(x,\ldots,x)=x$ for all of its operations f and all x in A. Note that if A is idempotent, then $s(0)=0$ and $s(1)=1$. A zero of a groupoid is an element z for which $zx = xz = z$ for all x. A groupoid element z is a unit if $zx = xz = x$ for all x.

To adjoin a constant to an algebra A means to add a particular constant function to the similarity type of A. If an algebra A has free spectrum $s(n)$, and if an algebra A' is obtained from A by adjoining a constant to A, the the free spectrum $s'(n)$ of A' satisfies the inequality

$$s(n) \leq s'(n) \leq s(n+1)$$

The adjoined constant is called generic if the equality $s'(n) = s(n+1)$ holds for all n. For example, the middle element in a 3-element distributive lattice is generic, the two other elements are not.

Given an algebra A there several ways to adjoin a new element z to A in order to create a new algebra B of the same similarity type as A. The element z is called an absorbing element if for any operation f of B, f restricted to A behaves as f does on A, otherwise f evaluates to z. In this case, B is obtained from A by adjoining an absorbing element to A. Absorbing elements come up in the study of regular equations. See Lakser & Padmanabhan & Platt(1972), Jonsson & Nelson(1974), or John(1976) for some results on this. The element z is said to be analogous to the element a of A if for any operation f of B, f restricted to A behaves as f does on A, otherwise for arguments of f that involve z, replace z by a, and evaluate as in A. In such a case the algebra B is said to be analog of the algebra A. (See Smiley(1962) or some of the "weak variants" in

Rescher(1969).) For example, the algebra in sequence #038# in the catalog is the 3-element analog of the 2-element distributive lattice: here z is 1 and a is 0. Finally, the element z is called invisible if there is some element a in A such that for any operation f of B, f restricted to A behaves as f does on A, otherwise f evaluates to a. The algebra in #049# is obtained by adjoining an invisible element to the 2-element distributive lattice.

Many of the entries in the catalog are derived from 3-valued propositional logics. Typically there are the binary operations of conjunction, disjunction, implication, and equivalence; the unary negation operation; and perhaps some logical constants. Of course frequently some of these operations can be defined in terms of the others. The reader is cautioned that there is no consistent pattern for which of the values 0,1, or 2 correspond to True or False in the logical system. A fragment of a logical system is a system in which only a subset of these connectives is allowed. For example if only implication is used, then the system is called an implicational fragment. If the point of view of universal algebra is used, then a fragment corresponds to a reduct of the algebra. In proving the independence of a set of axioms for a logical system, various ad hoc matrices are presented which satisfy some but not all of the given axioms. Some of the more interesting examples of such are also found in the catalog. For example, an algebra producing sequence #129# is a groupoid used in Sheffer(1913) to show the independence of his axioms for what is now called the Sheffer stroke. The groupoid has appeared sporadically in the literature since then.

3. THE INDICES. There are four indices following the catalog. The first is an index of all the binary operations that appear. If the 19683 possible binary operations on the set {0,1,2} are partitioned into classes of isomorphic or anti-isomorphic operations, then each class has at most 12 members. If an operation appears in the catalog, then the operation in its class having least value as a base 3 number when written as a 9-tuple is the representative chosen for the index. These representatives are then listed in increasing lexicographic (=numerical) order.

Next is an index of the number of essentially n-ary operations for each of the 235 free spectra listed. The number of essentially n-ary operations in an equational class is usually denoted by the sequence $p(n)$ for $n=0,1,2,\ldots$. For a given locally finite equational class the sequences $s(n)$ and $p(n)$ are related by

$$s(n) = \sum_{i=0}^{n} C(n,i)p(i) \qquad p(n) = \sum_{i=0}^{n} (-1)^{n-i} C(n,i)s(i)$$

Gratzer(1970) contains a survey of results on $p(n)$ sequences. The papers by Marczewski, Plonka, and Urbanik in the bibliography also contain work on these sequences.

The last two indices are more traditional. One is just an alphabetized list of words used in the description of the algebras and the equational classes of the catalog. The other is the bibliography, which is an index, since at the end of each item is a list of those sequences that cite it.

4. ACKNOWLEDGEMENTS. A number of people provided very useful correspondence while I was preparing this paper. K. Baker kindly shared with me his computations of the free spectra of 3-element groupoids with a zero element. I also thank W. Blok, G. Epstein, J. Jezek, P. Kohler, A. Pixley, R. Quackenbush, A. Romanowska, and I. Rosenberg for their help. Several people provided helpful comments and corrections to an early draft of this paper; especially helpful were B. Csakany, J. Demetrovics, R. Mckenzie, M Mukaidono, and W. Taylor. Computing was done at the Computer Center of the University of Illinois at Chicago.

CATALOG OF FREE ALGEBRAS IN EQUATIONAL CLASSES GENERATED BY 3-ELEMENT ALGEBRAS

line s: sequence of cardinalities of free algebras on 0,1,2,3,4 free generators, followed by general form if known. x*y means x times y; x**y means x raised to power y. C(n,i) is the binomial coefficient n choose i.
line f: the fundamental operations for the 3-element algebra. Parentheses enclose each operation of the algebra, binary functions are read across rows of Cayley table.
line d: description of the algebra, common name, properties etc.
line r: references, if any, to this variety or algebra. if reference contains information on free algebra, then this is indicated by a * .

lines f,d,r are repeated for polynomially equivalent algebras

lines f1,r1, etc. algebras with the same free spectra polynomially inequivalent to the previous ones

```
#001#s  0,1,2,3,4    n
#001#f  (012)
#001#d  1-unary: identity function
#001#f  (000 111 222)
#001#d  semigroup  xy=x

#002#s  0,1,3;7,15   2**n-1
#002#f  (000 010 002)
#002#d  semilattice
#002#f  (000 011 012)
#002#d  semilattice: chain

#003#s  0,1,3,9,27      3**(n-1)
#003#f  (021 210 102)
#003#d  groupoid: Steiner quasigroup, idempotent,  2x+2y (mod 3)
#003#r  Urbanik (1965), Gratzer & Padmanabhan(1971)*
#003#r  Baldwin & Lachlan(1973), Quackenbush(1976), Csakany(1980)

#004#s  0,1,3,15,531487  sum i=1 to n (C(n,i)*3**(3**(i-1)-2**i+1))
#004#f  (010 112 022)
#004#d  upper bound algebra; minimal binary clone; quasitrivial groupoid
#004#r  Kaiser(1975), Park(1976), Winker & Berman (1979)*
#004#r  Demetrovics & Hannak & Marchenkov(1980), Kepka(1981a), Csakany(1982)

#005#s  0,1,4,12,32      n*2**(n-1)
#005#f  (000 010 222)
#005#d  semigroup: idempotent, xyz=xzy, nearly quasitrivial
#005#r  Płonka(1971)*, Gerhard(1971)*, Jezek & Kepka(1978)
#005#f  (000 011 022)
#005#d  semigroup: idempotent, has zero, quasitrivial
#005#r  Plonka(1971)*, Gerhard(1971)*, Kepka(1981a)
#005#f1 (000 211 122)
#005#d1 groupoid: idempotent, (xy)y=x, quandle, kei
#005#r1 Takasaki(1943), Plonka(1971)*, Pierce(1978), Winker(1981)
#005#f2 (000 211 222)
#005#d2 groupoid: idempotent, (xy)y=xy, nearly quasitrivial
#005#r2 Plonka(1971)*, Day(1973)*, Jezek & Kepka(1978)

#006#s  0,1,4,15,64      sum i=0 to n (C(n,i)*(i factorial))
#006#f  (000 012 222)
#006#d  semigroup: idempotent, left distributive; minimal binary clone
#006#r  Gerhard(1971)*, Taylor(1976), Kepka(1981), Csakany(1982)
```

```
#007#s  0,1,4,18,140
#007#f  (000 011 222)
#007#d  groupoid: quasitrivial, left distributive; minimal binary clone
#007#r  Kepka(1981), Kepka(1981a), Csakany(1982)

#008#s  0,1,4,18,166,7579,7828352,2414682040996
#008#f  (000 011 012) (012 112 222)
#008#d  distributive lattice
#008#r  Birkhoff(1967),p.63*, Church(1965)*, Berman & Kohler(1976)*

#009#s  0,1,4,30
#009#f  (000 110 202)
#009#d  groupoid; minimal binary clone
#009#r  Csakany(1982)

#010#s  0,1,4,36
#010#f  (000 112 212)
#010#d  groupoid: quasitrivial, left distributive
#010#r  Kepka(1981), Kepka(1981a)

#011#s  0,1,4,54
#011#f  (000 011 212)
#011#d  groupoid: quasitrivial; minimal binary clone
#011#r  Kepka(1981a), Csakany(1982)

#012#s  0,1,4,162,88219206    #008#*3**(3**(n-1)-2**n+1)
#012#f  (002 011 212) (010 112 022)
#012#d  tournament: triangle
#012#r  Quackenbush(1972), Fried & Gratzer(1973)*

#013#s  0,1,5,28
#013#f  (000 010 012)
#013#d  groupoid: has zero

#014#s  0,1,5,96
#014#f  (012 110 202)
#014#d  groupoid: idempotent, has unit
#014#r  Rose(1961), Marczewski(1964), Robinson(1971), Leigh(1972)

#015#s  0,1,6,33,266         sum i=1 to n (C(n,i)*#008#)
#015#f  (000 011 012) (000 012 022)
#015#d  distributive bisemilattice, distributive quasilattice
#015#d  Bochvar fragment: disjunction, conjunction
#015#r  Plonka(1967), Padmanabhan(1971)*, Plonka(1971a)*

#016#s  0,1,6,39,316
#016#f  (000 111 102)
#016#d  groupoid: left distributive
#016#r  Kepka(1981)

#017#s  0,1,6,60,2367
#017#f  (000 011 012) (012 111 212)
#017#d  bisemilattice: bichain with one distributive law
#017#r  Padmanabhan(1971)*, Romanowska(1980)*, see #018#

#018#s  0,1,6,60
#018#f  (000 011 012) (000 010 002)
#018#d  bisemilattice: satisfies no distributive laws
#018#r  Dudek & Romanowska(1981)*, see #017#

#019#s  0,1,6,89
#019#f  (001 011 112)
```

#019#d groupoid: idempotent and commutative
#019#r Keir(1964), Gutierrez & Moraga(1974)

#020#s 0,1,6,100
#020#f (000 011 012) (022 212 222)
#020#d bisemilattice
#020#r Bielecka-Holda(1980), Dudek & Romanowska(1981)*

#021#s 0,1,6,183
#021#f (000 012 212)
#021#d groupoid: quasitrivial
#021#r Kepka(1981a)

#022#s 0,1,6,213
#022#f (000 011 012) (010 111 012)
#022#d bisemilattice: bichain satisfies no distributive law
#022#r Dudek & Romanowska(1981)*

#023#s 0,1,7,505
#023#f (012 110 212)
#023#d groupoid: idempotent, has unit

#024#s 0,1,8,285
#024#f (010 011 012) (012 012 222)
#024#d system used for independence of lattice axioms
#024#r Croisot(1951)

#025#s 0,1,8,331
#025#f (001 012 122) (011 111 112)
#025#d fragment of Hanson ternary threshold logic
#025#r Hanson(1963)

#026#s 0,1,9,129
#026#f (011 111 112) (000 011 012) (012 112 222)
#026#d distributive lattice with third semilattice operation
#026#r Arnold(1951)

#027#s 0,1,9,489
#027#f (000 011 012) (012 112 222) (000 012 022)
#027#d lattice ordered semigroup
#027#r Gabovich(1976), Saito(1977)

#028#s 0,1,9,6561 3**((3**n-3)/3)
#028#f (010 112 022) (021 210 102)
#028#d clone of self dual functions preserving 0; quasiprimal
#028#r Demetrovics & Hannak & Marchenkov(1980), Csakany & Gavalcova(1982)

#029#s 0,1,10,411
#029#f (010 011 102)
#029#d groupoid: not entropic, preserves sums of subgroupoids
#029#r Evans(1962)

#030#s 0,1,14
#030#f (000 011 102)
#030#d groupoid: nonassociative, but satisfies the inclusion property
#030#r Salomaa(1959), p.138

#031#s 0,1,15
#031#f (001 010 102)
#031#d groupoid: idempotent, commutative
#031#r Keir(1964)

#032#s 0,1,16
#032#f (000 010 002) (011 111 112)
#032#d bisemilattice

#033#s 0,1,27,531441 3**((3**n-3)/2)
#033#f (021 110 202)
#033#d groupoid; quasiprimal
#033#r Takasaki(1943), Csakany & Gavalcova(1982)

#034#s 0,1,729,282429536481 3**(3**n-3)
#034#f (012 112 222) (021 210 102)
#034#d all idempotent functions; quasiprimal
#034#r Quackenbush(1974)*

#035#s 0,2,4,6,8 2n
#035#f (002)
#035#d 1-unary: 2-chain with fixed point, f(f(x))=f(x)
#035#f (000 000 222)
#035#d semigroup: xy=xz
#035#f1 (021)
#035#d1 1-unary: 2-cycle with fixed point, involution, f(f(x))=x

#036#s 0,2,5,10,19 n+2**n-1
#036#f (000 000 002)
#036#d semigroup: has zero, analog of semilattice
#036#f (000 011 011)
#036#d semigroup: has zero, analog of semilattice
#036#r Bernstein(1921), Smiley(1962), Rescher(1969) p.336, Moraga(1975)

#037#s 0,2,6,18,68 n + #006#
#037#f (000 111 010)
#037#d groupoid: not entropic, preserves sums of subgroupoids
#037#r Evans(1962)

#038#s 0,2,6,21,170 n+#008#
#038#f (000 000 002) (002 002 222)
#038#d analog of distributive lattice
#038#d mutually distributive associative disjunction and conjunction
#038#r P. Dienes(1949), Rescher(1969) p.336

#039#s 0,2,7,19,47 (n+2)*2**(n-1)-1
#039#f (000 000 012)
#039#d semigroup: has zero; implication
#039#r Reichenbach(1944), Goddard & Routley(1973) p.351, Baker(1981)*

#040#s 0,2,7,22,69 n+3**n-2**n
#040#f (000 000 022)
#040#d groupoid: has zero

#041#s 0,2,7,25,181 #008# + 2**n -1 (?)
#041#f (000 000 002) (002 012 222)
#041#d mutually distributive conjunction and disjunction
#041#r P. Dienes(1949)

#042#s 0,2,8,24,64 n*2**n
#042#f (000 022 011)
#042#d groupoid: has zero, adjoin absorbing element to negation
#042#r Plonka(1971a)*, Baker(1981)*

#043#s 0,2,8,26,80 3**n-1
#043#f (000 001 012)
#043#d semigroup: has zero, xx=xxx; reduct of Chang MV algebra

#043#r Chang(1958)
#043#f1 (000 012 021)
#043#d1 semigroup: has zero, x=xxx
#043#d1 equivalential fragment of Bochvar and Kleene system
#043#r1 Rescher(1969), Chajda(1980)
#043#f1 (002 012 220)
#043#d1 semigroup: x=xxx

#044#s 0,2,8,35,212
#044#f (000 002 022)
#044#d groupoid: has zero

#045#s 0,2,8,59
#045#f (001 011 111)
#045#d groupoid
#045#r Moraga(1975)

#046#s 0,2,10,62,1138   sum i=1 to n (C(n,i)*#095#)
#046#f (000 011 021)
#046#d groupoid: has zero, adjoin absorbing element to implicatio
#046#d Bochvar fragment: implication
#046#r Plonka(1971a)*, Kalman(1980)*

#047#s 0,2,11,52,247
#047#f (011 122 222)
#047#d groupoid
#047#r Kabat & Wojick(1981)

#048#s 0,2,11,64,523
#048#f (000 001 022)
#048#d groupoid: has zero, not finitely based
#048#r Murskii(1965)

#049#s 0,2,11,492
#049#f (010 110 000) (000 010 000)
#049#d adjoin invisible element to distributive lattices

#050#s 0,2,12,114
#050#f (000 011 012) (012 111 211)
#050#d system used to show independence of lattice axioms
#050#r Sobocinski(1972)

#051#s 0,2,12,120
#051#f (112) (000 012 022) (012 112 222)
#051#d Conway's Kleene algebras
#051#r Conway(1971)

#052#s 0,2,12,158,33336 sum i=1 to n (C(n,i)*(2**(2**i-1)))
#052#f (000 012 021) (000 012 022)
#052#d adjoin zero to Boolean ring
#052#d Bochvar fragment: implication and equivalence

#053#s 0,2,12,174
#053#f (012 002 022)
#053#d regular implication
#053#r Cleave(1980)

#054#s 0,2,13,147
#054#f (000 011 012) (012 112 222) (111 111 112)
#054#d lattice ordered semigroup
#054#r Gabovich(1976), Saito(1977)

#055#s 0,2,13,174
#055#f (000 011 022) (012 122 222)
#055#d system used to show independence of lattice axioms
#055#r Sobocinski(1972)

#056#s 0,2,13,673
#056#f (012 101 212)
#056#d groupoid: has unit

#057#s 0,2,14,272
#057#f (000 001 012) (012 112 222)
#057#d system used to show independence of lattice axioms
#057#r Croisot(1951)

#058#s 0,2,16,659
#058#f (012 000 222)
#058#d implication; left distributive groupoid
#058#r McCarthy(1963), Bandler & Kohout(1979), Cleave(1980), Kepka(1981)

#059#s 0,2,18,1119
#059#f (000 110 210)
#059#d Kleene fragment: implication
#059#r Z.P. Dienes(1949), Church(1953)

#060#s 0,2,20,822
#060#f (012 121 221)
#060#d groupoid: has unit, adjoin unit to complementation

#061#s 0,2,22
#061#f (012 111 210) (012 112 222)
#061#d Kleene fragment: equivalence, conjunction

#062#s 0,2,25
#062#f (000 011 012) (012 111 210)
#062#d Kleene fragment: equivalence, disjunction

#063#s 0,2,28
#063#f (012 100 202)
#063#d groupoid: has unit, x(xx) and (xx)x need not be equal
#063#f1 (012 111 221)
#063#d1 groupoid: has unit, x(xx)=(xx)x=x, adjoin unit to implication

#064#s 0,2,60
#064#f (022 012 000)
#064#d implication
#064#r Sugihara(1955), Sobocinski(1952), Rose(1953), Dunn(1970)
#064#r Tokharz(1975)*, Biela(1975), Mortensen(1978)

#065#s 0,2,648,49589822592 2**(2**n-1)*3**(3**n-2**n-1)
#065#f (011 002 202) (011 002 222) (012 112 222) (000 011 012)
#065#d quasiprimal
#065#r Csakany & Gavalcova(1982)

#066#s 0,3,6,9,12 3n
#066#f (100)
#066#d 1-unary: 2-cycle with tail, pseudocomplementation
#066#f (002) (220)
#066#d 2-unary: 2-chain with fixed point, 2-cycle with tail
#066#f1 (120)
#066#d1 1-unary: 3-cycle, Post negation
#066#r1 Post(1921)
#066#f2 (002) (022)

#066#d2 2-unary: two 2-chains with fixed points
#066#r2 Belkin(1971), Gorbunov(1977)
#066#f3 (002) (112)
#066#d3 2-unary: two 2-chains with fixed points

#067#s 0,3,8,17,34 2**(n+1) + n - 2
#067#f (000 010 000) (222 212 222)
#067#d two analogs of semilattice

#068#s 0,3,9,27,81 3**n
#068#f (102 021 210)
#068#d groupoid: quasigroup, 2x+2y+1 (mod 3)
#068#r Clark & Krauss(1976)

#069#s 0,3,11,39,154 n + sum i=1 to n (C(n,i)*Bell number(i+1))
#069#f (000 010 001)
#069#d groupoid: has zero

#070#s 0,3,13,75
#070#f (000 010 011)
#070#d groupoid: has zero

#071#s 0,3,24
#071#f (000 010 021)
#071#d groupoid: has zero

#072#s 0,3,27,19683 3**(3**(n-1))
#072#f (122 020 110)
#072#d groupoid: satifies Martin's t-closing condition
#072#r Foxley(1962)
#072#f (120) (002 011 212)
#072#d upper bound algebra with 3-cycle adjoined
#072#d maximal clone of self dual functions; quasiprimal
#072#r Jablonskii(1958)*, Kaiser(1975), McKenzie(1982)*,
#072#r Demetrovics & Hannak & Ronyai(1982)*, Csakany & Gavalcova(1982)

#073#s 0,3,46
#073#f (012 122 222) (000 001 012)
#073#d reduct of Chang MV algebra S(2)
#073#d system used for independence of axioms for Kleene algebra
#073#r Chang(1958), Mukaidono(1981)

#074#s 0,3,68
#074#f (000 010 000) (012 012 102)
#074#d system used for indépendence of field axioms
#074#r Bernstein(1921)

#075#s 0,3,90
#075#f (000 110 120)
#075#d Rescher's version of Post implication
#075#r Rescher(1969) p.53

#076#s 0,3,138
#076#f (001 011 120)
#076#d groupoid: unknown if finitely based (due to Grzegorczyk)
#076#r Karnofsky(1968)

#077#s 0,3,168
#077#f (012 110 201)
#077#d groupoid: has unit

#078#s 0,3,432
#078#f (001 012 122) (012 111 210)
#078#d saturation arithmetic
#078#r Motil(1974)

#079#s 0,3,2187 3**(3**n-2)
#079#f (011) (012 112 222) (021 210 102)
#079#d quasiprimal
#079#r Csakany & Gavalcova(1982)

#080#s 0,4,8,12,16 4n
#080#f (002) (102)
#080#d 2-unary: 2-chain with fixed point, 2-cycle with fixed point

#081#s 0,4,16,52,160 2(3**n-1)
#081#f (021) (000 021 012)
#081#d adjoin zero to complemented Boolean group; Bochvar fragment: equivalence
#081#r Rescher(1969) p.29

#082#s 0,4,24,316,66672 sum i=1 to n (C(n,i)*2**(2**i)))
#082#f (000 021 011)
#082#d groupoid: has zero, adjoin absorbing element to Sheffer stroke
#082#r Plonka(1969), Tamthai & Chaiyakul(1980)
#082#f (210) (010 111 012)
#082#d Bochvar system of logic: negation and conjuction as primitive
#082#r Bochvar(1939), Church(1953), Rescher(1969) p.29, Goddard & Routley(1974) p.261

#083#s 0,4,56
#083#f (102) (000 012 222) (012 111 222)
#083#d logical system: modification of Kleene system
#083#r McCarthy(1963), Zaslavskii(1979)

#084#s 0,4,82,43916,160297985274
#084#f (210) (000 011 012) (012 112 222)
#084#d Kleene algebra, fuzzy switching functions, Lukasiewicz fragment
#084#r Kleene(1952) p.332, Balbes & Dwinger(1974)
#084#r Preparata & Yeh(1972)*, Mukaidono(1982)*, Berman & Mukaidono(1982)*
#084#f (222 211 210)
#084#d Sheffer function for Kleene algebra
#084#r Monteiro & Pico(1963), Sestakov(1964), Meredith(1969), Mouftah & Jordan(1974)

#085#s 0,4,264
#085#f (012 121 211)
#085#d groupoid: adjoin unit to Sheffer stroke
#085#f (210) (022 012 000)
#085#d Sobocinski system; Fragment Sugihara system; deontic logic
#085#r Sugihara(1955), Sobocinski(1952), Fisher(1961), Dunn(1970), Tokharz(1975)*

#086#s 0,4,1296,99179645184 2**(2**n)*3**(3**n-2**n-1)
#086#f (210) (000 011 012) (022 012 000)
#086#d Sugihara system; quasiprimal
#086#r Sugihara(1955), Dunn(1970), Tokharz(1975)*, Csakany & Gavalcova(1982)

#087#s 0,5,10,15,20 5n
#087#f (002) (200)
#087#d 2-unary: 2-chain with fixed point, 2-cycle with tail
#087#r Gratzer(1979) pp. 213-214.
#087#f1 (002) (221)
#087#d1 2-unary: 2-chain with fixed point, 2-cycle with tail
#087#f1 (100) (200)
#087#d1 2 unary: two 2-cycle with tail
#087#f2 (100) (101)
#087#d2 2-unary: two 2-cycle with tail

```
#088#s  0,6,12,18,24     6n
#088#f  (002) (210)
#088#d  2-unary: 2-chain with fixed point, 2-cycle with tail
#088#f  (021) (121)
#088#d  2-unary: 2-cycle with fixed point, 2-cycle with tail
#088#f1 (021) (100)
#088#d1 2-unary: 2-cycle with fixed point, 2-cycle with tail
#088#f2 (021) (102)
#088#d2 2-unary: two 2-cycle with fixed point
#088#f2 (021) (120)
#088#d2 2-unary:  2-cycle with fixed point, 3-cycle

#089#s  1,2,3,4,5         n+1
#089#f  (000)
#089#d  1-unary:  constant function
#089#f  (000 000 000)
#089#d  semigroup: has zero, xy=uv

#090#s  1,2,4,8,16       2**n
#090#f  (000) (000 011 012)
#090#d  semilattice with constant zero
#090#f1 (222) (000 011 012)
#090#d1 semilattice with constant unit

#091#s  1,2,5,13,33         1+n*2**(n-1)
#091#f  (000 000 010)
#091#d  groupoid: has zero
#091#r  Wronski(1979)

#092#s  1,2,5,16,55          2+n+3**n-2**(n+1)
#092#f  (000 001 020)
#092#d  groupoid: has zero
#092#r  Baker(1981)*

#093#s  1,2,5,19,167      1 + #008#
#093#f  (000) (000 011 012) (012 112 222)
#093#d  distributive lattice with constant minimal element
#093#f  (222) (000 011 012) (012 112 222)
#093#d  distributive lattice with constant maximal element

#094#s  1,2,6,19,57  1+n2**(n-1)+C(n,2)2**(n-2)
#094#f  (000 001 010)
#094#d  groupoid: has zero
#094#r  Baker(1981)*

#095#s  1,2,6,38,942  sum i=0 to n ((-1)**(i-1)*C(n,i)*2**(2**(n-i)))
#095#f  (012 002 010)
#095#d  implication algebra; BCK algebra; equivalent to 2-valued implication
#095#r  Mitschke(1971), Iseki(1966)

#096#s  1,2,6,52
#096#f  (012 100 200)
#096#d  groupoid: has unit; pseudosum
#096#r  Raca(1969)

#097#s  1,2,7,34,267     1+sum i=1 to n (C(n,i)*#008#)
#097#f  (000) (000 011 012)
#097#d  distributive quasilattices with  0  as constant

#098#s  1,2,7,46     n*(2**(2**(n-1)))-(n-1)  (?)
#098#f  (012 000 000)
#098#d  implication
#098#r  Brady(1971), Goddard & Routley(1973) p.324, Hardegree(1981), Cleave(1980)
```

```
#099#s  1,2,9,640
#099#f  (012 102 220)
#099#d  groupoid: has unit, Heyting fragment: equivalence
#099#r  Kabzinski & Wronski(1975)*
#099#f  (012 101 210)
#099#d  groupoid: has unit, Lukasiewicz fragment: equivalence
#099#d  distance function for Chang MV algebra
#099#r  Chang(1958), Kabzinski(1979), Byrd(1979)

#100#s  1,2,12     2**n*3**((3**n-2*2**n+1)/2) (?)
#100#f  (012 101 220)
#100#d  groupoid: endomorphisms compose, but not "Abelian"
#100#r  Lukasiewicz(1939), Klukovits(1973)

#101#s  1,2,14
#101#f  (222 022 012)
#101#d  Heyting fragment: implication; Hilbert algebra; BCK algebra
#101#r  Jaskowski(1936), Skolem(1952)*, Henkin(1950), Horn(1962), Diego(1965)*,
#101#r  Rielak(1974)*, Urquhart(1974)*, Iseki(1966)

#102#s  1,2,16
#102#f  (012 112 222) (222 022 012)
#102#d  Heyting fragment: disjunction, implication

#103#s  1,2,18,39366  product i=0 to n-1 ((2**(2**i-1) + 1)**C(n,i))
#103#f  (000 011 012) (222 022 012)
#103#d  Heyting fragment: conjunction, implication,  implicative semilattice
#103#r  Nemitz & Whaley(1971), Balbes(1973)*, Landholt & Whaley(1974)*
#103#f  (222) (000 011 012) (222 022 012)
#103#d  Brouwerian semilattice
#103#r  Kohler(1973)*,  Kohler(1975)*, Davey(1976)*
#103#f  (222) (000 011 012) (012 112 222) (222 022 012)
#103#d  relative Stone algebra
#103#r  Hecht & Katrinak(1972), Balbes & Dwinger(1974) pp. 166,176

#104#s  1,2,24,93312    2**(2**n-1)*3**((3**n-2*2**n+1)/2)
#104#f  (022 212 222) (000 111 012) (210 021 012)
#104#d  quasiprimal
#104#r  Csakany & Gavalcova(1982)

#105#s  1,2,40
#105#f  (012 001 000)
#105#d  Lukasiewicz fragment: implication; BCK algebra
#105#f  (012 001 010)
#105#d  example of failure of p*(q*r)=(p*q)*(p*r)
#105#r  Diego(1965) p.10, Iseki(1966), Byrd(1979)

#106#s  1,2,72,68024448    2**(2**n-1)*3**(3**n-2*2**n+1)
#106#f  (012 001 000) (012 112 222)
#106#d  complemented semigroup; quasiprimal algebra
#106#d  Lukasiewicz fragment: implication, disjunction
#106#r  Bosbach(1969), Csakany & Gavalcova(1982)
#106#f  (012 001 000) (012 101 210)
#106#d  Lukasiewicz fragment: implication, equivalence
#106#r  Lukasiewicz(1920)
#106#f  (012 101 210) (012 112 222)
#106#d  Lukasiewicz fragment: equivalence, conjunction

#107#s  1,3,5,7,9          2n+1
#107#f  (001)
#107#d  1-unary: 3-chain
#107#f  (000) (001)
```

#107#d 2-unary: constant function, 3-chain
#107#f1 (000) (002)
#107#d1 2-unary: constant function, 2-chain with fixed point
#107#f1 (000) (011)
#107#d1 2-unary: constant function, 2-chain with fixed point
#107#f2 (000) (021)
#107#d2 2-unary: constant function, 2-cycle with fixed point

#108#s 1,3,6,10,15 C(n+2,2)
#108#f (000 000 001)
#108#d semigroup: has zero, xyz=rst
#108#d variety does not have definable principal congruence relations
#108#r Evans(1971) p. 31, Moraga(1975), Harrop(1976), Taylor(1977)

#109#s 1,3,6,11,20 n+2**n
#109#f (011 100 100)
#109#d semigroup: analog of Boolean group; equivalence operation
#109#r Salomaa(1959), p.136, Wesselkamper(1974)
#109#f (002 002 220)
#109#d semigroup: analog of Boolean group
#109#r Rescher(1969) p.336

#110#s 1,3,7,15,31 2**(n+1) - 1
#110#f (111) (000 011 012)
#110#d semilattice with generic constant

#111#s 1,3,8,20,48 1 + #039#
#111#f (000 000 111)
#111#d groupoid: has 0
#111#r Gutierrez & Moraga(1974), also see #039#r

#112#s 1,3,8,41,946 n + #095#
#112#f (000 000 220)
#112#d groupoid: analog of implication
#112#r Reichenbach(1944), Salomaa(1959), Rescher(1969) p.336, Bandler & Kohout(1979)

#113#s 1,3,9,26,72 (n**2+3n+8)2**(n-3)
#113#f (000 001 011)
#113#d groupoid: has zero
#113#r Klein-Barmen(1953), Moraga(1975)

#114#s 1,3,9,27,81 3**n
#114#f (000 020 001)
#114#d groupoid: has zero
#114#r Baker(1981)*
#114#f (021) (000 010 002)
#114#d involutory semigroup; fragment of Hanson threshold logic
#114#r Hanson(1963), Fajtlowicz(1972)
#114#f1 (012 120 201)
#114#d1 group: Z3
#114#f1 (021 102 210)
#114#d1 groupoid: quasigroup, x + 2y (mod 3)
#114#r1 Bernstein(1924), Clark & Krauss(1980)
#114#f1 (000 000 000) (012 120 201)
#114#d1 ring: trivial multiplication

#115#s 1,3,10,32,96 (n**2+n+4)*2**(n-2)
#115#f (000 001 111)
#115#d leader threshold function
#115#r Gutierrez & Moraga(1974)

```
#116#s  1,3,10,41,282            sum i=1 to n (C(n,i)*#093#)
#116#f  (111) (000 011 012)
#116#d  distributive quasilattices with non zero constant adjoined

#117#s  1,3,10,131,32772      n + 2**(2**n-1)
#117#f  (000 000 002) (002 002 220)
#117#d  analog of Boolean ring
#117#r  Rescher(1969) p.336

#118#s  1,3,12,59,354
#118#f  (000 000 100)
#118#d  groupoid

#119#s  1,3,13,68,420
#119#f  (001 000 100)
#119#d  groupoid: commutative

#120#s  1,3,13,159  sum i=0 to n (C(n,i)*2**(2**i-1)) (?)
#120#f  (000 012 021) (100 011 011)
#120#d  two commutative semigroups
#120#r  Wesselkamper(1974)

#121#s  1,3,15,273
#121#f  (111) (000 012 020) (012 111 212)
#121#d  Conway's Kleene algebras
#121#r  Conway(1971)

#122#s  1,3,15,531487   (n+1)st term #004#
#122#f  (000) (002 011 212)
#122#d  adjoin generic constant to upper bound algebra

#123#s  1,3,16
#123#f  (000 000 200)
#123#d  groupoid
#123#r  Gutierrez & Moraga(1974), Anderson & Belnap(1975) p. 85

#124#s  1,3,19,1120     1 + #059#
#124#f  (000) (000 110 210)
#124#d  Kleene fragment: implication with  T  as constant

#125#s  1,3,23    1 + #061#
#125#f  (000) (012 111 210) (012 112 222)
#125#d  Kleene fragment: equivalence, conjunction, T as constant

#126#s  1,3,26    1 + #062#
#126#f  (000) (000 011 012) (012 111 210)
#126#d  Kleene fragment: equivalence, disjunction, T as constant

#127#s  1,3,28,796
#127#f  (001 000 000) (012 012 102)
#127#d  system used to show independence of field axioms
#127#r  Bernstein(1921)

#128#s  1,3,42
#128#f  (012 102 221)
#128#d  groupoid: has unit

#129#s  1,3,81,1594323   3**((3**n-1)/2)
#129#f  (012 220 101)
#129#d  groupoid: used in independence proof of axioms for Sheffer stroke
#129#r  Sheffer(1912)
#129#f  (210) (001 012 122)
```

#129#d fragment of Hanson threshold logic
#129#r Hanson(1963)
#129#f (120 201 012) (200 121 222)
#129#d complemented semigroup; quasiprimal algebra
#129#r Bosbach(1969), Csakany & Gavalcova(1982)

#130#s 1,3,81,2539107 one-half of #187#s
#130#f (000 011 012) (000 021 012) (012 100 200)
#130#d maximal subclone of #187#
#130#r Raca(1969)

#131#s 1,4,7,10,13 3n+1
#131#f (001) (002)
#131#d 2-unary: 3-chain, 2-chain with fixed point
#131#f1 (001) (010)
#131#d1 2-unary: 3-chain, 2-chain with fixed point
#131#f1 (001) (011)
#131#d1 2-unary: 3-chain, 2-chain with fixed point
#131#f2 (002) (010)
#131#d2 2-unary: two 2-chain with fixed point

#132#s 1,4,12,39,140
#132#f (010 121 010)
#132#d groupoid
#132#r Thelliez(1973), Wojciechowski & Wojcik(1979)

#133#s 1,4,17,72
#133#f (000 000 021)
#133#d groupoid: has zero

#134#s 1,4,18,166,7579 (n+1)st term of #008#
#134#f (111) (000 011 012) (012 112 222)
#134#d distributive lattice with one generic constant

#135#s 1,4,21,129, 991(?)
#135#f (000 001 022) (000 012 000) (000 000 012)
#135#d Murskii algebra with local discriminator operators
#135#r Pigozzi(1979)

#136#s 1,4,27,336
#136#f (000 001 021)
#136#d groupoid: has zero

#137#s 1,4,28
#137#f (000 002 021)
#137#d groupoid: has zero

#138#s 1,4,35
#138#f (002 002 100)
#138#d groupoid: leader for family of threshold functions
#138#r Gutierrez & Moraga(1974)

#139#s 1,4,49
#139#f (100 110 111)
#139#d groupoid: implication
#139#r Bernstein(1924), Turquette(1966), Biela(1975)

#140#s 1,4,56
#140#f (111) (000 011 012) (012 111 210)
#140#d Kleene fragment: equivalence, disjunction, U as consta
#140#r Kleene(1952) p.334

#141#s 1,4,64
#141#f (012 102 000)
#141#d implication
#141#r Goddard & Routley(1973) p. 365

#142#s 1,4,144,5038848 (2**(2**n-1))*#103#
#142#f (000 021 012) (200 121 222)
#142#d complemented semigroup; maximal subclone of #187#
#142#r Bosbach(1969), Raca(1969)

#143#s 1,4,162,88219206 (n+1)st term of #012#
#143#f (000) (002 011 212) (010 112 022)
#143#d tournament with one generic constant
#143#r Fried & Gratzer(1973)

#144#s 1,4,245
#144#f (222 201 212)
#144#d Rescher's version of Post equivalence operation
#144#r Rescher(1969) p.53

#145#s 1,4,576,8707129344 2**(2*2**n-2)*3**(3**n-2*2**n+1)
#145#f (022) (022 212 222) (000 111 012) (210 021 012)
#145#d quasiprimal
#145#r Csakany & Gavalcova(1982)

#146#s 1,5,9,13,17 4n+1
#146#f (002) (011)
#146#d 2-unary: two 2-chain with fixed point
#146#f (002) (212)
#146#d 2-unary: two 2-chain wih fixed point

#147#s 1,5,34,515
#147#f (200 002 022)
#147#d groupoid
#147#r Wojtylak(1979)

#148#s 1,5,43
#148#f (111) (000 110 210)
#148#d Kleene fragment: implication with u as constant

#149#s 1,5,63
#149#f (111) (012 111 210) (012 112 222)
#149#d Kleene fragment: equivalence, conjunction, u as constant
#149#r Kleene(1952) p.332

#150#s 1,5,114
#150#d (000 200 220)
#150#d implication
#150#r Salomaa(1959), Thomas(1962), Goddard & Routley(1973) p.320
#150#r Meyer & Parks(1972), Epstein(1976), Zakrzewska(1976)

#151#s 1,5,130 2**(3**n-2**n+n)+n (?)
#151#f (022 202 220)
#151#d groupoid: equivalence
#151#r Reichenbach(1944), Muehldorf(1960), Goddard & Routely(1973) p.318

#152#s 1,5,136
#152#f (222 020 002)
#152#d groupoid: implication
#152#r Anderson & Belnap(1975) p. 40

```
#153#s   1,5,154
#153#f   (110 010 000)
#153#d   groupoid; adjoin invisible element to implication
#153#r   Wajsberg(1937)

#154#s   1,6,11,16,21       5n+1
#154#f   (001) (020)
#154#d   2-unary:  two 3-chains
#154#f1  (001) (022)
#154#d1  2-unary: 3-chain, 2-chain with fixed point

#155#s   1,6,408
#155#f   (000 100 201)
#155#d   groupoid
#155#r   Rose(1961)

#156#s   1,6,480
#156#f   (022 001 000)
#156#d   implication
#156#r   Rescher(1969) p.135
#156#f   (022 001 020)

#157#s   1,6,594
#157#f   (022 001 010)
#157#d   implication
#157#r   Rescher(1969) p.135

#158#s   1,6,768
#158#f   (001 100 201)
#158#d   groupoid used to show independence of Sheffer axioms
#158#r   Dines(1915), Taylor(1920)

#159#s   1,6,1944     2**(2**n-1)*3**(3**n-2**n)
#159#f   (000 100 210) (012 122 222)
#159#d   complemented semigroup; quasiprimal
#159#r   Bosbach(1969), Werner(1978)

#160#s   1,7,13,19,25       6n+1
#160#f   (001) (021)
#160#d   2-unary: 3-chain, 2-cycle with fixed point
#160#f   (002) (021)
#160#d   2-unary: 2-chain with fixed point, 2-cycle with fixed point

#161#s   1,7,57
#161#f   (000 020 011)
#161#d   groupoid: has zero

#162#s   1,7,241
#162#f   (021 000 021)
#162#d   groupoid almost generating maximal clone
#162#r   Jablonskii(1958) p. 111

#163#s   1,9,161
#163#f   (102) (222) (012 111 222)
#163#d   Zaslavskii system without all the constants specified
#163#r   Zaslavskii(1979)

#164#s   1,9,6561,2541865828329  3**(3**n-1)
#164#f   (000 012 021) (012 120 201)
#164#d   ring:  addition and multiplication (mod 3); maximal clone; quasiprimal
#164#f   (012 202 121)
#164#d   groupoid: used for complete independence proof
```

```
#164#r  Dines(1915), Taylor(1920)
#164#f  (201 201 202)
#164#r  Carvallo(1968) p. 49

#165#s  2,3,4,5,6        n+2
#165#f  (000) (111)
#165#d  2-unary: two constant functions

#166#s  2,3,5,9,17        1+2**n
#166#f  (000) (222) (000 011 012)
#166#d  semilattice with zero and unit as constants

#167#s  2,3,6,20,168        2+#008#
#167#f  (000) (222) (000 011 012) (012 112 222)
#167#d  bounded distributive lattice: zero and unit as constants
#167#r  Balbes & Dwinger(1974)

#168#s  2,4,6,8,10        2n+2
#168#f  (000) (102)
#168#d  2-unary: constant, 2-cycle with fixed point
#168#f1 (000) (110)
#168#d1 2-unary: constant, 3-chain
#168#f2 (000) (112)
#168#d2 2-unary: constant, 2-chain with fixed point

#169#s  2,4,8,16,32        2**(n+1)
#169#f  (000) (111) (000 011 012)
#169#d  semilattice: has zero as constant and generic constant
#169#f1 (111) (222) (000 011 012)
#169#d1 semilattice: has unit as constant and generic constant

#170#s  2,5,8,11,14        3n+2
#170#f  (000) (100)
#170#d  2-unary: constant, 2-cycle with tail
#170#f  (000) (101)
#170#d  2-unary: constant, 2-cycle with tail
#170#f1 (001) (110)
#170#d1 2-unary: two 3-chains
#170#f2 (001) (112)
#170#d2 2-unary: 3-chain, 2-chain with fixed point

#171#s  2,5,10,19,36        n+2**(n+1)
#171#f  (220) (002 002 220)
#171#d  analog of complemented Boolean group
#171#r  Rescher(1969) p.336

#172#s  2,5,14,49,298        sum i=0 to n (C(n,i)*#167#)
#172#f  (111) (222) (000 011 012) (000 012 022)
#172#d  distributive quasilattices with two non-zero constants

#173#s  2,5,18,259,65540        n+2**(2**n)
#173#f  (220) (002 002 222)
#173#d  analog of negation and disjunction
#173#r  Church(1953), Smiley(1962), Rescher(1969) p.336

#174#s  2,5,19,167,7580        1 + (n+1)st term of #008#
#174#f  (000) (111) (000 011 012) (012 112 222)
#174#d  distributive lattice: with zero constant and generic constant

#175#s  2,5,22,983(?)
#175#f  (000) (222) (022 222 222) (000 000 002)
#175#d  monotonic for 3-element chain with 2-element range
```

```
#176#s  2,5,23,311,66659    1+sum i=0 to n (C(n,i)*2**(2**i) - 1)
#176#f  (200) (000 011 012)
#176#d  pseudocomplemented semilattice
#176#r  Jones(1972)*, Balbes(1973)*, Jones(1974), Taylor(1976)

#177#s  2,5,105
#177#f  (000) (212) (012 112 222) (000 021 012)
#177#d  maximal subclone of #187#
#177#r  Raca(1969)

#178#s  2,6,10,14 18      4n+2
#178#f  (002) (101)
#178#d  2-unary: 2-chain with fixed point, 2-cycle with tail
#178#f  (001) (102)
#178#d  2-unary: 3-chain, 2-cycle with fixed point

#179#s  2,6,26,318,66674       sum i=0 to n (C(n,i)*2**(2**i))
#179#f  (222) (000 011 021)
#179#d  Bochvar system with two nonzero constants adjoined

#180#s  2,6,45
#180#f  (111) (012 101 210)
#180#d  Lukasiewicz fragment: equivalence with Slupecki constant
#180#r  Slupecki(1936)
#180#f  (220) (012 102 220)
#180#d  Heyting fragment: equivalence, negation

#181#s  2,6,50
#181#f  (200) (012 112 222)
#181#d  Heyting fragment:  disjunction, negation

#182#s  2,6,70
#182#f  (200) (222 022 012)
#182#d  Heyting fragment:  implication, negation
#182#r  McCall(1962)*, Horn(1962)

#183#s  2,6,84
#183#f  (210) (012 101 210)
#183#d  Lukasiewicz fragment: equivalence and negation
#183#f  (111) (012 102 220)
#183#d  Heyting fragment: equivalence, 1 as constant
#183#d  compare #184#;  not congruence distributive

#184#s  2,6,84,43918,160297985276      2+#084#
#184#f  (000) (222) (210) (000 011 012)
#184#d  Kleene algebra with two constants; compare #183#

#185#s  2,6,90,60750  product i=0 to n ((1+2**i)**C(n,i))
#185#f  (200) (212) (000 021 012)
#185#d  maximal subclone of #187#
#185#r  Raca(1969)

#186#s  2,6,108,233280  product i=0 to n (i-th term #167#**C(n,i))
#186#f  (200) (000 011 012) (012 112 222)
#186#d  pseudocomplemented lattice; Stone lattice
#186#d  Heyting fragment: conjunction, disjunction, negation
#186#r  Balbes & Horn(1970)*, Gratzer(1971)*, Balbes & Dwinger(1974)*

#187#s  2,6,162,5078214  #103#*(2**(2**n-1)+1)
#187#f  (000) (000 011 012) (222 022 012)
#187#d  Heyting system: implication, conjunction, F as constant
#187#f  (000) (000 011 012) (012 112 222) (222 022 012)
```

#187#d Heyting algebra; L-algebra; pseudo Boolean algebra
#187#r Heyting(1930), Godel(1932), Birkhoff(1940), Rasiowa & Sikorski(1963)
#187#r Raca(1966), Raca(1969)*, Horn(1969)*, Kohler(1973)*, Monteiro(1972)*,
#187#r Balbes & Dwinger(1974), Kohler(1975)*, Davey(1976)*

#188#s 2,7,12,17,22 5n+2
#188#f (001) (100)
#188#d 2-unary: 3-chain, 2-cycle with tail
#188#f (001) (101)
#188#d 2-unary: 3-chain, 2-cycle with tail

#189#s 2,8,14,20,26 6n+2
#189#f (002) (100)
#189#d 2-unary: 2-chain with fixed point, 2-cycle with tail

#190#s 2,9,16,23,30 7n+2
#190#f (002) (020) (200)
#190#d 3-unary: three peak functions
#190#r Rosser & Turquette(1945), Rosenberg(1976) p.11

#191#s 2,9,514,134217731 n + 2**(3**n)
#191#f (100) (110 010 000)
#191#d implicational logic; adjoin invisible element to implication and negation
#191#r Wajsberg(1937)
#191#f (101) (110 010 110)
#191#d variant of implicational logic
#191#r Wajsberg(1937), Zakrzewska(1976)

#192#s 2,9, >1000
#192#f (000) (111) (002 011 212) (010 112 022)
#192#d tournament: two elements as constants
#192#r Fried & Gratzer(1973)

#193#s 2,10,18,26,34 2+8n
#193#f (022) (202) (220) (210)
#193#d 3 peaks and negation function
#193#r Rosser & Turquette(1945)

#194#s 2,10,516
#194#f (102) (000 011 011)
#194#d negation and implication used in independence proof
#194#r Bernays(1926), Meredith(1953)

#195#s 2,10,562
#195#f (101) (000 011 012) (012 112 222)
#195#d distributive lattice with additional unary operation
#195#r Kollar(1980)

#196#s 2,10,622
#196#f (101) (000 012 012)
#196#d negation and implication used in independence proof
#196#r Bernays(1926)
#196#f (022) (202) (220) (012 002 000)
#196#d example of implication with Rosser & Turquette J functions
#196#r Shoesmith & Smiley(1978) p. 358
#196#f (002) (022) (200) (012 000 000)
#196#d matrix used for independence proof in modal logic
#196#r Lukasiewicz(1953), attributed to C. A. Meredith

#197#s 2,10,626
#197#f (200) (220) (000 011 012)
#197#d semilattice with pseudocomplement and dual pseudocomplement

#197#f (002) (020) (200) (000 011 012)
#197#r fragment Muehldorf system as in Rosenberg(1976) p.12

#198#s 2,10,642
#198#f (100) (000 012 222)
#198#d negation and implication used in independence proof
#198#r Bernays(1926)

#199#s 2,10,808
#199#f (111) (012 001 000)
#199#d Lukasiewicz implication with Slupecki constant
#199#r Slupecki(1936)

#200#s 2,12,656
#200#f (102) (011 000 000) (012 112 222)
#200#d logical system similar to Bochvar system
#200#r Pirog-Rzepcka(1973)
#200#f (002) (020) (200) (210) (012 111 212)
#200#d logical system similar to Bochvar system
#200#r Finn & Grigolija(1979)

#201#s 2,12,3888,297538935552 (2**(2**n))*(3**(3**n-2**n))
#201#f (000) (222) (210 121 012) (222 122 012)
#201#d Lukasiewicz system: implication, equivalence, two constants
#201#d maximal clone, quasiprimal
#201#r Lukasiewicz(1920)
#201#f (210) (012 001 000)
#201#d Lukasiewicz system: negation, implication as primitive
#201#d implicaton = max(0,x-y), negation = 2-x
#201#r Slupecki(1936)
#201#f (210 100 000)
#201#d Sheffer stroke for Lukasiewicz algebra
#201#r McKinsey(1936), Evans & Hardy(1957)
#201#f (111) (222 022 012) (000 011 012)
#201#d Heyting fragment: implication, conjunction, 1 as constant
#201#f (000) (210) (002) (022) (000 011 012) (012 112 222)
#201#d Lukasiewicz algebra, Moisil algebra
#201#r Moisil(1940), Cignoli(1970)*, Balbes & Dwinger(1974)*
#201#f (102) (000 012 020)
#201#d negation and implication used in indpendence proof
#201#r Bernays(1926)
#201#f (210) (022 002 000) (000 011 012)
#201#d Chang MV algebra
#201#r Chang(1958)
#201#f (001) (102) (012 111 222)
#201#d EFC system for recursively defined predicates
#201#r McCarthy(1963)
#201#f (011) (102) (000 012 022)
#201#d Aqvist logic of nonsense
#201#r Aqvist(1962)
#201#f (002) (020) (200) (000 011 012) (012 112 222)
#201#d max, min, three peak functions
#201#r Rosser & Turquette(1945), Rosenberg(1976) p.11
#201#f (200) (220) (000 011 012) (012 112 222)
#201#d regular double Stone algebra
#201#r Varlet(1972), Katrinak(1974), Hecht & Katrinak(1974)*
#201#f (200) (220) (210) (000 011 012)
#201#d pseudocomplemented Kleene algebra
#201#r Romanowska(1981)
#201#f (000) (222) (000 011 012) (012 112 222) (222 022 002)
#201#d P-algebra
#201#r Epstein & Horn(1974)

```
#202#s  3,5,7,9,11          2n+3
#202#f  (000) (122)
#202#d  2-unary: constant, 3-chain

#203#s  3,5,9,17,33         1+2**(n+1)
#203#f  (000) (111) (222) (000 011 012)
#203#d  semilattice: all three constants adjoined

#204#s  3,6,9,12,15         3n+3
#204#f  (000) (120)
#204#d  2-unary:  constant, 3-cycle
#204#f1 (000) (121)
#204#d1 2-unary: constant, 2-cycle with tail

#205#s  3,6,12,24,48      3*2**n
#205#f  (111) (222) (000 010 002)
#205#d  semilattice:  has two constants

#206#s  3,6,20,168,7581       2+(n+1)st term of #008#
#206#f  (000) (111) (222) (000 011 012) (012 112 222)
#206#d  distributive lattice: all three constants named

#207#s  3,8,13,18,23           5n+3
#207#f  (100) (221)
#207#d  2-unary:  two 2-cycle with tail
#207#f1 (001) (221)
#207#d1 2-unary:  3-chain, 2-cycle with tail
#207#f1 (001) (220)
#207#d1 2-unary: 3-chain, 2-cycle with tail

#208#s  3,8,29,141
#208#f  (000) (111) (222) (000 001 0?2)
#208#d  Murski groupoid with all constants adjoined
#208#r  Pigozzi(1979)

#209#s  3,8,38,566      #176# + 2**(2**n)-1  (?)
#209#f  (111) (200) (000 011 012)
#209#d  Heyting fragment: conjunction, negation, all constants
#209#d  pseudocomplemented semilattice with all constants

#210#s  3,8,52
#210#f  (000) (111) (222) (100) (221) (000 011 012) (012 112 222)
#210#d  N-Boolean algebra
#210#r  Schmidt(1972)

#211#s  3,9,15,21,27           6n+3
#211#f  (002) (121)
#211#d  2-unary: 2-chain with fixed point, 2-cycle with tail
#211#f1 (000) (021) (120)
#211#d1 3-unary:  all permutations and constants

#212#s  3,9,27,81,243    3**(n+1)
#212#f  (111) (012 120 201)
#212#d  group Z3 with all constants named; maximal clone
#212#r  Jablonskii(1958), Clark & Krauss(1980)

#213#s  3,9,40,569
#213#f  (000 010 000) (222 222 221)
#213#d  analog of semilattice and analog of Sheffer stroke

#214#s  3,10,17,24,31          7n+3
#214#f  (100) (121)
```

```
#214#d  2-unary: two 2-cycle with tail
#214#f  (100) (220)
#214#d  2-unary: two 2-cycle with tail
#214#f1 (002) (020) (200) (111)
#214#d1 4-unary: three peaks and constant

#215#s  3,10,45,248
#215#f  (000) (111) (222) (000 001 022) (000 012 000) (000 000 012)
#215#d  Murski algebra with constants and local discriminators
#215#r  Pigozzi(1979)

#216#s  3,10,46,244
#216#f  (001) (002) (022) (111) (012 112 222)
#216#d  maximal subclone of monotonic functions #220#
#216#r  Machida(1979)

#217#s  3,10,59
#217#f  (001) (111) (112) (022 222 222) (000 000 002)
#217#d  maximal subclone of monotonic functions #220#
#217#d  intersection of clone #220# and #234#
#217#r  Kolpakov(1974), Machida(1979)

#218#s  3,10,83    n+3**(2**n) (?)
#218#f  (211 100 100)
#218#d  groupoid with large s(1)
#218#r  Foxley(1962), Muzio(1971)

#219#s  3,10,88
#219#f  (111) (200) (012 112 222)
#219#d  Heyting fragment: disjunction, negation, all constants

#220#s  3,10,175
#220#f  (111) (002) (022) (000 011 012) (012 112 222)
#220#d  maximal clone: monotonic functions
#220#r  Jablonskii(1958), Alexseev(1974)*, Schweigert(1979), Epstein & Liu(1982)

#221#s  3,11,163    2 + #163#
#221#f  (102) (111) (222) (012 111 222)
#221#r  Zaslavskii(1979)

#222#s  3,11,197,129615,430904428717
#222#f  (000) (111) (222) (210) (000 011 012)
#222#d  Fragment of Slupecki variant of Łukasiewicz system; Regular functions
#222#r  Kleene(1952) p.332, Berman & Mukaidono(1982)*

#223#s  3,12,21,30,39        9n+3
#223#f  (001) (200)
#223#d  2-unary: 3-chain, 2-cycle with tail
#223#f  (001) (121)
#223#d  2-unary: 3-chain, 2-cycle with tail
#223#f  (001) (212)
#223#d  2-unary: 3-chain, 2-chain with fixed point
#223#f1 (001) (211)
#223#d1 2-unary: two 3-chains
#223#f1 (001) (202)
#223#d1 2-unary: two 3-chains

#224#s  3,12,207
#224#f  (112 200 200)
#224#d  groupoid with large s(1)
#224#r  Muzio(1971)
```

#225#s 3,13,23,33,43 10n+3
#225#f (001) (210)
#225#d 2-unary: 3-chain, 2-cycle with fixed point
#225#f (021) (101)
#225#d 2-unary: 2-cycle with fixed point, 2-cycle with tail

#226#s 3,15,333
#226#f (121 100 100)
#226#d groupoid
#226#r Foxley(1962), Muzio(1971), Rose(1979)

#227#s 3,15,369
#227#f (111) (210) (012 101 210)
#227#d equivalence and negation in Lukasiewicz system with Slupecki constant
#227#f (111) (220) (012 102 220)
#227#d Heyting fragment: equivalence, negation, all constants

#228#s 3,15,525
#228#f (121 200 100)
#228#d groupoid with large s(1)
#228#r Muzio(1971)

#229#s 3,15,2275,473490375 product i=0 to n ((1+2**(2**i))**C(n,i))
#229#f (000) (111) (000 011 012) (222 022 012)
#229#d Heyting fragment: implication, conjunction, all truth values
#229#d Heyting algebra with all constants; maximal clone
#229#r Jablonskii(1958), McKenzie(1982)*, Demetrovics & Hannak & Ronyai(1982)*
#229#f (000) (112) (000 011 012) (222 022 012)
#229#d Heyting algebra with modal operator
#229#r Mcnab(1981)
#229#f (000) (122) (000 011 012) (222 022 012)
#229#d Heyting algebra with additional unary operation
#229#r Ursini(1979)

#230#s 3,17,1361
#230#f (222) (021 000 021) (001 020 100)
#230#d maximal clone: preserves central relation
#230#r Jablonskii(1958), Lau(1980), Demetrovics & Hannak & Ronyai(1982)*

#231#s 3,24,45,66,87 21n+3
#231#f (001) (120)
#231#d 2-unary: 3-chain, 3-cycle
#231#f (002) (120)
#231#d 2-unary: 2-chain with fixed point, 3-cycle
#231#f (100) (120)
#231#d 2-unary: 2-cycle with tail, 3-cycle

#232#s 3,27,51,75,99 24n+3
#232#f (001) (021) (120)
#232#d all unary operations
#232#r Picard(1935)

#233#s 3,27,105,399,1557 3*2**(2*n+1) + 6*n - 3
#233#f (120) (021) (001 001 110)
#233#d clone of quasilinear functions, maximal subclone of #234#
#233#r Burle(1967), Malcev(1972), Malcev(1973)
#233#r Rosenberg & Szendrei(1981), Berman & McKenzie(1982)*

#234#s 3,27,1545 3*2**(3**n) + 6*n - 3
#234#f (001) (021) (120) (011 111 111)
#234#d all unary and all non-onto n-ary operations; maximal clone
#234#r Jablonskii(1958), Burle(1967)

#235#s 3,27,19683,7625597484987 3**(3**n)
#235#f (201) (012 112 222)
#235#d Post system of 3-valued logic: negation, disjunction as primitive
#235#r Post(1921)
#235#f (121 222 120)
#235#d groupoid: commutative, min{x,y}+1 (mod 3)
#235#r Webb(1936)
#235#f (111) (210) (012 001 000)
#235#d Slupecki variant of Lukasiewicz system
#235#r Slupecki(1936)
#235#f (111) (000 012 021) (012 120 201)
#235#d ring of integers mod 3 with all constants; field GF(3)
#235#f (221 201 111)
#235#d Rescher's version of Post conjunction
#235#r Rescher(1969) p.53
#235#f (002) (200) (220) (022) (000 011 012) (012 112 222)
#235#r Yoeli & Rosenfeld(1965)
#235#f (000) (111) (222) (210) (022) (002) (000 011 012) (012 112 222)
#235#d Post algebra
#235#r Cignoli(1970)*, Dwinger(1972)*, Balbes & Dwinger(1974)*

INDEX OF BINARY OPERATIONS

The minimal member of isomorphism/anti-isomorphism class is given.

(000 011 012)	#002# #008# #015# #017# #018# #020# #022# #026# #027# #034# #041# #050# #051# #052# #054# #057# #061# #062# #065# #079# #082# #084# #086# #090# #093# #097# #102# #103# #106# #110# #116# #121# #125# #126# #130# #134# #140# #149# #166# #167# #169# #172# #174# #176# #177# #181# #184# #186# #187# #195# #197# #200# #201# #203# #206# #209# #210# #216# #219# #220# #222# #229# #235#
(000 011 021)	#046# #179#
(000 011 022)	#005# #024# #055# #196#
(000 011 102)	#030#
(000 011 212)	#011#
(000 011 222)	#007#
(000 012 021)	#043# #052# #061# #062# #078# #081# #120# #125# #126# #130# #140# #142# #149# #164# #177# #185# #235#
(000 012 111)	#058#
(000 012 122)	#023#
(000 012 212)	#021#
(000 012 220)	#063#
(000 012 222)	#006# #024# #083# #104# #145# #163# #198# #201# #221#
(000 020 001)	#114#
(000 020 011)	#161#
(000 021 011)	#082#
(000 021 021)	#042#
(000 021 222)	#053#
(000 022 112)	#065#
(000 100 100)	#200#
(000 100 111)	#191#
(000 100 200)	#098# #196#
(000 100 201)	#155#
(000 100 210)	#105# #106# #159# #199# #201# #235#
(000 100 220)	#101# #102# #103# #182# #187# #196# #201# #229#
(000 101 100)	#201#
(000 101 102)	#064# #085# #086#
(000 101 210)	#105#
(000 101 220)	#095# #129# #142#
(000 102 100)	#156#
(000 102 110)	#156#
(000 102 120)	#157#
(000 102 202)	#059# #124# #148#
(000 110 120)	#075#
(000 110 202)	#009#
(000 110 222)	#005#
(000 111 102)	#016#
(000 111 222)	#001#
(000 112 212)	#010#
(000 202 101)	#162# #230#
(000 211 122)	#005# #074# #127#
(001 000 100)	#119#
(001 000 220)	#138#
(001 001 110)	#233#
(001 010 102)	#031#
(001 011 111)	#045# #049#
(001 011 112)	#019#
(001 011 120)	#076#
(001 012 120)	#077#
(001 012 121)	#063#
(001 012 122)	#014# #025# #078# #129#
(001 020 100)	#230#
(001 021 111)	#084#
(001 100 201)	#158#
(001 101 000)	#139#
(001 101 100)	#152#
(001 101 111)	#153# #191#
(001 110 012)	#029#

(001 201 201) #156#
(001 210 122) #033#
(001 212 011) #065#
(002 000 201) #144#
(002 002 220) #109# #117# #120# #171#
(002 002 221) #132#
(002 011 212) #004# #012# #028# #072# #122# #143# #192#
(002 012 220) #043#
(002 012 221) #056#
(002 022 220) #147#
(002 101 200) #141#
(011 100 100) #109#
(011 101 110) #151#
(012 100 200) #096# #130#
(012 101 210) #099# #106# #180# #183# #201# #227#
(012 101 220) #100# #104# #145#
(012 102 221) #128#
(012 120 201) #114# #129# #164# #212# #235#
(012 121 211) #085#
(012 121 221) #060#
(012 201 120) #114#
(012 202 121) #156#
(012 220 101) #129#
(021 210 102) #003# #028# #034# #079#
(100 000 000) #213#
(101 020 101) #218#
(101 020 121) #224#
(101 021 111) #201#
(101 200 101) #226#
(101 221 200) #072#
(102 021 210) #068#
(111 120 100) #235#
(121 200 100) #228#

TABLE OF p(n) SEQUENCES

Table of number of essentially n-ary operations for n=0,1,2,3,4. If fewer than five values are given it is because the values are too large to print or are unknown

#001#p	0 1 0 0 0
#002#p	0 1 1 1 1
#003#p	0 1 1 3 5
#004#p	0 1 1 9 531441
#005#p	0 1 2 3 4
#006#p	0 1 2 6 24
#007#p	0 1 2 9 88
#008#p	0 1 2 9 114
#009#p	0 1 2 21
#010#p	0 1 2 27
#011#p	0 1 2 45
#012#p	0 1 2 153 88218578
#013#p	0 1 3 16
#014#p	0 1 3 84
#015#p	0 1 4 18 166
#016#p	0 1 4 24 192
#017#p	0 1 4 45 2159
#018#p	0 1 4 45
#019#p	0 1 4 74
#020#p	0 1 4 85
#021#p	0 1 4 168
#022#p	0 1 4 198
#023#p	0 1 5 487
#024#p	0 1 6 264
#025#p	0 1 6 310
#026#p	0 1 7 105
#027#p	0 1 7 465
#028#p	0 1 7 6537
#029#p	0 1 8 384
#030#p	0 1 12
#031#p	0 1 13
#032#p	0 1 14
#033#p	0 1 25 531363
#034#p	0 1 727 282429534297
#035#p	0 2 0 0 0
#036#p	0 2 1 1 1
#037#p	0 2 2 6 24
#038#p	0 2 2 9 114
#039#p	0 2 3 4 5
#040#p	0 2 3 7 15
#041#p	0 2 3 10 115
#042#p	0 2 4 6 8
#043#p	0 2 4 8 16
#044#p	0 2 4 17 112
#045#p	0 2 4 41
#046#p	0 2 6 38 942
#047#p	0 2 7 25 97
#048#p	0 2 7 37 325
#049#p	0 2 7 465
#050#p	0 2 8 84
#051#p	0 2 8 90
#052#p	0 2 8 128 32768
#053#p	0 2 8 144
#054#p	0 2 9 114
#055#p	0 2 9 141
#056#p	0 2 9 640
#057#p	0 2 10 236
#058#p	0 2 12 617
#059#p	0 2 14 1071
#060#p	0 2 16 768
#061#p	0 2 18
#062#p	0 2 21
#063#p	0 2 24
#064#p	0 2 56
#065#p	0 2 644 49589820654
#066#p	0 3 0 0 0
#067#p	0 3 2 2 2
#068#p	0 3 3 9 15
#069#p	0 3 5 15 52
#070#p	0 3 7 45
#071#p	0 3 18
#072#p	0 3 21 19611
#073#p	0 3 40
#074#p	0 3 62
#075#p	0 3 84
#076#p	0 3 132
#077#p	0 3 162
#078#p	0 3 426
#079#p	0 3 2181
#080#p	0 4 0 0 0
#081#p	0 4 8 16 32
#082#p	0 4 16 256 65536
#083#p	0 4 48
#084#p	0 4 74 43682 160297810086
#085#p	0 4 256
#086#p	0 4 1288 99179641308
#087#p	0 5 0 0 0
#088#p	0 6 0 0 0
#089#p	1 1 0 0 0
#090#p	1 1 1 1 1
#091#p	1 1 2 3 4
#092#p	1 1 2 6 14
#093#p	1 1 2 9 114
#094#p	1 1 3 6 10
#095#p	1 1 3 25 819
#096#p	1 1 3 39
#097#p	1 1 4 18 166
#098#p	1 1 4 30
#099#p	1 1 6 618
#100#p	1 1 9
#101#p	1 1 11
#102#p	1 1 13
#103#p	1 1 15 39317
#104#p	1 1 21 93245
#105#p	1 1 37
#106#p	1 1 69
#107#p	1 2 0 0 0
#108#p	1 2 1 0 0
#109#p	1 2 1 1 1
#110#p	1 2 2 2 2
#111#p	1 2 3 4 5
#112#p	1 2 3 25 819
#113#p	1 2 4 7 11
#114#p	1 2 4 8 16

#115#p 1 2 5 10 17
#116#p 1 2 5 19 167
#117#p 1 2 5 109 32297
#118#p 1 2 7 31 179
#119#p 1 2 8 37 215
#120#p 1 2 8 128
#121#p 1 2 10 236
#122#p 1 2 10 531450
#123#p 1 2 11
#124#p 1 2 14 1071
#125#p 1 2 18
#126#p 1 2 21
#127#p 1 2 23 720
#128#p 1 2 37
#129#p 1 2 76 1594088
#130#p 1 2 76 2538872
#131#p 1 3 0 0 0
#132#p 1 3 5 14 41
#133#p 1 3 10 32
#134#p 1 3 11 123 7008
#135#p 1 3 14 77
#136#p 1 3 20 266
#137#p 1 3 21
#138#p 1 3 28
#139#p 1 3 42
#140#p 1 3 49
#141#p 1 3 57
#142#p 1 3 137 5038427
#143#p 1 3 155 88218731
#144#p 1 3 238
#145#p 1 3 569 8707127627
#146#p 1 4 0 0 0
#147#p 1 4 25 427
#148#p 1 4 34
#149#p 1 4 54
#150#p 1 4 105
#151#p 1 4 121
#152#p 1 4 127
#153#p 1 4 145
#154#p 1 5 0 0 0
#155#p 1 5 397
#156#p 1 5 469
#157#p 1 5 583
#158#p 1 5 757
#159#p 1 5 1933
#160#p 1 6 0 0 0
#161#p 1 6 44
#162#p 1 6 228
#163#p 1 8 144
#164#p 1 8 6544 2541865808672
#165#p 2 1 0 0 0
#166#p 2 1 1 1 1
#167#p 2 1 2 9 114
#168#p 2 2 0 0 0
#169#p 2 2 2 2 2
#170#p 2 3 0 0 0
#171#p 2 3 2 2 2
#172#p 2 3 6 20 168
#173#p 2 3 10 218 64594
#174#p 2 3 11 123 7008
#175#p 2 3 14 930
#176#p 2 3 15 255 65535
#177#p 2 3 97
#178#p 2 4 0 0
#179#p 2 4 16 256 65536
#180#p 2 4 35
#181#p 2 4 40
#182#p 2 4 60
#183#p 2 4 74
#184#p 2 4 74 43682 160297810086
#185#p 2 4 80 60496
#186#p 2 4 98 232972
#187#p 2 4 152 5077744
#188#p 2 5 0 0 0
#189#p 2 6 0 0 0
#190#p 2 7 0 0 0
#191#p 2 7 498 134216214
#192#p 2 7
#193#p 2 8 0 0 0
#194#p 2 8 498
#195#p 2 8 544
#196#p 2 8 604
#197#p 2 8 608
#198#p 2 8 624
#199#p 2 8 790
#200#p 2 10 634
#201#p 2 10 3866 297538923922
#202#p 3 2 0 0 0
#203#p 3 2 2 2 2
#204#p 3 3 0 0 0
#205#p 3 3 3 3 3
#206#p 3 3 11 123 7008
#207#p 3 5 0 0 0
#208#p 3 5 16 75
#209#p 3 5 25 473
#210#p 3 5 39
#211#p 3 6 0 0 0
#212#p 3 6 12 24 48
#213#p 3 6 25 473
#214#p 3 7 0 0 0
#215#p 3 7 28 140
#216#p 3 7 29 133
#217#p 3 7 42
#218#p 3 7 66
#219#p 3 7 71
#220#p 3 7 158
#221#p 3 8 144
#222#p 3 8 178 129054 430903911398
#223#p 3 9 0 0 0
#224#p 3 9 186
#225#p 3 10 0 0 0
#226#p 3 12 306
#227#p 3 12 342
#228#p 3 12 498
#229#p 3 12 2248 473483592
#230#p 3 14 1330
#231#p 3 21 0 0 0
#232#p 3 24 0 0 0
#233#p 3 24 54 162 486
#234#p 3 24 1494
#235#p 3 24 19632 7625597426016

WORD INDEX

BIBLIOGRAPHY

The following abbreviations are used:

BSL - Polish Academy of Sciences. Institute of Philosphy and Sociology. Bulletin of the Section of Logic.
ISMVL - Proceedings of the International Symposium on Multiple-valued Logic.
MR - Mathematical Reviews.
NDJFL - Notre Dame Journal of Formal Logic
ZMLG - Zeitschrift fur Mathematische Logik und Grundlagen der Mathematik.

Alexseev, A. (1974), On the number of k-valued monotone functions, (in Russian), Problemy Kibernetiki 28, 5-24. #220#
Anderson, A.R. and Belnap, N.D. (1975), Entailment. The Logic of Relevance and necessity, Princeton University Press, Princeton, New Jersey. #123# #152#
Aqvist, L. (1962), Reflections on the logic of nonsense, Theoria 28, 138-157. #201#
Arnold, B.H. (1951), Distributive lattices with a third operation defined, Pacific J Math. 1, 33-41. #026#
Baker, K. (1981), Letter to J. Berman, August 1981. #039# #042# #092# #094# #114#
Balbes, R. (1973), On free pseudo-complemented and relatively pseudo-complemented semi-lattices, Fund. Math. 78, 119-131. #103# #176#
Balbes, R. and Dwinger, Ph. (1974), Distributive Lattices, Univ. of Missouri Press, Columbia, Mo. #084# #103# #167# #186# #187# #201# #235#
Balbes, R. and Horn, A. (1970), Injective and projective Heyting algebras, Trans. Amer. Math. Soc. 148, 549-559. #186#
Baldwin J.T. and Lachlan, A. (1973), On universal Horn classes categorical in some infinite power, Algebra Universalis 3, 98-111. #003#
Bandler, W. and Kohout, L. (1979), Application of fuzzy logic to computer protection structures, 9-th ISMVL, Bath, England, 200-207. #058# #112#
Belkin, V.P. (1977), Quasiidentities of certain finite algebras, (in Russian), Mat. Zametki 22, 335-338. Translated in Math. Notes 22 (1977), 676-678. #066#
Berman, J. (1980), Algebraic properties of k-valued logics, 10-th ISMVL, Evanston, Illinois, 195-204.
Berman, J. (1982), Varieties with log-linear free spectra, preprint.
Berman, J. and Kohler, P. (1976), Cardinalities of finite distributive lattices, Mitt. Math. Sem. Giessen 121, 103-124. #008#
Berman, J. and McKenzie, R. (1982), Clones with the term condition, preprint. #233#
Berman, J. and Mukaidono, M. (1981), Enumerating fuzzy switching functions and free Kleene algebras, preprint. #084# #222#
Berman, J. and Wolk, B. (1980), Free lattices in some small varieties, Algebra Universalis 10, 269-289.
Bernays, P. (1926), Axiomatische Untersuchung des Aussagen-Kalkuls der "Principia Mathematica", Math. Zeit. 25, 305-320. #194# #196# #198# #201#
Bernstein, B.A. (1921), On the complete independence of Hurwitz's postulates for abelian groups and fields, Annals of Math. 23, 313-316. #036# #074# #127#
Bernstein, B.A. (1924), Modular representations of finite algebras, Proc. International Congress Math., Toronto, vol. 1, 207-216. #114# #139#
Biela, A. (1975), Note on structural incompleteness of some modal propositional calculi, Reports Math. Logic 4, 3-6. #064# #139#
Bielecka-Holda, M. (1980), Independent bases for the consequence determined by non-degenerated distributive lattices, BSL 9, 141-144. #020#
Birkhoff, G. (1940), Lattice Theory, Amer. Math. Soc. Colloq. Pub. no. 25, New York. #187#
Birkhoff, G. (1967), Lattice Theory, 3-rd edition, Amer. Math. Soc. Colloq. Pub. no. 25, New York. #008#
Bochvar, D.A. (1939), On a 3-valued logical calculus and its application to the analysis of contradictions, (in Russian), Math. Sbornik 4, 287-308. Translated in Hist. Philos. Logic 2(1981), 87-112. #082#
Borkowski, L. (1970), editior, Jan Lukasiewicz Selected Works, North-Holland, Amsterdam.

Bosbach, B. (1969), Komplementare Halbgruppen, Fund. Math. 64, 257-287. #106# #129# #142# #159#

Brady, R. (1971), The consistency of the axioms of abstraction and extensionality in a three-valued logic, NDJFL 12, 447-453. #098#

Burle, G.A. (1967), The classes of k-valued logics containing all one variable functions, (in Russian), Diskret. Analiz 10, 3-7. MR 36, 1297. #233# #234#

Byrd, M. (1979), On Lukasiewiczian logics with several designated values, Logique et Analyse 22, 489-504. #099# #105#

Carvallo, M. (1968), Logique a trois valeurs, logique a seuil, Gauthier Villars, Paris. #164#

Chajda, I. (1980), Polynomially determined tolerances, Czech. Math. J. 30, 470-474. #043#

Chang, C.C. (1958), Algebraic analysis of many valued logics, Trans. Amer. Math. Soc. 88, 467-490. #043# #073# #099# #201#

Church, A. (1953), Non-normal truth-tables for the propositional calculus, Boletin de la Sociedad Matematica Mexicana 10, 41-52. #059# #082# #173#

Church, R. (1965), Enumeration by rank of the elements of the free distributive lattice with 7 generators, Notices Amer. Math. Soc. 12, 724. #008#

Cignoli, R. (1970), Moisil Algebras, Notas de Logica Matematica, No. 27, Universidad Nacional del Sur, Bahia Blanca. #201# #235#

Clark, D.M. and Krauss, P.H. (1976), Para primal algebras, Algebra Universalis 6, 165-192. #068#

Clark, D.M. and Krauss, P.H. (1980), Plain para primal algebras, Algebra Universalis 11, 365-388. #114# #212#

Cleave, J.P. (1980), Some remarks on the interpretation of 3-valued logics, Ratio 22, 52-60. #053# #058# #098#

Conway, J. (1971), Regular Algebra and Finite Machines, Chapman and Hall, London. #051# #121#

Croisot, R. (1951), Axiomatique des lattices distributives, Canad. J. Math. 3, 24-27. #024# #057#

Csakany, B. (1980), Homogeneous algebras are functionally complete, Algebra Universalis 11, 149-158. #003#

Csakany, B. (1982), Three-element groupoids with minimal clones, preprint. #004# #006# #007# #009# #011#

Csakany, B. and Gavalcova, T. (1982), Three-element quasi-primal algebras, Studia Sci. Math. Hungar., to appear. #028# #033# #065# #072# #079# #086# #104# #106# #129# #145#

Davey, B.A. (1976), Dualities for equational classes of Brouwerian algebras and Heyting algebras, Trans. Amer. Math. Soc. 221, 119-146. #085# #187#

Day, A. (1973), The congruence extension property and subdirectly irreducible algebras--an example, Algebra Universalis 3, 229-237. #005#

Demetrovics, J. and Hannak, L. and Marchenkov, S.S. (1980), Some remarks on the structure of P3, C. R. Math. Rep. Acad. Sci. Canada 2, 215-219. #004# #028#

Demetrovics, J. and Hannak, L. and Ronyai, L. (1982), On the free spectra of maximal clones, C.R. Math. Rep. Acad. Sci. Canada, to appear. #072# #229# #230#

Diego, A. (1965), Sobre Algebras de Hilbert, Notas de Logica Matematica No. 12, University Nacional del Sur, Bahia Blanca. #101# #105#

Dienes, P. (1949), On ternary logic, J. Symbolic Logic 14, 85-94. #038# #041#

Dienes, Z.P. (1949), On an implication function in many-valued systems of logic, J. Symbolic Logic 14, 95-97. #059#

Dines, L.L. (1915), Complete existential theory of Sheffer's postulates for Boolean algebras, BAMS 21, 183-188. #158# #164#

Dudek, J. and Romanowska, A. (1981), Bisemilattices with four essentially binary polynomials, preprint. #018# #020# #117#

Dunn, J.M. (1970), Algebraic completeness results for R-mingle, J. Symbolic Logic 35, 1-13. #064# #085#

Dwinger, Ph. (1972), Free Post algebras and coproducts of Post algebras, Bull. Acad. Polon. Sci. 20, 535-537. #235#

Epstein, G. (1976), Decisive Venn diagrams, 6-th ISMVL, Logan Utah, 142-149. #150#

Epstein, G. and Horn, A. (1974), P-algebras, an abstraction from Post algebras, Algebra Univesalis 4, 195-206. #201#

Epstein, G. and Liu, Y. (1982), Positive multiple-valued switching functions--an extension of Dedekind's problem, 12-th ISMVL, Paris, 248-252. #220#

Evans, T. (1962), Properties of algebras almost equivalent to identities, J. London Math. Soc. 37, 53-59. #029# #037#
Evans, T. (1971), The lattice of semigroup varieties, Semigroup Forum2, 1-43. #108#
Evans, T. and Hardy, L. (1957), Sheffer stroke functions in many-valued logics, Portugaliae Math. 16, 83-93. #201#
Fajtlowicz, S. (1972), Equationally complete semigroups with involution, Algebra Universalis 1, 356-358. #114#
Finn, V. and Grigolija, R. (1980), Bochvar's algebras and corresponding propositional calculi, BSL 9, 39-45. #200#
Fisher, M. (1961), A three valued calculus fot deontic logic, Theoria 27, 107-118. #085#
Foxley, E. (1962), The determination of all Sheffer functions in 3-valued logic, using a logical computer, NDJFL 3, 41-50. #072# #218# #226#
Fried, E. and Gratzer, G. (1973), A nonassociative extension of the class of distributive lattices, Pacific J. Math. 49, 59-78. #012# #143# #192#
Gabovich, E. Ya. (1976), Fully ordered semigroups and their applications, (in Russian), Uspekhi Mat. Nauk 31, 137-201. Translated in Russian Math. Surveys 31 (1976), 147-216. #027# #054#
Gerhard, J.A. (1971), The number of polynomials of idempotent semigroups, J. Algebra 18, 366-376. #005# #006#
Goddard, L. and Routley, R. (1973), The Logic of Significance and Context, Wiley, New York. #039# #082# #098# #141# #150# #151#
Godel, K. (1932), Zum intuitionistischen Aussagenkalkul, Anzeiger der Akademie der Wissenschaften Wien, Mathematisch, naturwissenschaftliche Klasse 69, 65-66. #187#
Goetz, A. (1966), On weak isomorphisms and weak homomorphisms of abstract algebras, Colloq. Math. 14, 163-167.
Gorbunov, A (1977), Covers in lattices of quasivarieties and independent axiomatizability, (in Russian), Algebra i Logika 16, 507-548. Translated Algebra and Logic 16, 340-369. #066#
Gratzer, G. (1970), Composition of functions, Proc. Conf. on Universal Algebra, Queens Univ., Kingston, Ontario, 1969, 1-106.
Gratzer, G. (1971), Lattice Theory. First Concepts and Distributive Lattices, W.H. Freeman and Co., San Francisco, California. #186#
Gratzer, G. (1979), Universal Algebra, 2-nd edition, Springer-Verlag, New York. #087#
Gratzer, G. and Padmanabhan, R. (1971), On idempotent, commutative, and nonassociative groupoids, Proc. Amer. Math. Soc. 28, 75-80. #003#
Gutierrez J. and Moraga, C. (1974), Multithreshold periodic ternary threshold logic, 4-th ISMVL, Morgantown, W. Virginia, 413-422. #019# #111# #115# #123# #138#
Hanson, W. (1963), Ternary threshold logic, IEEE Trans. on Computers EC-12, 191-197. #025# #114# #129#
Hardegree, G.M. (1981), Quasi-implication algebras, Part I: Elementary theory, Algebra Universalis 12, 30-47. #098#
Harrop, R. (1976), Some results concerning finite model separability of propositional calculi, Studia Logica 35, 179-189. #108#
Hecht, T. and Katrinak, T. (1972), Equational classes of relative stone algebras, NDJFL 13, 248-254. #103#
Hecht, T. and Katrinak, T. (1974), Free double Stone algebras, Colloq. Math. Soc. Janos Bolyai 14, Lattice Theory, 77-95. #201#
Heyting, A. (1930), Die Formalen Regeln der intuitionistischen Logik, Sitzungsberichte der Preussischen Akademie der Wissenschaften zu Berlin, 42-46. #187#
Horn, A. (1962), The separation theorem of intuitionist propositional calculus, J. Symbolic Logic 27, 391-399. #101#
Horn, A. (1969), Free L-algebras, J. Symbolic Logic 34, 475-480. #182# #187#
Hulanicki A. and Swierczkowski S. (1960), Number of algebras with a given set of elements, Bull. Acad. Polon. Sci. Ser. Sci. Math. Astronom. Phys. 8, 283-284.
Iseki, K. (1966), An algebra related with a propostional calculus, Proc. Japan Acad. 42, 26-29. #095# #101# #105#
Jablonskii, S.V. (1958), Functional constructions in k-valued logic, (in Russian), Trudy Mat. Inst. Steklov 51, 5-142. #072# #162# #212# #220# #229# #230# #234#
Jaskowski, S. (1936), Recherches sur le systeme de la logique intuitioniste, translated in McCall (1967), 259-263. #101#

Jezek, J. and Kepka, T. (1978), Quasitrivial and nearly quasitrivial distributive groupoids and semigroups, Acta Univ. Carolinae 19, 25-44. #005#
John, R. (1976), On classes of algebras definable by regular equations, Colloq. Math. 36, 17-21.
Jones, G.T. (1972), Pseudocomplemented Semilattices, Ph.D. Thesis, UCLA. #176#
Jones, G.T. (1974), Projective pseudocomplemented lattices, Pacific J. Math. 52, 443-456. #176#
Jonsson, B. and Nelson, E. (1974), Relatively free products in regular varieties, Algebra Universalis 4, 14-19.
Kabat, W.C. and Wojcik, A.S. (1981), Further results on the logic design of multiple valued circuits using and automated theorem proving system, 11-th ISMVL, Norman, Oklahoma, 135-145. #047#
Kabzinski, J. (1979), On equivalential fragment of the three-valued logic of Lukasiewicz, BSL 8, 182-187. #099#
Kabzinski, J. and Wronski, A. (1975), On equivalential algebras, 5-th ISMVL, Bloomington, Indiana, 419-428. #099#
Kaiser, H.K. (1975), On a problem in the theory of primal algebras, Algebra Universalis 5, 307-311. #004# #072#
Kalman, J.A. (1980), The join of the varieties of implication algebras and semilattices, Math. Chronicle 9, 41-52. #046#
Karnofsky, J. (1968), Some results on finite equational bases for finite algebras, Seminar notes, Univ. California Berkeley, 1-22. #076#
Katrinak, T. (1974), Injective double Stone algebras, Algebra Universalis 4, 259-267. #201#
Keir, Y. (1964), Algebraic properties of 3-valued compositions, IEEE Trans. Electronic Computers EC-13, 636-639. #019# #031#
Kepka, T. (1981), Notes on left distributive groupoids, Acta Univ. Carolinae 22, 23-27. #006# #007# #010# #016# #058#
Kepka, T. (1981a), Quasitrivial groupoids and balanced identities, Acta Univ. Carolinae 22, 49-64. #004# #005# #007# #010# #011# #021#
Kleene, S. (1952), Introduction to Metamathematics, Van Nostrand, New York. #084# #140# #149# #222#
Klein-Barmen, F. (1953), Pseudoverband und Flechtwerk, Math. Ann. 126, 138-143. #113#
Klukovits, L. (1973), On commutative universal algebras, Acta Sci. Math. Szeged 34, 171-174. #100#
Kohler, P. (1973), Freie endlich erzeugte Heyting-Algebren, Diplomarbeit, Justus Leibig Universitat, Giessen. #103# #187#
Kohler, P. (1975), Varieties of Brouwerian Algebras, Mitt. Math. Sem. Giessen 116, 1-83. #103# #187#
Kollar, J. (1980), Injectivity and congruence extension property in congruence distributive equational classes, Algebra Universalis 10, 21-26. #195#
Kolpakov, V.I. (1974), Subalgebras of monotonic functions in the algebra of Post, (in Russian), Diskret. Analiz 24, 30-45. #217#
Lakser, H., Padmanabhan, R. and Platt, C.R. (1972), Subdirect decompositon of Plonka sums, Duke Math. J. 39, 485-488.
Landholt, W.D. and Whaley, T.P. (1974), Relatively free implicative semilattices, Algebra Universalis 4, 166-184. #103#
Lau, D. (1980), Submaximale Klassen von P3, WPU Rostock, preprint. #230#
Leigh, V. (1972), Self dual set of unary and binary connectives for the 3-valued propostional calculus, ZMLG 18, 201-204. #014#
Lukasiewicz, J. (1920), On three valued logic, (in Polish), Ruch Filozoficzny 5, 170-171. Translated in Borkowski (1970), 87-88. #201#
Lukasiewicz, J. (1939), The equivalential calculus. Translated in Borkowski (1970), 250-277. #100#
Lukasiewicz, J. (1953), A system of modal logic, J. of Computing Systems 1, 111-149. #196#
Machida, H. (1979), On closed sets of three-valued monotone logical functions, Colloq. Math. Soc. Janos Bolyai 28, Finite Algebra and Multiple-valued Logic, 441-467, North-Holland, Amsterdam (1981). #216# #217#
Malcev, I.A. (1972), Some properties of cellular subalgebras of a Post algebra and their basic cells, (in Russian), Algebra i Logika 11, 571-587. Translated in Algebra and Logic 11, 315-325. #233#

Malcev, I.A. (1973), Certain properties of cells of Post algebras, (in Russian), Diskret. Analiz 23, 24-31. #233#
Marczewski, E. (1964), The number of independent elements in abstract algebras with unary or binary operations, Colloq. Math. 12, 723-727. #014#
Marczewski, E. (1966), Independence in abstract algebras - results and problems, Colloq. Math. 14, 169-188.
McCall, S. (1962), A simple decision procedure for one variable implication/negation formulae in intuitionist logic, NDJFL 3, 120-122. #182#
McCall, S. (1967), Polish Logic: 1920-1939, Clarendon Press, Oxford.
McCarthy, J. (1963), Predicate calculus with "undefined" as a truth value, Stanford Artificial Intelligence Project, Memo 1, 1-3. #058# #083# #201#
McKenzie, R. (1982), Letter to J. Berman, July 1982. #072# #229#
McKinsey, J.C.C. (1936), On the generation of the functions Cpq and Np of Lukasiewicz and Tarski by means of a single binary operation, Bull. Amer. Math. Soc. 42, 849-851. #201#
McNab, D. (1981), Modal operators on Heyting algebras, Algebra Universalis 12, 5-29. #229#
Meredith, C. A. (1969), Equational postulates for the Sheffer stroke, NDJFL 10, 266-270. #084#
Meredith, C.A. (1953), Single axioms for the systems (C,N), (C,0) and (A,N) of the two valued calculus, J. Computer Systems 1, 155-164. #194#
Meyer, R.K. and Parks, Z. (1972), Independent axioms for the implicational fragment of Sobocinski's three-valued logic, ZMLG 18, 291-295. #150#
Mitschke, A. (1971), Implication algebras are 3-permutable and 3-distributive, Algebra Universalis 1, 182-186. #095#
Moisil, G. (1969), The Algebraic Theory of Switching Circuits, Pergemon Press, Oxford.
Moisil, G. (1940), Recherches sur les logiques non-chrysippiennes, Ann. Sci. Univ. Jassy 26, 431-436. #201#
Monteiro, L. (1972), Algebre du calcul propostionel trivalent de Heyting, Fund. Math. 74, 99-109. #187#
Monteiro, L. and Pico, D. (1963), Les reticulees de Morgan et l'operation de Sheffer, Bull. Acad. Polon. Sci 11, 355-357. #084#
Moraga, C. (1975), Hybrid Logic (A fast ternary adder), 5-th ISMVL, Bloomington, Indiana, 344-358. #036# #045# #108# #113#
Mortensen, C. (1978), A theorem of versimilitude, BSL 7, 34-43. #064#
Motil, J.M. (1974), A multiple-valued digital "saturation" system, 4-th ISMVL, Morgantown, W. Virginia, 483-491. #078#
Mouftah, H.T. and Jordan, I.B. (1974), Integrated circuits for ternary logic, 4-th ISMVL, Morgantown, W. Virginia, 285-302. #084#
Muehldorf, E. (1960), Multivalued switching algebras and their application in digital systems, Proc. National Electronics Conference 15, 467-480. #151#
Mukaidono, M. (1981), A set of independent and complete axioms for a fuzzy algebra (Kleene Algebra), 11-th ISMVL, Norman, Oklahoma, 27-34. #073#
Mukaidono, M. (1982), New canonical forms and their applications to enumerating fuzzy switching functions, 12-th ISMVL, Paris, 275-279. #084#
Murskii, V.L. (1965), The existence in three-valued logic of a closed class with a finite basis having no finite complete system of identities, (in Russian), Dokl. Akad. Nauk SSSR 163, 815-818. Translation in Soviet Math. 6 (1965), 1020-1024. #048#
Muzio, J.C. (1971), A decision process for 3-valued Sheffer functions II, ZMLG 17, 97-114. #218# #224# #226# #228#
Nemitz, W. and Whaley, T. (1971), Varieties of implicative semilattices, I, Pacific J. Math. 37, 759-769. #103#
Padmanabhan, R. (1971), Regular identities in lattices, Trans. Amer. Math. Soc. 158, 179-188. #015# #017#
Park, R.E. (1976), Equational Classes of Non-Associative Ordered Algebras, Ph.D. Thesis, UCLA. #004#
Picard, S. (1935), Sur les fonctions defines dans les ensembles finis quelconques, Fund. Math. 24, 298-301. #232#
Pierce, R.S. (1978), Symmetric groupoids, Osaka J. Math. 15, 51-76. #005#
Pigozzi, D. (1979), Minimal, locally-finite varieties that are not finitely axiomatizable, Algebra Universalis 9, 374-390. #135# #208# #215#

Pirog-Rzepcka, K. (1973), A predicate calculus with formulas which lose sense and the corresponding propositional calculus, BSL 2, 22-29. #200#
Plonka, J. (1967), On a method of construction of abstract algebras, Fund. Math. 61, 183-189. #015#
Plonka, J. (1969), On equational classes of abstract algebras defined by regular equations, Fund. Math. 64, 241-247. #082#
Plonka, J. (1971), On algebras with n distinct essentially n-ary operations, Algebra Universalis 1, 73-79. #005#
Plonka, J. (1971a), On free algebras and algebraic decompositions of algebras from some equational classes defined by regular equations, Algebra Universalis 1, 261-264. #015# #042# #046#
Post, E.L. (1921), Introduction to a general theory of elementary propositions, Amer. J. Math. 43, 163-185. #066# #235#
Post, E.L. (1941), The two valued iterative systems of mathematical logic, Annals of Math. Studies No. 5, Princeton Univ. Press, Princeton, New Jersey.
Preparata, F. and Yeh, R. (1972), Continuously valued logic, J. Computer and System Sciences 6, 397-418. #084#
Quackenbush, R.W. (1972), The triangle is functionally complete, Algebra Universalis 2, 128. #012#
Quackenbush, R.W. (1974), Some classes of idempotent functions and their compositions, Colloq. Math. 29, 71-81. #034#
Quackenbush, R.W. (1976), Varieties of Steiner loops and Steiner quasigroups, Canad. J. Math. 28, 1187-1198. #003#
Raca, M.F. (1966), A test for functional completeness in the logic corresponding to Jaskowski's first matrix, (in Russian), Doklady Akad. Nauk 168, 524-527. Translated in Soviet Math. 7 (1966), 683-687. #187#
Raca, M.F. (1969), The class of functions of the three-valued logic that corresponds to the first matrix of Jaskowski, (in Russian), Problemy Kibernetiki 21, 185-214. #096# #130# #142# #177# #185# #187#
Rasiowa, H. and Sikorski, R. (1963), The Mathematics of Metamathematics, Polish Scientific Publishers, Warsaw. #187#
Reichenbach, H. (1944), Philosophical Foundations of Quantum Mechanics, University of California Press, Berkeley, California. #039# #112# #151#
Rescher, N. (1969), Many-valued Logic, McGraw-Hill, New York. #036# #038# #043# #075# #081# #082# #109# #112# #117# #144# #156# #157# #171# #173# #235#
Rielak, P. (1974), On functions definable in implicational algebras, BSL 3, 24-26. #101#
Robinson, D.F. (1971), A catalogue of binary operations, The New Zealand Mathematics Magazine 8, 2-11. #014#
Romanowska, A. (1980), Free bisemilattices with one distributive law, Demonstatio Mathematica 13, 565-572. #017#
Romanowska, A. (1981), Subdirectly irreducible pseudocomplemented de Morgan algebras, Algebra Universalis 70-75. #201#
Rose, A. (1953), A formalization of Sobocinski's three-valued implicational propositional calculus, J. Computing Systems 1, 165-168. #064#
Rose, A. (1961), Self dual binary and ternary connectives for m-valued logic, Math. Ann. 143, 448-462. #014# #161#
Rose, A. (1979), Many valued propositional calculi without constants, 9-th ISMVL, Bath, England, 128-134. #226#
Rosenberg, I.G. (1976), Some algebraic and combinatorial aspects of multiple-valued circuits, 6-th ISMVL, Logan, Utah, 9-23. #190# #197# #201#
Rosenberg, I.G. (1977), Completeness properties of multiple-valued logic algebras, in Computer Science and Multiple-valued Logic, Theory and application, North-Holland, 1977.
Rosenberg, I.G. and Szendrei, A. (1981), Degrees of clones and relations, CRMA, Univ. de Montreal, preprint. #233#
Rosser, J.B. and Turquette A.R. (1945), Axiom schemes for m-valued propositional calculi, J. Symbolic Logic 10, 61-82. #190# #193# #201#
Saito, T. (1977), There are 18 linearly ordered semigroups of order 3, Bulletin of Tokyo Gakugei Univ. Ser. IV 29, 79. #027# #054#
Salomaa, A. (1959), On many-valued systems of logic, Ajatus 22, 115-159. #030# #109# #112# #150#

Schmidt, E.T. (1972), On n-permutable equational classes, Acta Sci. Math. Szeged 33, 29-30. #210#
Schweigert, D. (1979), On prepolynomially complete algebras, J. London Math. Soc. 20, 179-185. #220#
Sestakov, V.I. (1964), On the relationship between certain three valued logical calculi, (in Russian), Uspekhi Mat. Nauk 19, 177-181. MR 31, 2140. #084#
Sheffer, H.M. (1913), A set of five independent postulates for Boolean algebras with application to logical constants, Trans. Amer. Math. Soc. 14, 481-488. #129#
Shoesmith, D.J. and Smiley, T.J. (1978), Multiple-conclusion Logic, Cambridge University Press, Cambridge, England. #196#
Skolem, T. (1952), Consideraciones sobre los fundamentos de la matematica, Revista Matematica Hispano-Americana 12, 169-200. MR 15, 92. #101#
Sloane, N.J.A. (1973), A Handbook of Integer Sequences, Academic Press, New York.
Slupecki, J. (1936), The full three-valued propostional calculus. Translated in McCall(1967), 335-337. #180# #199# #201# #235#
Smiley, T. (1962), The independence of connectives, Journal of Symbolic Logic 27, 426-436. #036# #173#
Sobocinski, B. (1952), Axiomatization of a partial system of three-valued calculus of propositions, J. Computer Systems 1, 23-55. #064# #085#
Sobocinski, B. (1972), Certain sets of postulates for distributive lattices with constant elements, NDJFL 13, 119-123. #050# #055#
Sugihara, T. (1955), Strict implication free from implicational paradoxes, Memoirs of the Faculty of Liberal Arts, Fukui University, Series 1, 55-59. #064# #085# #086#
Takasaki, M. (1943), Abstraction of symmetric transformations, (in Japanese), Tohoku Math. J. 49, 145-207. MR 9 p.8. #033#
Tamthai, M. and Chaiyakul, C. (1980), The endomorphism semigroup of algebras with reflexive elements, Algebra Universalis 11, 193-196. #082#
Taylor, J.S. (1920), Sheffer's set of five postulates for Boolean algebras in terms of the operation "rejection" made completely independent, Bull. Amer. Math. Soc. 26, 449-454. #158# #164#
Taylor, W. (1973), Characterizing Mal'cev conditions, Algebra Universalis 3, 351-397.
Taylor, W. (1976), Pure compactifications in quasi-primal varieties, Canad. J. Math. 28, 50-62. #006# #176#
Taylor, W. (1977), Letter to J. Baldwin, December, 1977. #108#
Thelliez, S. (1973), Introduction a l'Etude des Structures Ternaires de Communication. Translated by W.G. Stripp, Gordon and Breach, 1975. #132#
Thomas, I. (1962), The rule of excision in positive implication, NDJFL 3, 64. #150#
Tokharz, M. (1975), Functions definable in Sugihara algebras and their fragments (I), Studia Logica 34, 295-304. #064# #085# #086#
Tokharz, M. (1976), Functions definable in Sugihara algebras and their fragments (II), Studia Logica 35, 279-283.
Turquette, A.R. (1966), A method for constructing implication logics, ZMLG 12, 267-278. #139#
Urbanik, K. (1965), On algebraic operations in idempotent algebras, Colloq. Math. 13, 129-157. #003#
Urquhart, A. (1974), Implicational formulas in intuitionistic logic, J. Symbolic Logic 39, 661-664. #101#
Ursini, A. (1979), Intuitionistic diagonalizable algebras, Algebra Universalis 9, 229-237. #229#
Varlet, J. (1972), A regular variety of type <2,2,1,1,0,0>, Algebra Universalis 2, 218-223. #201#
Wajsberg, M. (1937), Contributions to metalogic. Translated in McCall(1967), 285-318. #153# #191#
Webb, D.L. (1936), Definition of Posts generalized negative and maximum in terms of one binary operation, Amer. J. Math. 58, 193-194. #235#
Werner, H. (1978), Discriminator-Algebras, Akademie-Verlag, Berlin. #159#
Wesselkamper, T. (1974), Some completeness results for Abelian semigroups and groups, 4-th ISMVL, Morgantown, W. Virginia, 393-400. #109# #120#
Winker, S. (1981), Letter to J. Berman, October 1981. #005#
Winker, S. and Berman, J. (1979), Finite basis and related results for an upper bound algebra, Notices Amer. Math. Soc. 26, A-427. #004#

Wojciechowski, W. and Wojcik, A.S. (1979), Multiple valued logic design by theorem proving, 9-th ISMVL, Bath, England, 196-199. #132#
Wojtylak, P. (1979), Strongly finite logics: Finite axiomatizability and the problem of supremum. BSL 8, 99-111. #147#
Wolf, R.G. (1977), A survey of many-valued logic (1966-1974), Appendix 1 in Modern Uses of Multiple-valued Logic, ed. by J.M. Dunn and G. Epstein, Reidel Pub., Dortecht, 167-323.
Wronski, A. (1979), A three element matrix whose consequence operation is not finitely based, BSL 8, 68-71. #091#
Yoeli, M. and Rosenfeld, G. (1965), Logical design of ternary switching circuits, IEEE Transactions on Electronic Computers EC-14, 19-29. #235#
Zakrzewska, T. (1976), Some remarks on three-valued implicative sentential calculi, BSL 5, 9-12. #150# #191#
Zaslavskii, I.D. (1979), Realization of three-valued logical functions by means of recursive and Turing operators, (in Russian), Studies in the theory of algorithms and mathematical logic, Nauka, Moscow, 52-61. MR 81i:03031. #083# #163# #231#

Department of Mathematics,
Statistics, and Computer Science
University of Illinois at Chicago
Chicago, Illinois 60680
U.S.A.

TREE ALGEBRAS AND CHAINS[1)]

Gary Brenner and Donald Monk[2)]

For any tree T, one may define the tree algebra B_T as the field of subsets of T generated by the collection of sets $S_t = \{s \in T : t \leqq s\}$ for $t \in T$. The notion was introduced and used to construct rigid Boolean algebras and to solve a question about weakly homogeneous Boolean algebras in Brenner [B]. Here we relate this notion to linear orderings.

We concern ourselves with two main questions. First, which chains occur in tree algebras? This is the topic of section 2. Our main results are that if C is a chain in a tree algebra and the cardinality of C is regular uncountable, then C contains a well-ordered or inversely well-ordered subset of the same power; and for κ regular uncountable, T has a branch of power $\geqq\kappa$ iff B_T contains a well-ordered chain of power $\geqq\kappa$.

In section 3 we consider the relationship between the classes of tree algebras and of interval algebras. We show that every tree algebra is isomorphic to a subalgebra of an interval algebra and use results from section 2 to show that some interval algebras embed in no tree algebra.

Section 1 contains definitions and lemmas used in the later sections, some of independent interest, as well as a discussion of several other methods of generating Boolean algebras from trees.

1. BASIC DEFINITIONS AND FACTS. We use "BA" to abbreviate "Boolean algebra." For any tree T and any $t \in T$, let $S_t^T = S_t = \{s \in T : t \leqq s\}$. The <u>tree algebra</u> B_T

---

1)The results of this paper are contained in chapters 1, 3 and 4 of the Ph.D. dissertation of the first author, prepared under the direction of the second author at the University of Colorado.

2)Research supported in part by Forschungsinstitut fur Mathematik, ETH-Zentrum, Zurich.

over T is the field of subsets of T generated by $\{S_t : t \in T\}$. For any $t \in T$, A_t is the set of immediate successors to t. A tree T is splitting if for any $t \in T$, $|A_t| \neq 1$; it is infinitely splitting if for all $t \in T$, A_t is infinite. The level of $t \in T$ is the order type of $\{s : s < t\}$; for any ordinal α, level $\alpha = \{t \in T :$ level of t is $\alpha\}$. The height of T is $\sup\{(\text{level of } t) + 1 : t \in T\}$. If $t \in T$, then S_t may be considered as a tree in its own right. An initial chain in T is a chain C in T such that $x \leq y \in C \rightarrow x \in C$. T is limit-normal if for every initial chain C in T without last element, there is at most one $t \in T$ such that $C = \{s \in T : s < t\}$. A maximal initial chain in T is called a branch.

If A is any BA and $a \in A$, we set $a^1 = a$, $a^0 = -a$. If $(L, \leq)$ is a linear ordering, the interval algebra on L is the BA of subsets of L generated by $\{[a,b) : a < b \text{ in } L\} \cup \{[a,\infty) : a \in L\}$. For any BA A, depth $A = \sup\{|X| : X \subseteq A, X \text{ well-ordered}\}$, and length $A = \sup\{|X| : X \subseteq A, X \text{ a chain}\}$. A partition of A is a subset P of A which is pairwise disjoint, with $0 \notin P$, and with $\sum P = 1$. For any cardinal κ, κ^+ is the least cardinal greater than κ, $\kappa^{+0} = \kappa$ and $\kappa^{+(n+1)} = (\kappa^{+n})^+$.

Other ways of associating Boolean algebras with trees are known, and for background, we mention several.

In Horn, Tarski [HT] the following notion is discussed. A ramification set in a BA A is a subset X of A satisfying the following conditions:

(1) For all $x \in X$, $x \neq 0$.

(2) For all $x,y \in X$, $x \leq y$ or $y \leq x$ or $x \cdot y = 0$.

(3) For all $x \in X$, $\{y : x < y\}$ is well-ordered by $\geq$.

PROPOSITION 1.1. B is isomorphic to a tree algebra iff B has a ramification set as a generating set.

PROOF. ($\rightarrow$) obvious. ($\leftarrow$): Let X be a ramification set in B. Then under $\geq$, X forms a tree. If X has finitely many roots, we may assume that $\sum \{t : t \text{ a root of } X\} = 1$. We now define a homomorphism f of B_X onto B. For any $x \in X$, let $fS_x = x$. Then f extends to a homomorphism by the Sikorski extension criterion. Since B is a homomorphic image of B_X, B is isomorphic to a tree algebra by Theorem 5.2 of the first author's dissertation.

Note that the mapping f in the proof of 1.1 is not in general an isomorphism. For example, if the ramification set has an element t with A_t finite, and $t = \sum A_t$, then f is not one-one.

Notice the similarity of 1.1 to the well-known fact that a BA B is isomorphic to an interval algebra iff B contains an ordered basis (i.e., a linearly ordered set which is a generating set).

One method of associating a BA with a tree is common in forcing arguments. Make T into a topological space by letting $\{S_t : t \in T\}$ be a base for the topology. Then RO(T) is the BA of regular open sets of T. It is a complete BA, so for T infinite, it is never isomorphic to B_T by Theorem 3.1. However, there is a close connec tion with B_T, given by our next result.

PROPOSITION 1.2. If T is infinitely splitting, then B_T is isomorphic to the subalgebra of RO(T) generated by $\{S_t : t \in T\}$.

PROOF. By the Sikorski extension criterion.

Note the following about RO(T) and the operations in it.

$$\text{int cl } S_t = \{s : \text{For all } r \geqq s, \text{ r and t are comparable}\}.$$

Thus for T splitting, int cl $S_t = S_t$.

$$S_t \cdot S_s = S_t \cap S_s$$

$$S_{t_1} + \ldots + S_{t_m} = \{s\text{: For all } r \geqq s, \text{ r is comparable with one of } t_1, \ldots, t_m\}.$$

Hence for T infinitely splitting,

$$S_{t_1} + \ldots + S_{t_m} = S_{t_1} \cup \ldots \cup S_{t_m}$$

$$-S_t = \{s : \text{s and t are incomparable}\}.$$

Thus $-S_t \neq {\sim}S_t$ unless t is the unique root of T.

For T not splitting, Proposition 1.2 can fail. For example, if T is a well-ordered chain, then RO(T) = 2, while B_T is isomorphic to the interval algebra on T.

Shelah in [S] makes use of the following construction. If T is a tree, let F_T be a BA freely generated by $\{x_t : t \in T\}$ subject to $x_t \leqq x_s$ for $s \leqq t$. Of course B_T

is a homomorphic image of F_T, but in general F_T is not isomorphic to a tree algebra. For example, if T consists just of uncountably many roots, then F_T is an uncountable free BA, which by Theorem 3.1 cannot be embedded in a tree algebra. Shelah also considers F'_T, which is freely generated by $\{x_t : t \in T\}$ subject to $x_t \leqq x_s$ for $s \leqq t$ and $x_t \cdot x_s = 0$ for s and t incomparable.

PROPOSITION 1.3. If T has infinitely many roots, then $B_T \cong F'_T$. If T has finitely many roots, then $a = \Pi\{-x_r : r \text{ is a root}\}$ is an atom of F'_T and $B_T \cong F'_T \restriction -a$.

PROOF. Note that $S_{t_1} \cdot \ldots \cdot S_{t_m} \cdot -S_{s_1} \cdot \ldots \cdot -S_{s_n} = 0$ iff one of the following conditions holds:

(1) t_i and t_j are incomparable for some $i,j \in \{1,\ldots,m\}$,

(2) $s_i \leqq t_j$ for some $i \in \{1,\ldots,n\}$, some $j \in \{1,\ldots,m\}$,

(3) R is a subset of $\{s_1,\ldots,s_n\}$.

On the other hand, $x_{t_1} \cdot \ldots \cdot x_{t_m} \cdot -x_{s_1} \cdot \ldots \cdot -x_{s_n} = 0$ iff (1) or (2) holds. Hence the proposition follows.

The final method of associating a BA with a tree has been used implicitly in several constructions, and was made explicit in a letter from Judy Roitman to the second author. Ch(T) is the BA of subsets of T generated by {C : C is an initial chain of T}. It is easy to see that Ch(T) is always hereditarily atomic, and hence there are tree algebras not embeddable in any algebra Ch(T) (see, e.g., Theorem 2.9)

We now turn to several simple facts about tree algebras which will be used later. First we have a normal form lemma.

LEMMA 1.4. Let $b \in B_T$. Then b can be expressed in the form $\sum_{i \leqq n} f_i$ where $n \in \omega$ and

(i) For all $i,j \leqq n$, $i \neq j \rightarrow f_i \cdot f_j = 0$;

(ii) If $b \leqq \sum_{t \in J} S_t$ for some $J \in [T]^{<\omega}$, then $f_n = 0$ and $J_n = 0$; otherwise $f_n = -\sum_{t \in J_n} S_t$ with $J_n \in [T]^{<\omega}$;

(iii) For all $i < n$, $f_i = S_{t_i} - \sum_{s \in J_i} S_s$ with J_i a finite set of successors to t_i;

(iv) for all $i \leqq n$, J_i is pairwise incomparable;

(v) for all $i < n$, for all $j \leqq n$, for all $s \in J_j$, $t_i \neq s$.

PROOF. Since $\{S_t : t \in T\}$ generates B_T, we can write

$$b = \sum_{i \in p} f_i,$$

each $f_i \neq 0$, $f_i \cdot f_j = 0$ for $i \neq j$, and

$$f_i = \prod_{j < m_i} S_{t_{i,j}}^{e(i,j)}$$

each $e(i,j) \in \{0,1\}$. Since $S_t \cdot S_s = 0$ if s and t are incomparable and $S_t \cdot S_s = S_t$ if $s \leqq t$, we may assume that each f_i has the form

(1) $f_i = S_{t_i} - \sum_{s \in J_i} S_s$, J_i a pairwise incomparable set of successors to t_i, or

(2) $f_i = -\sum_{s \in J_i} S_s$, J_i a pairwise incomparable set.

If $f_i \leqq \sum_{u \in K} S_u$ for some $K \in [T]^{<\omega}$, then $f_i = \sum_{u \in K} (f_i \cdot S_u)$; hence we may assume that (2) holds only if $f_i \nleqq \sum_{u \in K} S_u$ for all $K \in [T]^{<\omega}$. Clearly (2) occurs for some i iff $b \nleqq \sum_{u \in K} S_u$ for all $K \in [T]^{<\omega}$. This is possible only if T has infinitely many roots. Now (2) can hold for at most one $i < p$; for if it holds for $i,j < p$ with $i \neq j$, then choose a root v of T such that $v \notin \sum_{u \in J_i \cup J_j} S_u$. Then $v \in f_i \cdot f_j$, a contradiction. Finally , note that if f_i and f_j have the form (1) and $t_j \in J_i$, then

$$f_i + f_j = S_{t_i} - \sum_{s \in J_i \cup J_j,\ s \neq t_j} S_s;$$

similarly, if f_i has the form (2). Thus we may assume that (i)-(v) hold.

The following supplement to the normal form lemma is sometimes useful.

LEMMA 1.5. (i) Suppose $b \leqq \sum_{t \in J} S_t$ for some $J \in [T]^{<\omega}$ and $b = \sum_{i \leqq m} f_i$ and $c = \sum_{i \leqq n} g_i$ are the normal forms of b and c. Then $b \leqq c$ iff for all $i \leqq m$, there is $j \leqq n$ such that $f_i \leqq g_j$.

(ii) Let $\{s,t\} \cup J \cup K \in [T]^{<\omega}$, with J and K pairwise incomparable sets. (a) If J is a set of successors to s and K a set of successors to t, then $S_s - \sum_{u \in J} S_u \leqq S_t - \sum_{u \in K} S_u$ iff the following conditions hold: (I) $t \leqq s$, (II) for any $u \in K$, $u \nleqq s$, and (III) for all $u \in K$, $s < u \rightarrow$ there is $v \in J$, $v \leqq u$. (b) If J is a set of successors to s, then $S_s - \sum_{u \in J} S_u \leqq - \sum_{u \in K} S_u$ iff (II) and (III) hold. (c) If K is a set of successors to t, then $- \sum_{u \in J} S_u \leqq S_t - \sum_{u \in K} S_u$ iff either $\sum_{u \in J} S_u = 1$ or else the following conditions hold: (A) t is a root, (B) $\{r \in T : r \text{ is a root}, r \neq t\}$ is a subset of J, (C) for all $u \in K$, there is $v \in J$, $v \leqq u$. (d) $- \sum_{u \in J} S_u \leqq - \sum_{u \in K} S_u$ iff for all $u \in K$, there is $v \in J$, $v \leqq u$.

(iii) If $b \leqq \sum_{u \in J} S_u$ for some $J \in [T]^{<\omega}$, and $b = \sum_{i \leqq m} f_i = \sum_{j \leqq n} g_j$ are two normal forms for b, then $n = m$, $g_m = f_m = 0$, and $\{g_i : i < m\} = \{f_i : i < m\}$.

PROOF. (i). We only need to show ($\rightarrow$). Say $f_i = S_{t_i} - \sum_{s \in J_i} S_s$ for all $i < m$, $f_m = 0$, $g_i = S_{u_i} - \sum_{s \in K_i} S_s$ for all $i < n$, $g_n = - \sum_{s \in K_n} S_s$ or $g_n = 0$, with all conditions of the normal form lemma satisfied. Suppose there is $i \leqq m$, for all $j \leqq n$, $f_i \nleqq g_j$. Thus $i < m$. Now $t_i \in f_i \leqq b \leqq c$, so $t_i \in g_j$ for some $j \leqq n$. Since $f_i \nleqq g_j$, we can choose $w \in f_i - g_j$ of lowest level. Since $t_i \leqq w$ and $t_i \in g_j$, it follows that $w \in S_s$ for some $s \in K_j$. Now

(1) $\quad s = w$

For, assume $s < w$. Then $t_i \leqq w$, $s < w$, so t_i and s are comparable. Since $t_i \in g_j$ and $s \in K_j$, we have $t_i < s$. Thus $s \in f_i - g_j$, contradicting the choice of w.

Now $w \in f_i \leqq b \leqq c$, so choose $k \leqq n$ so that $w \in g_k$. Recall that $w \notin g_j$, so $k \neq j$. Also, $u_k \leqq w$, and by 1.4(v), $u_k \neq w$.

CASE 1. $j,k < n$. So $u_k < w$ and $u_j < w$. It follows that $u_k \leqq u_j$ - hence $u_j \in g_k$, $g_j \cdot g_k \neq 0$, a contradiction; or $u_j < u_k$ - hence $u_k \in g_j$, $g_j \cdot g_k \neq 0$, again a contradiction.

CASE 2. $j < n$, $k = n$. Since $t_i \leqq w \in g_k$, we also have $t_i \in g_k$, so $t_i \in g_j \cdot g_k$, a contradiction.

CASE 3. $j = n$, $k < n$. Then $u_k \in g_k \cdot g_n$, a contradiction.

It is straightforward to verify (ii). Condition (iii) is immediate from (i).

We note that the hypothesis $b \leqq \sum_{t \in J} S_t$ for some $J \in [T]^{<\omega}$ is necessary in 1.5(i) and 1.5(iii). For example, if T has infinitely many roots $r_0, r_1, \ldots$, then $b = c = T = S_{r_0} + -S_{r_0} = S_{r_1} + -S_{r_1}$ are two normal forms that violate 1.5(i) and 1.5(iii).

COROLLARY 1.6. (i) For any $b \in B_T$, b is an atom iff there is $t \in T$, A_t is finite and $b = S_t - \sum_{s \in A_t} S_s$.

(ii) $\{S_t : t \in T,\ A_t \text{ is infinite}\} \cup \{b \in B_T : b \text{ is an atom}\}$ is dense in B_T.

COROLLARY 1.7. B_T is atomless iff for all $t \in T$, A_t is infinite. B_T is atomic iff for all $t \in T$, there is $s \geqq t$, A_s is finite.

It can be shown that B_T is hereditarily atomic iff T does not contain a subtree T' with exactly one root, height ω, such that $|A_t| = \omega$ for all $t \in T'$.

The following result is frequently useful.

THEOREM 1.8. For any tree T there is a tree T' with a single root such that $B_T \cong B_{T'}$.

PROOF. CASE 1. T has a finite set R of roots. Fix $r \in R$. Let $T' = T$, and

$$\leqq' = \{(x,y) : x,y \in T' \text{ and either } x \leqq y \text{ or } x = r\}$$

The identity on $\{S_t^{T'} : t \in T \setminus \{r\}\}$ extends to an isomorphism from $B_{T'}$ onto B_T.

CASE 2. T has an infinite set of roots. Fix $z \notin T$, and let $T' = T \cup \{z\}$,

$$\leqq' = \{(x,y) : x,y \in T' \text{ and either } x \leqq y \text{ or } x = z\}$$

The identity on $\{S_t^T : t \in T\}$ extends to an isomorphism from B_T onto $B_{T'}$.

THEOREM 1.9. $B_T \restriction S_t = B_{S_t}$.

THEOREM 1.10. If T and T' are trees and $T' \subseteq T$, then $B_{T'}$ embeds in B_T.

PROOF. First suppose that T' contains all the roots of T, or T' has infinitely many roots. In this case the map $S_t^{T'} \mapsto S_t^T$, $t \in T'$, extends to an embedding.

Second, suppose T' has only finitely many roots $t_1, \ldots, t_m$. For all $i \leq m$, let $S_i = S_{t_i}^T$ and $R_i = S_{t_i}^{T'}$. Now by the first case, B_{R_i} embeds in B_{S_i} for all i, so

$$\begin{aligned} B_{T'} &\cong (B_{T'} \restriction R_1) \times \cdots \times (B_{T'} \restriction R_m) \\ &= B_{R_1} \times \cdots \times B_{R_m} \end{aligned}$$

embeds in

$$\begin{aligned} B_{S_1} \times \cdots \times B_{S_m} &= (B_T \restriction S_1) \times \cdots \times (B_T \restriction S_m) \\ &\cong B_T \restriction (S_1 + \cdots + S_m) \end{aligned}$$

which, as is well-known, embeds in B_T.

2. CHAINS CONTAINED IN TREE ALGEBRAS. Some of our methods here are adapted from McKenzie, Monk [MM].

THEOREM 2.1. Let κ be uncountable and regular, and suppose C is a chain of cardinality κ in B_T. Then there is a $W \in [C]^\kappa$ which is well-ordered or inversely well-ordered, and T has a chain of type κ.

PROOF. By 1.8 and its proof, we may assume that T has only one root. We say that $b \in B_T$ has <u>wedge - size</u> n iff in the normal form of 1.4 we have $b = \sum_{i \leq n} f_i$ (recall also that $f_n = 0$ in our case). It suffices to show by induction on n that the conclusion of the theorem holds when all members of C have wedge-size n.

First suppose that n = 1. Say $b = S_{t_b} - \sum_{s \in J_b} S_s$, for each $b \in C$, in normal form. By 1.5(ii), if $b, c \in C$ and $b < c$, then $t_c \leq t_b$.

CASE 1. There is $C' \in [C]^\kappa$, for all $b, c \in C'$, $t_b = t_c$. Say $t_b = t$, for all $b \in C'$. Then by 1.5(ii) again, we have

(1) if $b, c \in C'$ and $b < c$, then for all $s \in J_c$, there is $u \in J_b$, $u \leq s$.

Now we choose $C'' \in [C']^\kappa$ so that $(J_b : b \in C'')$ forms a Δ-system, say with kernel K, and $J_b \neq K$ for all $b \in C''$. Then (1) clearly extends to

(2) if $b,c \in C''$ and $b < c$, then for all $s \in J_c \setminus K$, there is $u \in J_b \setminus K$, $u < s$.

Now we claim

(3) There is $f \in \prod_{b \in C''} (J_b \setminus K)$, for all $b,c \in C''$, $b < c \to fb < fc$.

This follows from

(4) For all $n \in \omega$, for all $b \in {}^nC''$, ($b_0 < \ldots < b_{n-1} \to$ There is $c \in \prod_{i \in n} (J_{b_i} \setminus K)$ such that $c_0 < \ldots < c_{n-1}$).

Condition (4) is clear from (2). One can derive (3) from (4) by using the Tychonoff product theorem or the compactness theorem. By (3), C'' is a chain of type $\geqq\kappa$ in B_T and $\{fb : b \in C''\}$ is a chain of type $\geqq\kappa$ in T.

CASE 2. Otherwise, there is a $C' \in [C]^\kappa$ such that for all $b,c \in C'$, $b < c \to t_c < t_b$ Hence C' is inversely well-ordered, and $\{t_b : b \in C'\}$ is a chain of type $\geqq\kappa$ in T.

Now suppose inductively that $n > 1$. Say $b = \sum_{i < n} f_i^b$, $f_i^b = S_{t_{bi}} - \sum_{s \in J_{bi}} S_s$ in normal form, for each $b \in C$. By 1.5(i) we have:

If $b,c \in C$ and $b < c$, then for all $i < n$, there is $j < n$, $f_i^b \leqq f_j^c$.

Hence by the Tychonoff product theorem, there is an $x : C \to n$ such that for all $b,c \in C$, if $b < c$ then $f_{xb}^b \leqq f_{xc}^c$. Without loss of generality, $xb = 0$ for all $b \in C$. Thus $f_0^b \leqq f_0^c$ whenever $b,c \in C$ and $b < c$.

CASE 1. There is $C' \in [C]^\kappa$, for all $b,c \in C'$, $f_0^b = f_0^c$. For all $b \in C'$ let $b' = b - f_0^b$. Thus

(5) if $b,c \in C'$ then ($b < c$ iff $b' < c'$).

Now $\{b' : b \in C'\}$ is a chain of cardinality κ, all members of which have wedge-size n-1. By the induction hypothesis, there is a $C'' \in [C']^\kappa$ such that $\{b' : b \in C''\}$ is well-ordered or inversely well-ordered, and T has a chain of type κ. By (5), C'' itself is well-ordered or inversely well-ordered.

CASE 2. Otherwise, there is $C' \in [C]^\kappa$, for all $b,c \in C'$, $b < c \to f_0^b < f_0^c$. By the case $n = 1$, there is a $C'' \in [C']^{\kappa}$ such that $\{f_0^b : b \in C''\}$ is well-ordered or inversely well-ordered, and T has a chain of type κ. Clearly C'' is itself well-ordered or inversely well-ordered.

COROLLARY 2.2. Let κ be regular and uncountable. Then the following conditions are equivalent:

(i) T has no branch of type $\geqq\kappa$.

(ii) B_T has no chain of cardinality κ.

COROLLARY 2.3. If T is an infinite tree, then length B_T = depth B_T = $\sup\{|X| : X \text{ is a branch in } T\}$.

PROOF. Clearly $\sup\{|X| : X \text{ is a branch in } T\}$ = depth $B_T \leqq$ length B_T. If the corollary is false, then B_T has a chain of size $(\sup\{|X| : X \text{ is a branch in } T\})^+$, contradicting 2.1.

PROPOSITION 2.4. If κ is singular, then there is a tree T of cardinality κ and height κ which has no branch of size κ, but B_T has a chain C of order type κ and a chain D of size κ with no well-ordered or inversely well-ordered subset of D of size κ.

PROOF. Let $(\lambda_\alpha : \alpha < \text{cf } \kappa)$ be a strictly increasing sequence of infinite cardinals with supremum κ. Let $T = \{t_{\alpha\beta} : \alpha < \text{cf } \kappa,\ \beta < \lambda_\alpha\}$ and define

$$t_{\alpha\beta} \leqq t_{\alpha'\beta'} \text{ iff } (\alpha = \alpha' \text{ and } \beta \leqq \beta') \text{ or } (\alpha \leqq \alpha' \text{ and } \beta = 0).$$

Clearly T contains no branch of length κ, $|T| = \kappa$, and T has height κ. Let $C = \{S_{t_{\alpha\beta}} + S_{t_{\alpha+1,0}} : \alpha < \text{cf } \kappa,\ \beta < \lambda_\alpha\}$, $D = \{S_{t_{\alpha+1,0}} + (S_{t_{\alpha,0}} - S_{t_{\alpha,\beta}}) : \alpha < \text{cf } \kappa,$ $0 < \beta < \lambda_\alpha\}$. It is easily checked that C is inversely well-ordered in type κ, and D satisfies the desired conditions.

One might ask about the very existence of a non-well-ordered chain in B_T, since no such exists in T. If for all $t \in T$, $|A_t| \geqq \omega$, then B_T is atomless, and so η is embeddable in B_T. However, this is not a necessary condition. For example, let T be the full binary tree of height ω (T has one root, height ω, and $|A_t| = 2$ for every

$t \in T$). It is not hard to see that T', the full ω-tree of height ω is embeddable in T; see, e.g. Rabin [R] (T' has one root, height ω, and $|A_t| = \omega$ for all $t \in T'$). Hence $B_{T'}$, which is atomless, is embeddable in B_T by 1.10, so η is embeddable in B_T. See the comment following corollary 1.7. In this connection we have:

PROPOSITION 2.5. Let T be a splitting tree, and let $\omega \leqq \kappa < \min\{\lambda : T$ has no branch of power $\lambda\}$. Then in B_T there is a dense chain of size κ.

PROOF. For all $t \in T$, let $R_t \subseteq B_T \upharpoonright S_t$ be a chain of type η. Let C be an initial chain of limit type in T of size κ. For every $t \in C$ let s_t be an immediate successor to t which is different from the immediate successor u_t to t in C. Set $D = \{S_{u_t} + r : t \in C,\ r \in R_{s_t}\}$. It is easily checked that D is as desired.

3. THE RELATIONSHIP OF TREE ALGEBRAS TO INTERVAL ALGEBRAS.

THEOREM 3.1. For any T, B_T embeds in an interval algebra.

PROOF. By theorem 1.8 we may assume that T has a single root, and by 1.10 that T is limit-normal and infinitely splitting.

For all $t \in T$, let $\leqq_t$ well-order A_t in a type with last element. Let $L = \{b : b$ is a branch in $T\}$. We define an ordering $\leqq_L$ on L as follows: for $b = c$, $b \leqq_L c$; for $b \neq c$, since T is limit-normal and has one root, the first ordinal ξ where $b(\xi) \neq c(\xi)$ is a successor, say $\xi = \zeta + 1$. We let $b \leqq_L c$ iff $b(\xi) \leqq_{b(\zeta)} c(\xi)$.

The map $S_t \mapsto [b_t^{\min}, b_t^{\max})$ for $t \in T$, where $b_t^{\min}$ and $b_t^{\max}$ are, respectively, the $\leqq_L$-minimal and $\leqq_L$-maximal elements of $\{b : b$ is a branch in T and $t \in b\}$, is easily seen to extend to an embedding of B_T into the interval algebra on L.

A BA B is <u>retractive</u> iff for all homomorphisms f mapping B onto A, there is a one-one homomorphism g mapping A into B such that $f \cdot g$ is the identity on A. Rubin [Ru] contains a proof that if A is a subalgebra of an interval algebra, then A is retractive. So 3.1 has the following immediate corollary.

COROLLARY 3.2. If A is a tree algebra, then A is retractive.

Now we show that not every interval algebra embeds in a tree algebra.

PROPOSITION 3.3. For X an uncountable subset of the real numbers, Int(X), the interval algebra on X, cannot be embedded in any tree algebra.

PROOF. Given X as above, clearly Int(X) contains a chain C of power ω_1. Suppose for contradiction that Int(X) embeds in B_T for some T. Let D be the image of C under the embedding. By theorem 2.1, there is $D' \subseteq D$ such that D' has order type ω_1 or $\omega_1{}^*$ (the order type of ω_1 under $\geqq$). So the preimage of D' in Int(X) has order type ω_1 or $\omega_1{}^*$, which as is well-known cannot occur.

Next we exhibit tree algebras that are not isomorphic to any interval algebra. The finite-cofinite algebra on any cardinal κ (consisting of all finite or cofinite subsets of κ) is isomorphic to the tree algebra generated by a tree of κ roots. In [MM] it is shown that no finite-cofinite algebra contains a chain of type $\omega + \omega$. Thus for any uncountable κ, the finite-cofinite algebra is not isomorphic to any interval algebra. We use theorem 2.1 to obtain atomless examples.

PROPOSITION 3.4. For any regular uncountable κ, if T is a tree satisfying

(1) $|T| = \kappa$,

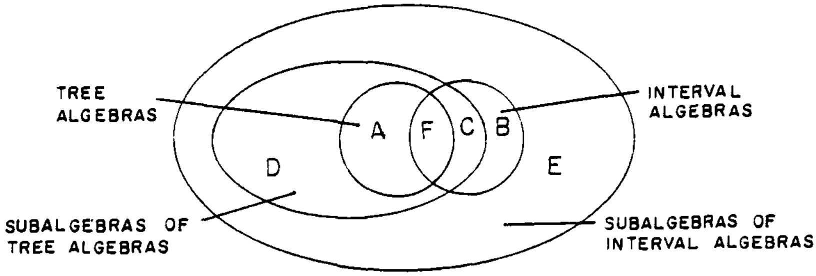
(2) height $T < \kappa$,

(3) for all $t \in T$, A_t is infinite,

then B_T is atomless and is not isomorphic to any interval algebra.

PROOF. Suppose $B_T \cong \mathrm{Int}(L)$ for some L. By 2.1 and condition (2) on T, B_T does not contain a chain of cardinality κ. However, $\kappa = |T| = |B_T| = |\mathrm{Int}(L)| = |L|$. So Int(L) contains a chain of cardinality κ.

Theorem 3.1, proposition 3.3 and proposition 3.4 yield the following diagram.



Proposition 3.4 gives examples that lie in region A. Proposition 3.3 gives examples that lie in region B. Examples that lie in region D are given in the first author's dissertation. These results will appear in a forthcoming paper.

The denumerable atomless BA is isomorphic to the tree algebra generated from any infinitely splitting countable tree. It is an example that lies in region F.

Finally, for any uncountable cardinal κ, if A is the algebra obtained from κ as in proposition 3.4 and B is the interval algebra on the reals, then $A \times B$ is atomless and lies in region E (If A is the finite-cofinite algebra on κ, then $A \times B$ is an atomic example.). Only region C may possibly be empty. Thus we ask the following question.

QUESTION. Is there a BA which is isomorphic to an interval algebra and to a subalgebra of a tree algebra but is not isomorphic to any tree algebra?

REFERENCES

[B] Brenner, G. A simple construction for rigid and weakly homogeneous Boolean algebras answering a question of Rubin, to appear, Proc. AMS.

[HT] Horn, A. and Tarski, A. Measures in Boolean algebras, Trans. AMS 64(1948), 467-497.

[MM] McKenzie, R. and Monk, J.D. Chains in Boolean algebras, to appear, Ann. Math. Logic.

[R] Rabin, M.O. Decidability of second-order theories and automata on infinite trees, Trans. AMS 14(1969), 1-35.

[Ru] Rubin, M. A Boolean algebra with few subalgebras, interval algebras and retractiveness, preprint.

[S] Shelah, S. Constructions of many complicated uncountable structures and Boolean algebras, preprint.

University of Colorado

First author's current address: University of Hawaii

BOOLEAN CONSTRUCTIONS

Stanley Burris

When I was first studying decidability results in the late 1960's and early 1970's it seemed there must be some fundamental connection between classes of algebras having a decidable first-order theory and classes of algebras having a fairly transparent structure theory. We have made alot of progress in recent years, and at present it seems that the only good candidates for constructions to describe a good structure theory are certain Boolean constructions called Boolean products.

Since Boolean products were so useful in obtaining positive decidability results it came as somewhat of a surprise that a modification of the more specialized Boolean power construction would lead to sweeping undecidability results. The tale of these developments, and many others, will be sketched in the following survey.

CONTENTS

§1. AN EXAMPLE CONCERNING BOOLEAN CONSTRUCTIONS

As mentioned in the introduction I became interested in structure theorems about ten years ago because of work on decidability. A basic example is that of a variety generated by a finite Abelian group G -- certainly this has a very good structure theory since every member of the variety is isomorphic to a direct sum of copies of cyclic subgroups of G. And the variety $V(Z_2)$ generated by the ring Z_2 of integers modulo 2, where the language is $\{+,\cdot,-,0,1\}$, is considered to be well-behaved, being the variety of Boolean rings. Now let us look at the variety $V(Z_3)$ generated by the ring Z_3. At first one might be inclined to think that this variety is quite different from Boolean rings -- we shall see that there is a very tight bond between them.

By a result of McCoy and Montgomery [1937] we know that every member of $V(Z_3)$ is isomorphic to a subdirect power of Z_3, so let $R \leq (Z_3)^I$ be a subdirect power of Z_3. For $X \subseteq I$ let us define χ_X by

$$\chi_X = \begin{cases} 1 & \text{if } i \in X \\ 0 & \text{if } i \notin X. \end{cases}$$

Now the set $B = \{X \subseteq I: \chi_X \in R\}$ is a field of subsets of I as

$$\chi_{X\cup Y} = \chi_X + \chi_Y - \chi_X \cdot \chi_Y$$
$$\chi_{X\cap Y} = \chi_X \cdot \chi_Y$$
$$\chi_{-X} = 1 - \chi_X.$$

Next, for $f \in R$ let

$$f_0 = 1 - f^2$$
$$f_1 = 1 - (f-1)^2$$
$$f_2 = 1 - (f+1)^2.$$

Then one can check that $\chi_{f^{-1}(i)} = f_i \in R$ for $i = 0,1,2$. Thus we see that there is a one-one mapping ϕ from R to B^3 defined by $\phi(f) = \langle f^{-1}(0), f^{-1}(1), f^{-1}(2)\rangle$. If now $f \in R$ and $\phi(f) = \langle X,Y,Z\rangle$ then clearly

(1) $$X \cap Y = X \cap Z = Y \cap Z = \emptyset$$

(2) $$X \cup Y \cup Z = I.$$

Conversely, if $\langle X,Y,Z\rangle$ is any triple from B^3 satisfying (1) and (2) then $f = \chi_Y + 2\chi_Z$ is an element of R, and $\phi(f) = \langle X,Y,Z\rangle$. Thus letting R^* be the set of triples from B^3 which satisfy (1) and (2) we see that ϕ is a bijection from R to R^*. Next we wish to endow R^* with the unique ring structure which makes ϕ an isomorphism. We can express this in the language of sets by observing that, for $f,g \in R$,

$$(f+g)^{-1}(0) = [f^{-1}(0) \cap g^{-1}(0)] \cup [f^{-1}(1) \cap g^{-1}(2)] \cup [f^{-1}(2) \cap g^{-1}(1)]$$
$$(f+g)^{-1}(1) = [f^{-1}(0) \cap g^{-1}(1)] \cup [f^{-1}(1) \cap g^{-1}(0)] \cup [f^{-1}(2) \cap g^{-1}(2)]$$
$$(f+g)^{-1}(2) = [f^{-1}(0) \cap g^{-1}(2)] \cup [f^{-1}(2) \cap g^{-1}(0)] \cup [f^{-1}(1) \cap g^{-1}(1)].$$

Thus given $\langle X,Y,Z\rangle$, $\langle U,V,W\rangle \in R^*$ we must define

(3) $\langle X,Y,Z\rangle + \langle U,V,W\rangle = \langle (X\cap U)\cup(Y\cap W)\cup(Z\cap V),\ (X\cap V)\cup(Y\cap U)\cup(Z\cap W),\ (X\cap W)\cup(Z\cap U)\cup(Y\cap V)\rangle.$

Likewise we can derive

(4) $\qquad \langle X,Y,Z\rangle \cdot \langle U,V,W\rangle = \langle X\cup U,\ (Y\cap V)\cup(Z\cap W),\ (Y\cap W)\cup(Z\cap V)\rangle$

(5) $\qquad -\langle X,Y,Z\rangle = \langle X,Z,Y\rangle.$

The zero element of R^* is $\langle I,\emptyset,\emptyset\rangle$, and the identity is $\langle \emptyset,I,\emptyset\rangle$.

Since the definitions (1)-(5) are phrased entirely in terms of union and intersection it is clear that, given B, we can readily reconstruct R. Furthermore, given any Boolean algebra $\langle B,\vee,\wedge,',0,1\rangle$ we can use (1)-(5), replacing $\cup$ by $\vee$ and $\cap$ by $\wedge$, to obtain a member of $V(Z_3)$. Thus, in the language of logicians, we have interpreted the theory of $V(Z_3)$ into the theory of Boolean algebras.

These same ideas show that the theory of $V(Z_p)$, for p a prime, can be interpreted into the theory of Boolean algebras, by using p-tuples instead of 3-tuples. Thus the reader can readily see that the study of a number of interesting varieties reduces to the study of Boolean algebras. We will return to this construction in §4.

One might try similar ideas on $V(Z_4)$. The only nontrivial subdirectly irreducibles in this variety are Z_2 and Z_4. But there is a major obstacle here.

§2. THE DEVELOPMENT OF BOOLEAN ALGEBRA

When Boole first presented his mathematical analysis of the laws of human thought in 1847 he did not have the notion of an algebraic structure $\langle B,\vee,\wedge,',0,1\rangle$, but rather he was concerned with the syntactic side of Boolean algebras. This seems to have been the vantage point until Huntington's 1904 paper on postulates for the algebra of logic.

G. BOOLE 1847, 1854

Boole introduced a mathematical analysis into logic which was analogous to existing work in algebra. He was primarily concerned with equations and deductions from equations -- however in modern terminology he was not working with equations in the language of Boolean algebras since his $+$ was a partial operation which could only be applied to disjoint elements.

W.S. JEVONS 1864

C.S. PEIRCE 1867

They suggest that Boole's exclusive + be replaced by the now common inclusive +.

C.S. PEIRCE 1880

Peirce presented a mathematical development of the algebra of logic based on the copula, denoted by $-\!\!<$. On pages 32-33 of this paper he gives what appears to be a flawless development of the equational axioms for lattices based on what we now call a partial order with g.l.b.s. and l.u.b.s. (He does not isolate the concept that we call lattices in any way -- this is just a fragment of his development of an algebra of logic.) There are two difficulties with his treatment. First, although the copula is treated like a partial order in this development, in previous pages and subsequent pages it acts like a binary operation, for example on page 34 one sees the expression $(a+b -\!\!< a) -\!\!< (b -\!\!< a)$. The second problem is that he claims the distributive laws follow from his definitions.

It is interesting to note the significance attached to each identity discovered. Peirce is careful about allocating credits, and his list includes:

$x = x + x;\ x \times x = x$	(Jevons 1864)
$a + b = b + a;\ a \times b = b \times a$	(Boole, Jevons)
$(a+b)+c = a+(b+c);\ a\times(b\times c) = (a\times b)\times c$	(Boole, Jevons)
$(a+b)\times c = (a\times c) + (b\times c)$	(Boole, Jevons)
$(a\times b)+c = (a+c)\times(b+c)$	(Peirce 1867)
$a+(a\times b) = a;\ a\times(a+b) = a$	(Grassmann, Schröder)

E. SCHRÖDER 1890 - 1895

Schröder was strongly influenced by Peirce's axiomatic approach to the algebra of logic and wrote three volumes (approximately 2,000 pages) on the subject. He followed the aforementioned development of Peirce, but used subsumption, denoted by $\Subset$, as his fundamental notion. Also he realized the distributive law could not be derived as Peirce had claimed, and indeed gives two counterexamples in the appendices to volume one. The difficulty he encountered in constructing a counterexample seems to indicate that he never achieved a thoroughly abstract view of the algebra of logic -- the counterexamples he constructed were intimately connected with deductive systems. The first counterexample was obtained by looking at deductively closed subsets of a collection of 990 quasigroup equations. (We note that Schröder had invented, equationally defined, and studied abstract quasigroups previously.) His second counterexample uses, in modern terminology, the subalgebras of the free Boolean algebra with three free generators.

R. DEDEKIND 1897

Dedekind realized that Schröder's development of the laws of logic overlapped considerably with his unpublished investigations into the laws which govern the combinations of modules (in algebraic number theory) using g.c.d. and l.c.m. Then, as a common abstraction, he defines in full generality what we now call lattices (he called them dualgroups) using the following set of axioms (replacing his operation symbols +,- by $\vee,\wedge$):

(1') $\alpha \vee \beta = \beta \vee \alpha$

(1") $\alpha \wedge \beta = \beta \wedge \alpha$

(2') $(\alpha\vee\beta)\vee\gamma = \alpha\vee(\beta\vee\gamma)$

(2") $(\alpha\wedge\beta)\wedge\gamma = \alpha\wedge(\beta\wedge\gamma)$

(3') $\alpha\vee(\alpha\wedge\beta) = \alpha$

(3") $\alpha\wedge(\alpha\vee\beta) = \alpha.$

Shortly after listing these axioms he proceeds to find the smallest examples of lattices which fail to satisfy (1) the modular law, and (2) the distributive law, namely the lattices we now call N_5 and M_5.

A.N. WHITEHEAD 1898

Whitehead's book Universal Algebra was an attempt to unify the study of the important algebraic systems -- all had two binary operations called addition and multiplication, and these operations satisfied several basic laws such as $a + b = b + a$, etc. Such algebras were divided into two basic types, those of numerical genus and those of non-numerical genus, the latter satisfying $a + a = a$. His only example of an algebra of non-numerical genus was the algebra of symbolic logic. Linear associative algebras give examples of algebras of the numerical genus. He does not treat scalar multiplication by complex numbers as fundamental operations requiring further axioms, but rather as a natural extension of writing $2a$ for $a + a$. By current standards his scope was extremely narrow, not even including groups.

E.V. HUNTINGTON 1904

Huntington gives three sets of postulates for the algebra of logic, one based on $\oplus, \odot$, one on $\oslash$, and one on $\oplus$. He does not use the word 'algebra' to describe a set with operations. However he does introduce systems $\langle K,\oplus,\odot\rangle$, $\langle K,\oslash\rangle$, and $\langle K,\oplus\rangle$ to prove his postulates are independent. In the appendix he suggests that one use the name logical field (analogous to Galois field) for systems $\langle K,\oplus,\odot,\oslash\rangle$ which satisfy the laws of the algebra of logic. Then he shows (1) every finite logical field has 2^m elements, and (2) for each m there is exactly one logical field with 2^m elements.

E.L. POST 1921

The completeness of the propositional calculus is proved, and n-valued logics are introduced.

O. FRINK 1928

He shows that every Boolean algebra can be considered as a ring using the operations symmetric difference and meet.

M.H. STONE 1935, 1936

Stone rediscovers the result of Frink above, and proves that conversely every Boolean ring can be considered as a Boolean algebra.

G. BIRKHOFF 1933

He proves that every distributive lattice can be represented as a ring of sets.

M.H. STONE 1934, 1936

Every Boolean algebra can be represented as a field of sets.

M.H. STONE 1934, 1937

Stone develops the duality between Boolean algebras and Boolean spaces.

M.H. STONE 1938

"I believe it would be accurate to say that of the many books, memoirs, notes, and reviews (more than one hundred seventy-five in number [6]) which deal with Boolean algebras the great majority draw their inspiration directly or indirectly from the work of Boole. The orientation of these studies toward symbolic logic is apparent in their preoccupation with algorithms, identities, and equations, or with the logical interrelations of the formal properties of the various Boolean operations. Recently there has emerged a different tendency, namely, to view Boolean algebras structurally, as organic systems, rather than algorithmically. Although this tendency might naturally have been expected to take its origin either in the rich experience of algebraists or in the needs of mathematicians concerned with the calculus of classes, it sprang, in fact, from quite different sources as a recognizable, if somewhat remote, consequence of the work of Hilbert. The most intensive exploitation of this new tendency is due to Tarski and myself [28]-[39]. Tarski's theory of deductive systems, which is but one illustration of the way in which logic has been enriched by the sort of metamathematical inquiry first seriously attempted by Hilbert, deals with systems of propositions which are complete with respect to logical inference; from a mathematical point of view, it is therefore a theory of the relations between special subalgebras of a Boolean algebra. My own investigations are a systematic attempt to discuss the structure of Boolean algebras by the methods which have thrown so much light on far deeper algebraic problems. The need for investigations of this character was suggested to me by the theory of operator-rings in Hilbert space: there, as in other rings and linear algebras, the 'spectral' representation as a 'direct sum' of irreducible subrings reposes in essence upon the construction of an abstract Boolean algebra; and this construction, trivial for rings with strong chain conditions, is not trivial in the case of operator-rings."

§3. THE DEVELOPMENT OF STRUCTURE THEOREMS FOR VARIETIES

N.H. McCOY and D. MONTGOMERY 1937

They point out that Stone's representation of Boolean rings by rings of sets is clearly equivalent to the statement that every Boolean ring is isomorphic to a subring of a direct sum of rings F_2. They go on to prove that every p-ring (a commutative ring satisfying $a^p = a$ and $pa = 0$) is isomorphic to a subring of a direct sum of rings F_p. One of their basic observations is that given (abstract) algebras A and B, $A \in ISP(B)$ iff there are homomorphisms from A to B which separate points.

I. GELFAND 1941

Gelfand showed that certain Banach algebras are isomorphic to the algebra of continuous functions $C(X,R)$ or $C(X,¢)$, where X is a compact Hausdorff space and R is the reals, $¢$ the complex numbers.

P.C. ROSENBLOOM 1942

Rosenbloom introduces the equational class P_n of n-valued Post algebras, for $n = 1,2,\ldots,$ and proves that the finite members of P_n are finite powers of the smallest nontrivial member P_n. He does not know if $P_n = ISP(P_n)$.

G. BIRKHOFF 1944

Birkhoff introduces the concepts of subdirect product (he calls it subdirect union) and subdirectly irreducible, and proves that every algebra is a subdirect product of subdirectly irreducible algebras.

L.I. WADE 1945

He proves that P_n is the only nontrivial subdirectly irreducible n-valued Post algebra.

§4. THE INTRODUCTION OF BOOLEAN POWERS

R.F. ARENS and I. KAPLANSKY 1948

They blend the ideas of Stone and Gelfand, and thus introduce the first Boolean constructions. "Stone [23, Theorem 1] has shown that a Boolean ring with unit is the set of all open and closed sets in a compact zero-dimensional space. In slightly different terminology: a Boolean ring with unit is the set of all continuous functions from a compact zero-dimensional space to the field GF(2) of two elements." Then they proceed to look at representations of the form $C(X,R)$ where X is a Boolean space and R is a simple ring or algebra, and generalizations of such representations. Thus they introduced, for rings, what is now the most popular definition of a bounded Boolean power, namely the algebra of continuous functions $C(X,R)$ where X is a Boolean space and R is given the discrete topology. (This gives a subdirect power of R.)

A.L. FOSTER 1953a

Foster was apparently working completely independently of Arens and Kaplansky when he presented his version of Boolean powers. Given any algebra A and Boolean algebra B he defined the universe of the Boolean power $A[B]$ to be

$$\{f \in B^A\colon f(a_1)\wedge f(a_2) = 0 \quad \text{if} \quad a_1 \neq a_2,\ \bigvee_{a \in A} f(a) = 1\}.$$

If A is infinite then B is required to be a complete Boolean algebra. The fundamental operations are defined on $A[B]$ by

$$F(f_1,\ldots,f_n)(a) = \bigvee_{F(a_1,\ldots,a_n)=a} f_1(a_1) \wedge \ldots \wedge f_n(a_n).$$

(In the case that A is Z_3 note that this is exactly the construction we developed in §1.)

Foster also introduced a notion of normal subdirect power, and proved that for special finite algebras (so-called f-algebras), normal subdirect powers were essentially the same as Boolean powers.

A.L. FOSTER 1961

Foster introduces the bounded Boolean power construction $A[B]^*$ by adding the requirement "$|\{a \in A\colon f(a) \neq 0\}| < \omega$" to the definition of $A[B]$. Thus for A finite, $A[B] = A[B]^*$.

B. JÓNSSON 1962

In his review of Foster's 1961 paper, Jónsson points out that $A[B]^*$ is, in a natural manner, isomorphic to $C(X,A)$, where X is the Boolean space of B.

M. GOULD and G. GRÄTZER 1967

They give a new, more general definition of normal subdirect power (based on the normal transform) and prove that this construction is equivalent to the bounded Boolean power.

C.J. ASH 1975

S. BURRIS 1975

If we let $P_B(K)$ denote the class of all bounded Boolean powers of algebras in K then one has $P_B \cdot P_B \leq I \cdot P_B$. This is based on the observation that $(A[B_1]^*)[B_2]^* \cong A[B_1 * B_2]^*$, $B_1 * B_2$ being the free product of B_1 and B_2.

§5. BOUNDED BOOLEAN POWER REPRESENTATION THEOREMS FOR VARIETIES

In the following $\mathcal{BA}$ denotes the variety of Boolean algebras.

M.H. STONE 1934, 1936

(rephrased) Let $\underset{\sim}{2}$ be a two-element Boolean algebra. Then $\mathcal{BA} = IP_B(\underset{\sim}{2})$.

R.F. ARENS and I. KAPLANSKY 1948

For F a finite field, $\{$algebras over F$\} = IP_B(F)$.

A.L. FOSTER 1953a/b

For A a primal algebra, $V(A) = IP_B(A)$.

R. QUACKENBUSH 1980

For finite algebras A, $V(A) = IP_B(A)$ iff A is quasiprimal with no proper subalgebras or A is simple modular-Abelian with a trivial subalgebra.

S. BURRIS and R. McKENZIE 1981

A variety V can be expressed as $IP_B(K)$ for some finite set K of finite algebras iff $V = V(A)$ where (a) A is quasiprimal with no proper subalgebras, or (b) A is a finite simple modular-Abelian algebra.

§6. DIRECT PRODUCT PHENOMENA AND THE NUMBER OF MODELS

Bounded Boolean powers have been extremely useful to show that the various direct product phenomena observed by Hanf in $\mathcal{BA}$ transfer to numerous other varieties, and to show that many varieties have the maximum possible number of isomorphism types of algebras in all suitably high powers. The key concept is that of a B-separating algebra -- A is such an algebra if for any $B_1, B_2 \in \mathcal{BA}$, $A[B_1]^* \cong A[B_2]^* \Rightarrow B_1 \cong B_2$.

W. HANF 1957

Hanf proved the following results:

(1) There exist denumerable Boolean algebras B_1 and B_2, given a positive integer n, such that for any positive integers m,k we have $B_1{}^m \cong B_2{}^m \times B_2{}^k$ iff $n|k$.

(2) There exist denumerable Boolean algebras B_1 and B_2, given n, such that $B_1{}^k \cong B_2{}^k$ iff $n|k$. (This was pointed out by Tarski.)

(3) There exists, for any $n \geq 2$, a Boolean algebra B such that $B \cong B \times \underset{\sim}{2}^n$ but $B \ncong B \times \underset{\sim}{2}^k$ for $k = 1,\ldots,n-1$.

(4) There exists, for any $n \geq 3$, a Boolean algebra B such that $B \cong B^n$ but $B \ncong B^k$ for $k = 2,3,\ldots,n-1$.

(5) There exist Boolean algebras B_1 and B_2 such that $B_1 \times B_2 \cong B_1 \times B_2 \times \underset{\sim}{2}$ but neither $B_1 \cong B_1 \times \underset{\sim}{2}$ nor $B_2 \cong B_2 \times \underset{\sim}{2}$.

A. TARSKI 1957

Letting A be the semigroup $\langle\omega,+\rangle$ Tarski shows that $A[B_1 \times B_2]^* \cong A[B_1]^* \times A[B_2]^*$, and also that A is B-separating. From this he concludes that the Hanf phenomena above (replacing $\underset{\sim}{2}$ by A) apply to commutative semigroups.

B. JÓNSSON 1957

Jónsson shows that indecomposable centerless countable algebras (defined within a special class of algebras) are B-separating, and hence again we have the Hanf phenomena.

G. BERGMAN 1972

He shows that if M is any module and B_1,B_2 are Boolean algebras of the same cardinality then $M[B_1]^* \cong M[B_2]^*$.

S. BURRIS 1975

(1) In this paper it is noted that if A is a B-separating algebra then $IP_B(A)$ has 2^κ isomorphism types of algebras for each $\kappa \geq |A|$.

(2) If S is an algebra such that for every positive n, $|\mathrm{Con}\, S^n| = 2^n$, then S is B-separating. In particular this shows that the nontrivial simple algebras in congruence-distributive varieties are B-separating.

J. KETONEN 1978

Ketonen vastly increases the possibilities for curious direct product phenomena in Boolean algebras by showing that any countable commutative semigroup can be embedded into the semigroup of isomorphism types of countable Boolean algebras under direct product.

J. LAWRENCE 1981

Lawrence shows the following results for groups:

(1) Every finite subdirectly irreducible group is B-separating.

(2) $G \times G$ is not B-separating for any group G.

K. HICKIN and J.M. PLOTKIN 1981

They continue the study of groups and prove:

(1) If G is a nonabelian group which (i) is not a central product of two nonabelian groups, or (ii) is finitely subdirectly irreducible, then G is B-separating.

(2) If G is a finitely generated nonabelian group then G has 2^{ω} countable Boolean powers.

J.T. BALDWIN and R.N. McKENZIE [a]

Using Boolean powers to help count the number of models in universal Horn classes they prove:

(1) Every nonabelian subdirectly irreducible algebra in a modular variety is B-separating.

(2) Every countable nonabelian algebra A has 2^{λ} distinct bounded Boolean powers of power λ for every uncountable λ, each of which is elementarily equivalent to $A[F_{BA}(\omega)]^*$.

§7. BOUNDED BOOLEAN POWERS AND INJECTIVES

B.A. DAVEY and H. WERNER 1979

A series of papers, starting in 1972, which show that in certain varieties the injectives, or weak injectives, are of the form (*) $A_1[B_1]^* \times \ldots \times A_n[B_n]^*$, where the A_i's are certain subdirectly irreducible algebras and the B_i's are complete Boolean algebras, are brought under the following theorem.

Let V be a variety, let K be a finite set of finite algebras from V and suppose $V_{SI} \subseteq IS(K)$, where V_{SI} is the class of subdirectly irreducibles in V. If there is a simplicity formula for K and K has factorizable congruences then the following are equivalent:

(i) A is a [weak] injective in V

(ii) A is of the form (*) above where each $A_i \in H(K) \cap V_{SI}$, A_i is a [weak] injective in V, B_i is a complete Boolean algebra, and the A_i are pairwise nonisomorphic.

P.H. KRAUSS [a]

Krauss shows that in filtral varieties with a finite number of nonisomorphic simple members in each finite cardinal the [weak] injectives are characterized as direct products of bounded Boolean powers of [weak] V_{SI}-injectives using complete Boolean algebras.

§8. RIGID ALGEBRAS

An algebra A is rigid if it has exactly one automorphism.

B. JÓNSSON 1951

Answering Problem 74 of Birkhoff's Lattice Theory Jónsson proves that there is an infinite rigid Boolean algebra.

S. BURRIS 1978 [b]

Suppose that S is a finitely generated algebra which is rigid and $|\text{Con } S^n| = 2^n$ for all positive n. Then if B is a rigid Boolean algebra it follows that $S[B]^*$ is rigid.

J.D. MONK and W. RASSBACH 1979

They prove there exist 2^κ rigid Boolean algebras in every uncountable cardinal κ.

§9. MATRIX RINGS

In the following R denotes a Boolean ring, B the corresponding Boolean algebra, and S an arbitrary ring.

J.G. ROSENSTEIN 1972

He proves that $GL_2(R) \cong GL_2(F_2)[B]^*$.

H. GONSHOR 1975

Gonshor generalizes and simplifies Rosenstein's work in his proof of $GL_n(R) \cong GL_n(F_2)[B]^*$ for n any positive integer.

S. BURRIS and H. WERNER 1980

Specializations of the results in this paper show that

(1) $M_n(S[B]^*) \cong M_n(S)[B]^*$

(2) $GL_n(S[B]^*) \cong GL_n(S)[B]^*$

(3) $SL_n(S[B]^*) \cong SL_n(S)[B]^*$

(4) $PSL_n(S[B]^*) \cong PSL_n(S)[B]^*$.

§10. FIRST ORDER ASPECTS OF BOOLEAN POWERS

A. TARSKI 1949

The elementary types of Boolean algebras are characterized (using the Tarski invariants). Also the theory of Boolean algebras is proved to be decidable.

YU. L. ERSHOV 1964

Ershov shows that for every Boolean algebra B there is a filter F over ω

such that $B \equiv 2^{\omega}/F$.

YU. L. ERSHOV 1967

He shows that if P is a primal algebra then one can semantically embed the variety $V(P)$ into $\mathcal{BA}$. (We did this in §1 for the case $P = Z_3$.)

A. WOJCIECHOWSKA 1969

She gives a Feferman-Vaught analysis of $A[B]^*$. From this it follows that $A[B]^*$ preserves elementary equivalence and elementary embeddings in both arguments -- see also Burris 1975, Ash 1975.

R. MANSFIELD 1971

Mansfield proves that two structures are elementarily equivalent iff they have isomorphic Boolean ultrapowers.

J.T. BALDWIN and A.H. LACHLAN 1973

They show that if A is a finite structure and B is the denumerable free Boolean algebra then $A[B]^*$ is ω-categorical.

B. WEGLORZ 1974

He shows that free products of Boolean algebras preserve $\equiv$.

S. BURRIS 1975

This paper contains the following results:

(1) If A is a finite algebra and B is a complete Boolean algebra then $A[B]^*$ is equationally compact.
(2) If A is a finite B-separating algebra then $A[B_1]^* \equiv A[B_2]^*$ implies $B_1 \equiv B_2$.
(3) Every bounded Boolean power of an algebra A is elementarily equivalent to a reduced power of A, and vice-versa.
(4) A first-order sentence is preserved by bounded Boolean powers iff it is equivalent to a disjunction of Horn sentences.
(5) An elementary class K is closed under bounded Boolean powers iff it is closed under reduced powers iff it is defined by a set of disjunctions of Horn sentences.

S. BURRIS 1978 [a]

We say that $A \equiv_n B$ if A and B satisfy the same sentences with at most n alternations of quantifiers. In this paper it is proved that if A is a finite B-separating algebra then for any positive n there exist Boolean algebras B_1, B_2 such that $A[B_1]^* \equiv_n A[B_2]^*$ but $A[B_1]^* \not\equiv A[B_2]^*$.

B. BANASCHEWSKI and E. NELSON 1980

They show $A[B]$ preserves elementary equivalence and elementary embeddings in both arguments, that $A[B]^* \equiv A[B]$, and the canonical embedding of $A[B]^*$ into $A[B]$ is elementary.

S. GARAVAGLIA and J.M. PLOTKIN [a]

They construct an infinite B-separating structure A and two Boolean algebras B_1 and B_2 such that $A[B_1]^* \equiv A[B_2]^*$ but $B_1 \not\equiv B_2$.

§11. FILTERED BOOLEAN POWERS

R.F. ARENS and I. KAPLANSKY 1948

They realized that bounded Boolean powers were going to be severely limited as a method of proving representation theorems for rings, so they introduced two generalizations of this construction, the first of which we call a filtered Boolean power. This construction proceeds as follows (we describe it for arbitrary algebras, whereas they were only concerned with rings): Let A be an algebra and let A_i, $i \in I$, be the family of its subalgebras indexed by some set I. Then, given a Boolean space X and an indexed family $(X_i)_{i \in I}$ of closed subsets we construct the subalgebra of A^X whose universe is given by $\{f \in C(X,A) : f(X_i) \subseteq A_i \text{ for } i \in I\}$. Given a class of algebras K let $P_{FB}(K)$ denote the class of all filtered Boolean powers of members of K. In the following we use $V_{\omega_1}(K)$ to denote the countable members in the variety $V(K)$. Arens and Kaplansky proved the following two results on filtered Boolean powers:

(1) For the variety $V(F_4)$ of rings generated by the 4-element field F_4 one has $V(F_4) \neq IP_{FB}(F_4)$.

(2) For any finite field F, $V_{\omega_1}(F) \subseteq IP_{FB}(F)$.

M.O. RABIN 1969

In this paper Rabin proves, as a corollary to his work on two successor functions, that the theory of countable Boolean algebras with quantification over filters is decidable.

S.D. COMER 1974

Comer realized that the result (2) of Arens and Kaplansky above could be used to interpret the theory of $(x^m = x)$-rings into the theory of countable Boolean algebras with quantification over filters; hence the theory of $(x^m = x)$-rings is decidable.

S.D. COMER 1975

Comer shows that if A is a finite monadic algebra then there is another finite monadic algebra A' such that $V_{\omega_1}(A) \subseteq IP_{FB}(A')$. Then using Rabin's result he concludes that any finitely generated variety of monadic algebras has a decidable theory.

H. WERNER 1978

S. BURRIS and H. WERNER 1979

Werner extends Comer's methods to show that if $V(A)$ is a finitely generated discriminator variety then there is a finite algebra A' such that $V_{\omega_1}(A) \subseteq IP_{FB}(A')$; hence if $V(A)$ is also of finite type then it has a decidable theory.

S. BURRIS and R. McKENZIE 1981

In this monograph there are three fundamental theorems on filtered Boolean powers (= sub-Boolean powers):

(1) For a finite algebra C, $V(C) = IP_{FB}(C)$ iff the following conditions hold:

(i) $C = A \times D$ where A is modular-Abelian and D generates a discriminator variety.

(ii) $V(C)$ is congruence permutable.

(iii) If A and D are both nontrivial then they both have trivial subalgebras.

(iv) $V(A) = IP_{FB}(A)$ and $V(D) = IP_{FB}(D)$.

(2) If A is a quasiprimal algebra then $V(A) = IP_{FB}(A)$ iff every isomorphism between nontrivial subalgebras of A has a unique extension to an automorphism of A, and the only automorphism of A with a fixed point is the identity map.

(3) If A is a quasiprimal algebra then $V_{\omega_1}(A) \subset IP_{FB}(A)$ iff every isomorphism between nontrivial subalgebras of A extends to an automorphism of A.

§12. MODIFYING BOUNDED BOOLEAN POWERS USING HOMEOMORPHISMS

This modification of bounded Boolean powers introduced by Arens and Kaplansky is a more applicable, less tractable construction for representations, as is the Boolean product in the following sections.

R.F. ARENS and I. KAPLANSKY 1948

They show that if R is a ring of characteristic p such that each element satisfies $x^{p^n} = x$ then there is a Boolean space X with a homeomorphism α whose n^{th} power is the identity such that, letting F be the finite field of order p^n, we have R is isomorphic to the subring of $C(X,F)$ whose universe is

$$\{f \in C(X,F) : f(\alpha x) = (f(x))^p \text{ for } x \in X\}.$$

K. KEIMEL and H. WERNER 1974

They generalize the above to obtain representations for finitely generated discriminator varieties.

A. WOLF 1975

If G is a group, let $\mathcal{BA}(G)$ be the variety of Boolean algebras expanded by the group of automorphisms G. Wolf shows that if G is a finite solvable group then $\mathcal{BA}(G)$ has a decidable theory, and uses this to show that varieties generated by certain quasiprimals have a decidable theory.

S. BURRIS [b]

For G a finite group $\mathcal{BA}(G)$ has a decidable theory.

§13. THE DEFINITION OF BOOLEAN PRODUCTS

We will use the notation $A \leq_{s.d.} \prod_{x\in X} A_x$ to mean that A is a subdirect product of the indexed family of algebras $(A_x)_{x\in X}$. For $\Phi(x_1,\ldots,x_n)$ a first-order formula and $f_1,\ldots,f_n \in A$, let $[\![\Phi(f_1,\ldots,f_n)]\!] = \{x \in X\colon A_x \models \Phi(f_1(x),\ldots,f_n(x))\}$

An algebra A is a Boolean product of members of K if there is a family $(A_x)_{x\in X}$ of algebras $A_x \in K$ indexed by a Boolean space X such that

(i) $A \leq_{s.d.} \prod_{x\in X} A_x$

(ii) (atomic extension property) for $f,g \in A$, $[\![f = g]\!]$ is a clopen subset of X.

(iii) (Patchwork property) for $f,g \in A$ and N a clopen subset of X we have $f\restriction_N \cup g\restriction_{X-N} \in A$.

The Boolean product construction was introduced by Burris and Werner [1979] as a reformulation of the Boolean sheaf construction, popularized by Dauns and Hofmann [1966]. Given a class K of algebras we let $\Gamma^a(K)$ denote the class of Boolean products of members of K. On can check that $P_B \leq P_{FB} \leq \Gamma^a$.

§14. BOOLEAN PRODUCT REPRESENTATION THEOREMS

If V is a variety let V_{SI} be the subdirectly irreducible members of V, let V_S be the simple algebras in V, and let V_{DI} be the directly indecomposable members of V.

J. DAUNS and K.H. HOFMANN 1966

They prove that for R a biregular ring one has $R \in I\Gamma^a(K)$ where K is the class of simple rings with 1 (in the language $\{+,\cdot,-,0\}$).

R.S. PIERCE 1967

In this study of Boolean product representations of rings (in the language $\{+,\cdot,-,0,1\}$) he states and proves the following:

(1) "Roughly speaking we would like to obtain a representation of rings by means of indecomposable rings."

(2) For R a commutative ring, $R \in I\Gamma^a(CR_{DI})$, CR being the variety of commutative rings.

(3) For R a commutative regular ring, $R \in I\Gamma^a(F)$, F being the class of fields.

(4) For any ring R a Boolean product representation is constructed using the central idempotents of R. (This construction is now called the Pierce sheaf of R.)

S.D. COMER 1971

He discusses a general result to the effect that if the factor congruences of an algebra form a Boolean algebra then one obtains a Boolean product representation of the algebra in a natural way.

S.D. COMER 1972

Letting CA_n be the variety of cylindric algebras of dimension n he shows that $CA_n = I\Gamma^a((CA_n)_S)$.

K. KEIMEL and H. WERNER 1974

They show that for V a finitely generated discriminator variety we have $V = I\Gamma^a(V_S)$.

S. BULMAN-FLEMING and H. WERNER 1977

They improve on the previous result by showing that for any discriminator variety V, $V = I\Gamma^a(V_S)$.

W.D. BURGESS and W. STEPHENSON 1978

They show that iterations of the Pierce sheaf construction (applied to rings) need not terminate in finitely many steps with directly indecomposable stalks.

W.D. BURGESS and W. STEPHENSON 1979

Let R be the class of rings in the language $\{+,\cdot,-,0,1\}$. Then $R \in I\Gamma^a(R_{DI})$ iff every idempotent of R is central.

H. WERNER 1978

S. BURRIS and H. WERNER 1979

These papers contain Werner's generalization of Comer's key result on monadic algebras, namely Werner shows that for K a finite set of finite algebras there exists a finite algebra A' such that $\{A \in \Gamma^a(K) : |A| \le \omega\} \subseteq IP_{FB}(A')$. This is a key step in proving the decidability of finitely generated discriminator varieties of finite type.

S. BURRIS and R. McKENZIE 1981

The limitations of using Boolean constructions for representation theorems is most clearly set forth in the following result from this monograph: Let V be a finitely generated variety. Then there is a finite set K of finite algebras such that $V = I\Gamma^a(K)$ iff $V = V_{ab} \otimes V_{discr}$ and the ring $R(V_{ab})$ associated with V_{ab} is of finite representation type. (V_{ab} is an Abelian subvariety of V, V_{discr} is a discriminator subvariety of V.)

S. BURRIS [a]

D.M. CLARK and P.H. KRAUSS [a]

Suppose V is a congruence-distributive variety. Then $V = I\Gamma^a(V_{SI})$ iff V is a discriminator variety.

§15. FIRST-ORDER ASPECTS OF BOOLEAN PRODUCTS

A. MACINTYRE 1973

Macintyre uses Boolean products to study the model companions of classes of rings, giving conditions which ensure that K has a model-complete theory implies certain Boolean products of K have a model-complete theory.

S.D. COMER 1974

Let Γ^e be the class operator obtained by replacing condition (ii) of the definition of Γ^a by: (ii') $[\![\Phi(\vec{f})]\!]$ is clopen for any first-order formula. Comer presents a Feferman-Vaught theorem for Γ^e.

S.D. COMER 1976

Comer generalizes Macintyre's conditions to study model companions of varieties of monadic algebras.

S. BURRIS and H. WERNER 1979

This paper is devoted to the elementary properties of Boolean products and includes the following results:

(1) $ISP_R = IS\Gamma^e_0 S^{(\alpha)} P_U$.

(2) Any finitely generated universal Horn class has a model companion.

(3) If V is a discriminator variety and V_S has a model companion then V has a model companion.

(4) If K is a model-complete elementary class with a discriminator formula then $ISP_R(K)$ has a model companion, and the algebraically closed members form an elementary class. Both are described using Boolean products.

(5) A sentence is preserved by Γ^e iff it is equivalent to a Horn sentence. (This answers Prob. 1 of Mansfield [1977].)

P.H. KRAUSS [a]

In this paper Krauss uses Boolean products to characterize the algebraically closed and the existentially closed members of filtral varieties, and to describe injectives in these varieties.

S. BURRIS and R. McKENZIE 1981

A discriminator formula for the class of simple aglebras in a variety with equationally definable principal congruences is given.

S. BURRIS [c]

Using the Boolean product construction the following are proved:

(1) If T^* is the model companion of a finitely generated universal Horn class $ISP(K)$ then the following are equivalent: (a) T^* is ω - categorical, (b) T^* is complete, (c) $ISP(K)$ has the joint embedding property, (d) $ISP(K) = ISP(A)$ for some finite A. (We assume the language is finite.)

(2) For T^* as above, T^* admits a primitive recursive elimination of quantifiers. As the theory T^* is primitive recursive, it follows that T^* is decidable.

§16. DOUBLE BOOLEAN POWERS

I discovered double Boolean powers in late 1978 while constructing directly indecomposable algebras, and shortly thereafter realized their value in proving undecidability results. McKenzie modified this construction yet further in order to prove the wide-ranging undecidability results of our 1981 Memoir. It is quite remarkable that both our best decidability and our best undecidability results depend on Boolean constructions.

M. RUBIN 1976

Rubin answers a longstanding question on monadic algebras by showing their first-order theory is undecidable. As a consequence the theory of Boolean pairs BP, the class of Boolean algebras with a distinguished subalgebra, is undecidable.

Let us use this result to show that the variety generated by the three-element

Heyting algebra $H = \langle\{0,e,1\},\vee,\wedge,\rightarrow,0,1\rangle$ has an undecidable theory. Given a field B of subsets of an index set I and a subfield B_0 of B let us define the subalgebra $H(B,B_0)$ of H^I by letting its universe be

$$\{f \in H^I\colon f^{-1}(0) \in B_0,\quad f^{-1}(1) \in B\}.$$

For $X \subseteq I$ let χ_X be defined by

$$\chi_X = \begin{cases} 1 & \text{if } i \in X \\ e & \text{if } i \notin X \end{cases},$$

and let e^* be the constant function in $H(B,B_0)$ with value e. Then

$$C \overset{\text{def}}{=} \{\chi_X\colon X \in B\} = \{f \vee e^*\colon f \in H(B,B_0)\}$$

$$C_0 \overset{\text{def}}{=} \{\chi_X\colon X \in B_0\} = \{(e^* \rightarrow f) \vee e^*\colon f \in H(B,B_0)\}.$$

Now we clearly have an isomorphism between the structures $\langle B,B_0,\subseteq\rangle$ and $\langle C,C_0,\leq\rangle$; hence we can semantically embed $\mathcal{BP}$ into $V(H)$.

S. BURRIS and R. McKENZIE 1981

Double Boolean powers are used along with a modification of a technique of Zamjatin and results from the study of the modular comutator to show that if a locally finite modular variety has a decidable theory then it decomposes into the product of an Abelian variety and a discriminator variety. Then it is shown that for finitely generated varieties of finite type which are modular the decidability question reduces to the decidability question for all unitary left R-modules, for R a finite ring with 1.

S. BURRIS and J. LAWRENCE [a]

Double Boolean powers are used to give brief proofs of Ershov's theorem on decidable varieties of groups and Zamjatin's results on decidable varieties of rings with 1.

S. BURRIS [b]

Using double Boolean powers this paper shows that if G is not a locally finite group then $\mathcal{BA}(G)$ has an undecidable theory.

Acknowledgements: This work has been supported by NSERC Grant No. A7256.

REFERENCES

R.F. ARENS and I. KAPLANSKY
[1948] Topological representations of algebras, *Trans. Amer. Math. Soc.* 63, 457-481.

C.J. ASH
[1975] Reduced powers and Boolean extensions, *J. London Math. Soc.* 9, 429-432.

J.T. BALDWIN and A.H. LACHLAN
[1973] On Universal Horn classes, *Algebra Universalis* 3, 98-111.

J.T. BALDWIN and R.N. McKENZIE
[a] Counting models in universal Horn classes [Preprint 1981].

B. BANASCHEWSKI and E. NELSON
[1980] Boolean powers as algebras of continuous functions, *Dissertationes Mathematicae* 179, Warsaw.

G. BERGMAN
[1972] Boolean rings of projections maps, *J. London Math. Soc.* 4, 593-598.

G. BIRKHOFF
[1933] On the combination of subalgebras, *Proc. Camb. Philos. Soc.* 29, 441-464.

[1935] On the structure of abstract algebras, *Proc. Camb. Philos. Soc.* 31, 443-445.

[1944] Subdirect unions in universal algebra, *Bull. Amer. Math. Soc.* 50, 764-768.

G. BOOLE
[1847] The mathematical analysis of logic.

[1854] An investigation of the Laws of thought.

S. BULMAN-FLEMING and H. WERNER
[1977] Equational compactness in quasi-primal varieties, *Algebra Universalis* 7, 33-46.

W.D. BURGESS and W. STEPHENSON
[1976] Pierce sheaves of non-commutative rings, *Communications in Algebra* 4, 51-75.

[1978] An analogue of the Pierce sheaf for non-commutative rings, *Communications in Algebra* 6, 863-886.

[1979] Rings all of whose Pierce stalks are local, *Canad. Math. Bull.* 22, 159-164.

S. BURRIS
[1975] Boolean powers, *Algebra Universalis* 5, 341-360.

[1978a] Bounded Boolean powers and $\equiv_n$, *Algebra Universalis* 8, 137-138.

[1978b] Rigid Boolean powers, *Algebra Universalis* 8, 264-265.

[a] A note on directly indecomposable algebras (to appear in *Algebra Universalis*).

[b] The first-order theory of Boolean algebras with a distinguished group of automorphisms (to appear in *Algebra Universalis*).

[c] Model companions for finitely generated universal Horn classes (to appear in the *J. of Symbolic Logic*).

S. BURRIS and J. LAWRENCE
[a] Two undecidability results using modified Boolean powers (to appear in the *Canad. J. of Math.*).

S. BURRIS and R. McKENZIE
[1981] Decidability and Boolean Representations, *Memoirs Amer. Math. Soc.* No. 246.

S. BURRIS and H. WERNER
[1979] Sheaf constructions and their elementary properties, *Trans. Amer. Math. Soc.* 248, 269-309.

[1980] Remarks on Boolean products, *Algebra Universalis* 10, 333-344.

D.M. CLARK and P.H. KRAUSS
[a] Boolean representation of congruence distributive varieties, Preprint No. 19/79 *Gesamthochschule Kassel* Dec. 1979.

S.D. COMER
[1971] Representations by algebras of sections over Boolean spaces, *Pacific J. Math.* 38, 29-38.

[1972] A sheaf theoretic duality for cylindric algebras, *Trans. Amer. Math. Soc.* 169, 75-87.

[1974] Elementary properties of structures of sections, *Bol. Soc. Math. Mexicana* 19, 78-85.

[1975] Monadic algebras with finite degree, *Algebra Universalis* 5, 315-327.

[1976] Complete and model-complete theories of monadic algebras, *Colloq. Math.* 34, 183-190.

J. DAUNS and K.H. HOFMANN
[1966] The representation of biregular rings by sheaves, *Math. Z.* 91, 103-123.

R. DEDEKIND
[1897] Über Zerlegungen von Zahlen durch ihre grössten gemeinsamen Teiler, *Festschrift Techn. Hoch. Braunschweig.*

B.A. DAVEY and H. WERNER
[1979] Injectivity and Boolean powers, *Math Z.* 166, 205-223.

YU. L. ERSHOV
[1964] Decidability of the elementary theory of relatively complemented distributive lattices and the theory of filters, *Algebra i Logika Sem.* 3, 17-38.(Russian)

[1967] On the elementary theory of Post varieties, *Alg. i. Logika* 6, 7-15. (Russian)

A.L. FOSTER
[1945] The idempotent elements of a commutative ring form a Boolean algebra; ring duality and transformation theory, *Duke Math. J.* 12, 143-152.

[1953a] Generalized "Boolean" theory of universal algebras. Part I: Subdirect sums and normal representation theorem, *Math. Z.* 58, 306-336.

[1953b] Generalized "Boolean" theory of universal algebras. Part II: Identities and subdirect sums in functionally complete algebras, *Math. Z.* 59, 191-199.

[1961] Functional completeness in the small. Algebraic structure theorems and identities, *Math. Ann.* 143, 29-53.

O. FRINK
[1928] On the existence of linear algebras in Boolean algebras, *Bull. Amer. Math. Soc.* 34, 329-333.

S. GARAVAGLIA and J.M. PLOTKIN
[a] Separation properties and Boolean powers.

I. GELFAND
[1941] Normierte Ringe. *Rec. Math. (Mat. Sbornik)* N.S. 9, 1-23.

H. GONSHOR
[1975] On $GL_n(B)$ where B is a Boolean ring, *Canad. Math. Bull.* 18, 209-215.

M. GOULD and G. GRÄTZER
[1967] Boolean extensions and normal subdirect powers of finite universal algebras, *Math. Z.* 99, 16-25.

W. HANF
[1957] On some fundamental problems concerning isomorphism of Boolean algebras, *Math. Scand.* 5, 205-217.

K. HICKIN and J.M. PLOTKIN
[1981] Boolean powers: Direct decomposition and isomorphism types, *Trans. Amer. Math. Soc.* 265, 607-621.

E.V. HUNTINGTON
[1904] Sets of independent postulates for the algebra of logic, *Trans. Amer. Math. Soc.* 5, 288-309.

W.S. JEVONS
[1864] Pure Logic, *London, E. Stanford.*

B. JÓNSSON
[1951] A Boolean algebra without proper automorphisms, *Proc. Amer. Math. Soc.* 2, 766-770.

[1957] On isomorphism types of groups and other algebraic systems, *Math. Scand.* 5, 224-229.

[1962] Review of Foster's 1961 paper, *Math. Rev.* 23, No. A.85.

K. KEIMEL and H. WERNER
[1974] Stone duality for varieties generated by quasiprimal algebras, *Memoirs Amer. Math. Soc.* No. 148, 59-85.

J. KETONEN
[1978] The structure of countable Boolean algebras, *Ann. of Math.* (2) 108, 41-89.

P.H. KRAUSS
[a] The structure of filtral varieties, *Gesamthochschule Kassel, Reprint No. 6/81*, June, 1981.

J. LAWRENCE
[1981] Boolean powers of groups, *Proc. Amer. Math. Soc.* 82, 512-515.

A. MACINTYRE
[1973/74] Model completeness for sheaves of structures, *Fund. Math.* 81, 73-89.

R. MANSFIELD
[1971] The theory of Boolean ultrapowers, *Ann. of Math. Logic* 2, 297-325.

[1977] Sheaves and normal submodels, *J. of Symbolic Logic* 42, 241-250.

N.H. McCOY and D. MONTGOMERY
[1937] A representation of generalized Boolean rings, *Duke Math. J.* 3, 455-459.

R. McKENZIE and J.D. MONK
[1973] On automorphism groups of Boolean algebras, *Colloquia Mathematica Societatis Janos Boylai*, Keszthely, Hungary, 951-988.

J.D. MONK and W. RASSBACH
[1979] The number of rigid Boolean algebras, *Algebra Universalis* 9, 207-210.

C.S. PEIRCE
[1867] On an improvement in Boole's calculus of logic, *Proc. of Amer. Acad. of Arts and Sciences* 7, 250-261.

[1880] On the algebra of logic, *Amer. J. Math.* 3, 15-57.

R.S. PIERCE
[1967] Modules over Commutative Regular Rings, *Memoirs Amer. Math. Soc.* No. 70.

E.L. POST
[1921] Introduction to a general theory of elementary propositions, *Amer. J. of Math* 43, 163-185.

R. QUACKENBUSH
[1980] Algebras with minimum spectrum, *Algebra Universalis* 10, 117-129.

M.O. RABIN
[1969] Decidability of second-order theories and automata on infinite trees, *Trans. Amer. Math. Soc.* 141, 1-35.

P.C. ROSENBLOOM
[1942] Post algebras I. Postulates and general theory, *Amer. J. Math.* 64, 167-188.

J.G. ROSENSTEIN
[1972] On $GL_2(R)$ where R is a Boolean ring, *Canad. Math. Bull.* 15, 263-275.

M. RUBIN
[1976] The theory of Boolean algebras with a distinguished subalgebra is undecidable, *Ann. Sci. Univ. Clermont No. 60 Math. No. 13*, 129-134.

E. SCHRÖDER
[1966] Die Algebra der Logik (3 vols.), *Chelsea Publishing Co., N.Y.*

M.H. STONE
[1934] Boolean algebras and their application to topology, *Proc. N.A.S.* 20, 197-202.

[1935] Subsumption of the theory of Boolean algebras under the theory of rings, *Proc. N.A.S.* 21, 103-105.

[1936] The theory of representations for Boolean algebras, *Trans. Amer. Math. Soc.* 40, 37-111.

[1937] Applications of the theory of Boolean rings to general topology, *Trans. Amer. Math. Soc.* 41, 375-481.

[1938] The representation of Boolean Algebras, *Bull. Amer. Math. Soc.* 44, 807-816.

A. TARSKI
[1949] Arithmetical classes and types of mathematical systems, mathematical aspects of arithmetical classes and types, arithmetical classes and types of Boolean algebras, arithmetical classes and types of algebraically closed and real-closed fields, *Bull. Amer. Math. Soc.* 55, 63-64.

[1957] Remarks on direct products of commutative semigroups, *Math. Scand.* 5, 218-223.

L.I. WADE
[1945] Post algebras and rings, *Duke Math. J.* 12, 389-395.

B. WEGLORZ
[1974] Some remarks on reduced powers, (Abstract) *J. Symbolic Logic* 39, 387.

H. WERNER
[1978] Discriminator Algebras. Studien zur Algebra und ihre Anwendungen, Band 6, *Akademie-Verlag*, Berlin.

A.N. WHITEHEAD
[1898] A Treatise on Universal Algebra, with Applications, Vol. 1, *Cambridge*.

A. WOJCIECHOWSKA
[1969] Generalized limit powers, *Bull. Acad. Polon. Sci. Ser. Sci. Math. Astronom. Phys.* 17, 121-122.

A. WOLF
[1975] Decidability for Boolean algebras with automorphisms, *Notices Amer. Math. Soc.* #75t-E73, 22, No. 164, p.A-648.

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada, N2L 3G1

EXTENSION OF POLYGROUPS BY POLYGROUPS

AND THEIR REPRESENTATIONS USING COLOR SCHEMES

Stephen D. Comer*

In this paper we introduce a construction for building a "big" polygroup from two "small" ones and show that the important classes of polygroups are closed under this construction. In general, it is very hard to determine whether a given polygroup is chromatic or not. A sufficient condition was given in Section 5 of [2] and generalized in [3]. The construction here gives an easy way to show that a large number of polygroups are chromatic. In view of Theorem 5 perhaps the product $\mathfrak{A}[\mathfrak{B}]$ could be called the *wreath product* of $\mathfrak{A}$ by $\mathfrak{B}$.

To make the paper reasonably self-contained basic definitions are collected in Section 1. The product construction $\mathfrak{A}[\mathfrak{B}]$ is described in Section 2. Section 3 contains the main results, namely, that the product operation $\mathfrak{A}[\mathfrak{B}]$ preserves various properties. For example Theorems 2 and 6 show that polygroups $\mathfrak{A}$ and $\mathfrak{B}$ are chromatic iff $\mathfrak{A}[\mathfrak{B}]$ is chromatic. An easy application of the product construction to the study of relation algebras is given in Section 4.

1. PRELIMINARIES. We recall a few basic definitions from [2].

A *polygroup* is a system $\mathfrak{M} = \langle M, \cdot, e, ^{-1}\rangle$ where $e \in M$, $^{-1}$ is a unary operation on M, $\cdot$ maps M^2 into nonempty subsets of M, and the following axioms hold for all $x,y,z \in M$:

(P_1) $(x\cdot y)\cdot z = x\cdot(y\cdot z)$

(P_2) $x\cdot e = x = e\cdot x$

(P_3) $x \in y\cdot z$ implies $y \in x\cdot z^{-1}$ and $z \in y^{-1}\cdot x$.

Many important polygroups are derived from color schemes, a notion that extends D.G. Higman's homogeneous coherent configuration (see [5]). Suppose C is a set (of colors) and ι is an involution of C. A *color scheme* is a system $\mathcal{V} = \langle V, C_a\rangle_{a\in C}$ where

(i) $\{C_a : a \in C\}$ is a partition of $V^2 \sim Id = \{(x,y) \in V^2 : x \neq y\}$,

---

* Research supported by NSF grant MCS-8003896 and by the Citadel Development Foundation.

(ii) $C_a^{\smile} = C_{\iota(a)}$ for all $a \varepsilon C$,

(iii) for each color and vertex the color is present on some edge from the vertex,

(iv) for $a,b,c \varepsilon C$ if $(x,y) \varepsilon C_c$ the existence of an (a,b)-path from x to y is independent of the choice of x and y, in symbols,

$$C_c \cap (C_a | C_b) \neq \emptyset \quad \Rightarrow \quad C_c \subseteq C_a | C_b .$$

Given a color scheme $\mathscr{V}$, choose a new symbol $I \notin C$. (Think of I as the identity relation.) The *algebra* (*color algebra*, or *configuration algebra*) of $\mathscr{V}$ is the system

$$\mathfrak{M}_{\mathscr{V}} = \langle C \cup \{I\}, \cdot, I, {}^{-1} \rangle$$

where $a^{-1} = \iota(a)$ for $a \varepsilon C$, $I^{-1} = I$, $x \cdot I = x = I \cdot x$ for all $x \varepsilon C \cup \{I\}$, and for a,b, and c in C,

$$a \cdot b = \{c \varepsilon C : C_c \subseteq C_a | C_b \} \cup \{I : b = a^{-1}\}.$$

A polygroup is *chromatic* if it is isomorphic to the algebra of some color scheme.

A natural example of a chromatic polygroup is the system $G/\!/H$ of all double cosets of a group modulo a subgroup H. Namely,

$$G/\!/H = \langle \{HgH : g \varepsilon G\}, \cdot, H, {}^{-1} \rangle$$

where $(HgH) \cdot (Hg'H) = \{Hghg'H : h \varepsilon H\}$ and $(HgH)^{-1} = Hg^{-1}H$. That these systems are chromatic was established in [2]. The double coset construction generalizes to the idea of a double quotient. This idea will not be needed in this paper for a general polygroup but only for ordinary groups. The general notion (see [2]) is equivalent to the following when restricted to groups. An equivalence relation θ on a group G is called a *conjugation* on G if

(i) $(\theta x)^{-1} = \theta x^{-1}$ for all x, and

(ii) $\theta(xy) \subseteq (\theta x)(\theta y)$ for all $x,y \varepsilon G$.

The natural quotient system $G/\!/\theta$ is a chromatic polygroup ([2]) and we define

$$Q^2(\text{Group}) = \{ G/\!/\theta : \theta \text{ is a conjugation on some group } G\}.$$

A conjugation θ is called *special* if it satisfies

(iii) $x \theta e \quad \Rightarrow \quad x = e.$

The class of all polygroups isomorphic to double quotients of groups via special conjugations is denoted by $Q_s^2(\text{Group})$.

2. AN EXTENSION CONSTRUCTION. Suppose $\mathfrak{A}$ and $\mathfrak{B}$ are polygroups whose elements have been renamed so that $A \cap B = \{e\}$ where e is the (common) identity of both $\mathfrak{A}$ and $\mathfrak{B}$. We use M^- to denote $\{ x \varepsilon M : x \neq e \}$, the non-identity elements of a polygroup $\mathfrak{M}$. A new system $\mathfrak{A}[\mathfrak{B}] = \langle M, *, e, {}^I \rangle$, called the *extension of* $\mathfrak{A}$ *by* $\mathfrak{B}$, is formed in the

following way. Set $M = A^- \cup B^- \cup \{e\}$ and let $e^I = e$, $x^I = x^{-1}$ (in the appropiate system), $e*x = x*e = x$ for all $x \in M$, and for all $x,y \in M^-$,

$$x*y = \begin{cases} x\cdot y & \text{if } x,y \in A \\ x & \text{if } x \in B,\ y \in A \\ y & \text{if } x \in A,\ y \in B \\ x\cdot y & \text{if } x,y \in B,\ y \neq x^{-1} \\ x\cdot y \cup A & \text{if } x,y \in B \text{ and } y = x^{-1}. \end{cases}$$

In the last clause, e occurs in both $x\cdot y$ and A. If $A = \{e,a_1,a_2,\ldots\}$ and $B = \{e,b_1,b_2,\ldots\}$, the table for $*$ in $\mathfrak{A}[\mathfrak{B}]$ has the form

	e	a_1	a_2	$\cdots$	b_1	b_2	$\cdots$
e	e	a_1	a_2	$\cdots$	b_1	b_2	$\cdots$
a_1	a_1	a_1a_1	a_1a_2	$\cdots$	b_1	b_2	$\cdots$
a_2	a_2	a_2a_1	a_2a_2	$\cdots$	b_1	b_2	$\cdots$
.	.	.	.	...	.	.	...
.	.	.	.	...	.	.	...
.	.	.	.	...	.	.	...
b_1	b_1	b_1	b_1	$\cdots$	b_1*b_1	b_1*b_2	$\cdots$
b_2	b_2	b_2	b_2	$\cdots$	b_2*b_1	b_2*b_2	$\cdots$
.	.	.	.	...	.	.	...
.	.	.	.	...	.	.	...
.	.	.	.	...	.	.	...

Several special cases of the algebra $\mathfrak{A}[\mathfrak{B}]$ are useful. Before describing them we need to assign names to the two 2-element polygroups. Let $\mathfrak{2}$ denote the group Z_2 and let $\mathfrak{3}$ denote the polygroup $S_3 /\!/ \langle (12) \rangle \cong Z_3 /\!/ \theta$ where θ is the special conjugation with blocks $\{0\}\{1,2\}$. The multiplication table for $\mathfrak{3}$ is

	0	1
0	0	1
1	1	0,1

The names $\mathfrak{2}$ and $\mathfrak{3}$ are suggested by the color schemes that represent the algebras (see Section 3).

EXAMPLE 1. Adjoining a new identity element.

The system $\mathfrak{3}[\mathfrak{M}]$ is the result of adding a "new" identity element to the polygroup $\mathfrak{M}$. The system $\mathfrak{2}[\mathfrak{M}]$ is almost as good. For example, suppose $\mathfrak{N}$ is the system with table

	0	1	2
0	0	1	2
1	1	02	12
2	2	12	01

Then

	0	a	1	2
0	0	a	1	2
a	a	0a	1	2
1	1	1	0a2	12
2	2	2	12	0a1

$3[\mathfrak{R}]$

	0	a	1	2
0	0	a	1	2
a	a	0	1	2
1	1	1	0a2	12
2	2	2	12	0a1

$2[\mathfrak{R}]$

The element "a" acts like the "old" identity on $\mathfrak{R}$.

EXAMPLE 2. Adding a "last" element.

In section 20 of [1] two non-isomorphic one-element extensions of a polygroup $\mathfrak{M}$ were introduced. In the present terminology these algebras are just $\mathfrak{M}[2]$ and $\mathfrak{M}[3]$. For example, the tables for $\mathfrak{R}[2]$ and $\mathfrak{R}[3]$ are given below.

	0	1	2	a
0	0	1	2	a
1	1	02	12	a
2	2	12	01	a
a	a	a	a	012

$\mathfrak{R}[2]$

	0	1	2	a
0	0	1	2	a
1	1	02	12	a
2	2	12	01	a
a	a	a	a	012a

$\mathfrak{R}[3]$

EXAMPLE 3. As an example of $\mathfrak{A}[\mathfrak{B}]$ where neither $\mathfrak{A}$ nor $\mathfrak{B}$ are minimal systems we consider $\mathfrak{R}[\mathfrak{R}]$ whose table is given below.

	0	1	2	a	b
0	0	1	2	a	b
1	1	02	12	a	b
2	2	12	01	a	b
a	a	a	a	012b	ab
b	b	b	b	ab	012a

We finish this section by showing that the extension construction will always yield a polygroup.

THEOREM 1. $\mathfrak{A}[\mathfrak{B}]$ *is a polygroup.*

Proof. Since (P_2) is clear it is enough to check (P_1) and (P_3).

(P_1) : $(x*y)*z = x*(y*z)$.

Without loss of generality we may assume $x,y,z \neq e$ and not all elements belong to A. Note that

(1) if $u \in B$ and $v \in A$, then $u*v = v*u = u$.

If exactly one of x,y,z belong to B, then (1) implies that both sides of (P_1) equal the element in $\{x,y,z\} \cap B$. If exactly two of x,y,z belong to B, say u and v, then (1) implies that both sides of (P_1) equal $u*v$. We assume $x,y,z \in B^-$ and show

(2) $u \in (x*y)*z$ implies $u \in x*(y*z)$.

If $u \notin A$, then $u \in w*z$ for some $w \in x*y$. Now, if $w \notin A$, $w \in x \cdot y$ and $u \in w \cdot z$ so

$$u \in (xy)z = x(yz) \quad (\text{in } B) \quad \subseteq x*(y*z).$$

Also, if $w \in A$, $u \in w*z = z$ (so $u = z$) and $e \in xy$. Thus,

$$u = z \in (xy)z = x(yz) \subseteq x*(y*z).$$

Now, suppose $u \in A$. Then $z^{-1} \in x*y$. $z^{-1} \notin A$ so $z^{-1} \in xy$ (in B), so $e \in (xy)z = x(yz)$. Thus,

$$x^{-1} \in y \cdot z \subseteq y*z \text{ and hence } u \in A \subseteq x*(y*z).$$

The proof of the opposite inclusion $x*(y*z) \subseteq (x*y)*z$ is similar to (2).

(P_3) : $x \in y*z$ implies $y \in x*z^I$ and $z \in y^I*x$.

The condition is clear if $x,y,z \in A$. Since $x \in B^-$ implies y or z belongs to B^- and $x \in A$ implies $z \in B^-$, we may assume at least two of x,y,z belong to B^-. On the other hand, if $x,y,z \in B^-$, then $x \in y*z$ implies $x \in y \cdot z$ (in B) from which (P_3) follows. Therefore we may assume exactly two of x,y,z belong to B^-. This reduces to two cases.

(3) $x \varepsilon y{*}z$ where $x, y \varepsilon B^-$ and $z \varepsilon A$.

By (1), $y{*}z = y$ so $x = y$; thus $y = x = x{*}z^{-1}$ using (1) again and $z \varepsilon A \subseteq x^{-1}{*}x$ $= y^{-1}{*}x$.

(4) $x \varepsilon y{*}z$ where $x \varepsilon A$ and $y, z \varepsilon B^-$.

In this case $y = z^{-1}$ so the desired conclusion follows using (1). This completes the proof of (P_3) and hence the theorem.

Where there is no confusion possible we write $* = \cdot$ and ${}^I = {}^{-1}$.

3. PROPERTIES OF $\mathfrak{A}[\mathfrak{B}]$. The first result shows that the extension of $\mathfrak{A}$ by $\mathfrak{B}$ preserves being chromatic.

THEOREM 2. *If* $\mathfrak{A} \cong \mathfrak{M}_{\mathscr{V}}$ *and* $\mathfrak{B} \cong \mathfrak{M}_{\mathscr{W}}$, *then* $\mathfrak{A}[\mathfrak{B}]$ *is also chromatic.*

Proof. Suppose $\mathscr{V} = \langle V, C_a \rangle_{a \varepsilon A^-}$. First introduce a family of pairwise disjoint color schemes $\{ \mathscr{V}_w : w \varepsilon W \}$ where each $\mathscr{V}_w$ is isomorphic to $\mathscr{V}$. Assume the vertex set of $\mathscr{V}_w$ is V_w and the isomorphism of $\mathscr{V}$ onto $\mathscr{V}_w$ sends x to x_w. We construct a scheme $\mathscr{V}[\mathscr{W}]$ in the following way. Replace each vertex w of the scheme $\mathscr{W}$ by the copy of $\mathscr{V}$ with vertex set V_w. Thus the set of all vertices of $\mathscr{V}[\mathscr{W}]$ is just the union of all V_w's. An edge coloring using the elements of $A^- \cup B^-$ as colors is introduced in the following way. For $a \varepsilon A^-$ and $b \varepsilon B^-$ let

$$(x_u, y_v) \varepsilon C_a \quad \text{iff} \quad u = v \quad \text{and} \quad (x,y) \varepsilon C_a \quad (\text{in } \mathscr{V}_u),$$

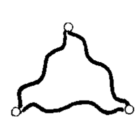
$$(x_u, x_v) \varepsilon C_b \quad \text{iff} \quad (u,v) \varepsilon C_b \quad (\text{in } \mathscr{W}).$$

It is easily seen that $\mathscr{V}[\mathscr{W}]$ is a scheme that represents $\mathfrak{A}[\mathfrak{B}]$.

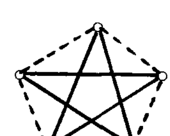
The converse of Theorem 2 will be established later (Theorem 6).

The construction given in the proof above can be carried out in practice. The idea is to take a color scheme representing $\mathfrak{B}$ and "blow-it-up" by replacing each vertex by the configuration that represents $\mathfrak{A}$. As an illustration we use this method to produce representations for the systems $2[\mathfrak{N}]$, $3[\mathfrak{N}]$, $\mathfrak{N}[2]$, $\mathfrak{N}[3]$, and $\mathfrak{N}[\mathfrak{N}]$ given in Examples 1,2,3. The systems 2, 3, and $\mathfrak{N}$ have representations given as follows.

2

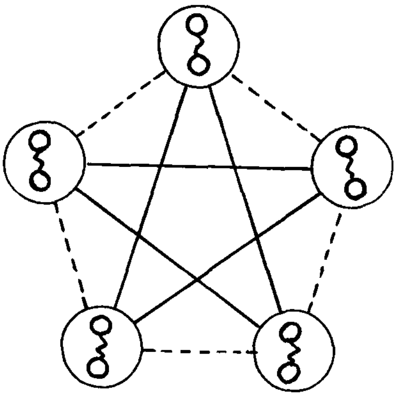


3

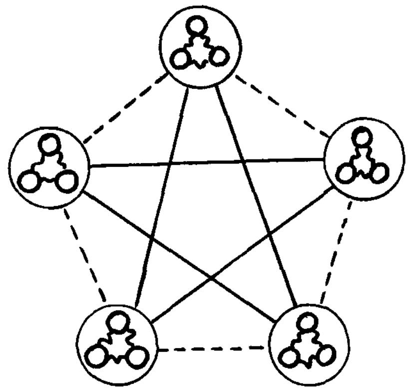


$\mathfrak{N}$

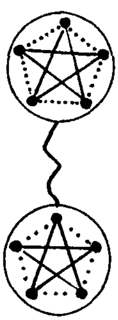
The method of Theorem 2 yields:



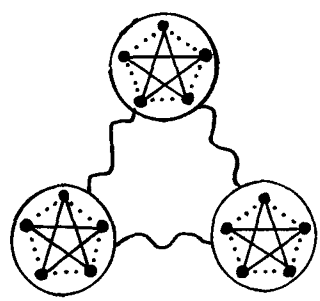
$2[\mathfrak{R}]$



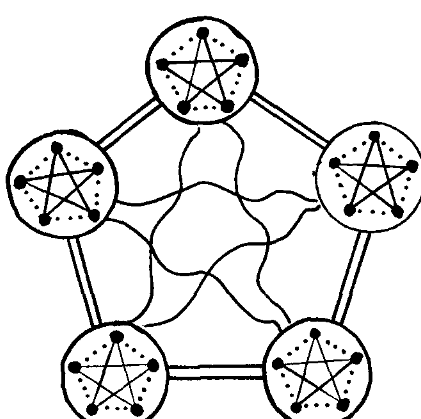
$3[\mathfrak{R}]$



$\mathfrak{R}[2]$



$\mathfrak{R}[3]$



$\mathfrak{R}[\mathfrak{R}]$

The next three results show that various important special classes of chromatic polygroups are closed under the extension operation $\mathfrak{A}[\mathfrak{B}]$. Several types of proofs are offered. The approach via automorphism groups, illustrated by the proof of Theorem 3, could be used to establish all three theorems. A more concrete approach is used to prove Theorems 4 and 5. When using a special representation of a polygroup it is often convenient to explicitly give the groups and/or conjugations involved.

THEOREM 3. *If* $\mathfrak{A}, \mathfrak{B} \in Q^2(\text{Group})$, *then* $\mathfrak{A}[\mathfrak{B}] \in Q^2(\text{Group})$.

Proof. Recall (Theorem 4.1 of [2]) that for a polygroup $\mathfrak{M}$,

(*) $\mathfrak{M} \in Q^2(\text{Group})$ iff $\mathfrak{M} \cong \mathfrak{M}_{\mathscr{V}}$ where $\text{Aut}(\mathscr{V})$ is transitive on vertices.

Suppose $\mathfrak{A} \cong \mathfrak{M}_{\mathscr{V}}$, $\mathfrak{B} \cong \mathfrak{M}_{\mathscr{W}}$, and $\mathscr{V}[\mathscr{W}]$ is the color scheme constructed from $\mathscr{V}$ and $\mathscr{W}$ in the proof of Theorem 2. Automorphisms τ on $\mathscr{V}$ and σ on $\mathscr{W}$ induce automorphisms on $\mathscr{V}[\mathscr{W}]$ in the following way.

(i) For $\sigma \in \text{Aut}(\mathscr{W})$ define $\hat{\sigma}$ on $\mathscr{V}[\mathscr{W}]$ by $\hat{\sigma}(x_w) = x_{\sigma(w)}$ for all $w \in W$.

(ii) For $\tau \in \text{Aut}(\mathscr{V})$ and $w \in W$, define $\bar{\tau}_w$ on $\mathscr{V}[\mathscr{W}]$ so that $\bar{\tau}_w$ acts like τ on $\mathscr{V}_w$ and is the identity otherwise.

It is easily seen that the maps $\hat{\sigma}$ and $\bar{\tau}_w$ described in (i) and (ii) are automorphisms of $\mathscr{V}[\mathscr{W}]$. From (*) we may assume $\text{Aut}(\mathscr{V})$ and $\text{Aut}(\mathscr{W})$ are transitive. Using maps of type (i) and (ii) it easily follows that $\text{Aut}(\mathscr{V}[\mathscr{W}])$ is transitive on vertices so (*) yields the desired conclusion.

THEOREM 4. *If* $\mathfrak{A}, \mathfrak{B} \in Q^2_s(\text{Group})$, *then* $\mathfrak{A}[\mathfrak{B}] \in Q^2_s(\text{Group})$.

Proof. Suppose $\mathfrak{A} = G_1/\!\!/\theta_1$ and $\mathfrak{B} = G_2/\!\!/\theta_2$ where θ_1 and θ_2 are special conjugations on G_1 and G_2 respectively. Let $G = G_1 \times G_2$ and define θ on G by

$$(g_1,g_2)\theta(g_1',g_2') \text{ iff } (g_2=g_2'=e \text{ and } g_1\theta_1 g_1') \text{ or } (g_2,g_2' \neq e \text{ and } g_2\theta_2 g_2').$$

Note that the θ-classes are

$$\theta(g,e) = \{ (h,e) : h\theta_1 g \}$$

and, for $h \neq e$,

$$\theta(e,h) = \{ (g,h') : h'\theta_2 h \}.$$

To show θ is a special conjugation, conditions (i),(ii), and (iii) need to be checked. First, (iii) holds because θ_1 special implies $\theta(e,e) = \{(e,e)\}$. Also (i), $\theta(g,h)^{-1} = (\theta(g,h))^{-1}$, holds since θ_1 and θ_2 have similar properties. It remains to check

(ii) $\theta((g_1,h_1)(g_2,h_2)) \subseteq (\theta(g_1,h_1))(\theta(g_2,h_2))$.

Suppose $(g,h) \in \theta(g_1g_2,h_1h_2) = \theta((g_1,h_1)(g_2,h_2))$. The definition of θ gives two cases:

Case 1. $h = h_1h_2 = e$ and $g\theta_1(g_1g_2)$.

Since θ_1 is a conjugation, $g = g_1'g_2'$ for some $g_1'\theta_1 g_1$ and $g_2'\theta_1 g_2$. Then $(g,e) = (g_1',h_1)(g_2',h_2)$ so it suffices to show that $(g_i',h_i)\theta(g_i,h_i)$ for $i=1,2$. The conclusion follows from $g_i'\theta_1 g_i$ when $h_1 = h_2 = e$ while it follows from $h_i\theta_2 h_i$ if

h_1 , $h_2 \neq e$.

<u>Case</u> 2. h, $h_1h_2 \neq e$ and $h\theta_2 h_1h_2$.

Since θ_2 is a conjugation, $h = h_1'h_2'$ for some $h_1'\theta_2 h_1$ and $h_2'\theta_2 h_2$. This yields $(g,h_1')\theta(g_1,h_1)$ and $(e,h_2')\theta(g_2,h_2)$ whenever $h_1',h_2' \neq e$; so

$$(g,h) = (g,h_1')(e,h_2') \in (\theta(g_1,h_1))(\theta(g_2,h_2)).$$

On the other hand, suppose one of h_1', h_2' is e, say $h_1' = e$ and $h_2' = h \neq e$. Then $(g_1,e)\theta(g_1,h_1)$ and $(g_1^{-1}g,h)\theta(g_2,h)$ since $h \neq e$ from which it follows that (g,h) belongs to $(\theta(g_1,h_1))(\theta(g_2,h_2))$.

Thus, θ is a special conjugation on the group $G_1 \times G_2$. A bijection F between the elements of $\mathfrak{A}[\mathfrak{B}]$ and $G_1 \times G_2 /\!/ \theta$ is defined in the following way. Let F(e) = $\theta(e,e)$ and, for $a = \theta_1 g_1 \neq e$ in A^- let

$$F(a) = \theta(g_1,e),$$

and, for $b = \theta_2 g_2 \neq e$ in B^-, let

$$F(b) = \theta(e,g_2).$$

From the description of the θ-classes above it is clear that F maps $\mathfrak{A}[\mathfrak{B}]$ one-one onto $G_1 \times G_2 /\!/ \theta$. By properties (i) and (ii) of θ the inverses and identity elements correspond. Computations, as in the proof of (ii), show that F preserves products in case at least one factor belongs to $\mathfrak{A}$. When both factors belong to $\mathfrak{B}$ there are two cases. First, if $\theta_2 g_2$, $\theta_2 g_2' \in B^-$ and $\theta_2 g_2 \neq (\theta_2 g_2')^{-1}$, then

$$\begin{aligned} F(\theta_2 g_2, \theta_2 g_2') &= F(\{\theta_2 g : e \neq g \in (\theta_2 g_2)(\theta_2 g_2')\}) \\ &= \{\theta(e,g) : g \in (\theta_2 g_2)(\theta_2 g_2')\} \\ &= \{(h,g) : g \in (\theta_2 g_2)(\theta_2 g_2')\} \\ &= (\theta(e,g_2))(\theta(e,g_2')) \\ &= F(\theta_2 g_2)F(\theta_2 g_2') \end{aligned}$$

Finally, suppose $\theta_2 g_2, \theta_2 g_2' \in B^-$ and $\theta_2 g_2' = (\theta_2 g_2)^{-1}$. Then $e \in (\theta_2 g_2)(\theta_2 g_2')$ so

$$\begin{aligned} F((\theta_2 g_2)(\theta_2 g_2')) &= F(\{\theta_2 g : g \in (\theta_2 g_2)(\theta_2 g_2')\} \cup A \\ &= \{\theta(e,g) : g \in (\theta_2 g_2)(\theta_2 g_2')\} \cup (G_1 \times \{e\}) \\ &= \{(h,g) : g \in (\theta_2 g_2)(\theta_2 g_2')\} \quad \text{since } e \in (\theta_2 g_2)(\theta_2 g_2') \\ &= (\theta(e,g_2))(\theta(e,g_2')) \\ &= F(\theta_2 g_2)\, F(\theta_2 g_2'). \end{aligned}$$

The theorem follows from the fact F is an isomorphism.

The next result shows the class of double coset algebras is closed under the extension construction. For information on semi-direct products see M.Hall [4]. The group $\hat{G}$ defined below is also known as the wreath product of G_1 and G_2, see e.g., H. Neumann [7], p.45ff.

THEOREM 5. *If* $\mathfrak{A} \cong G_1 /\!\!/ H_1$ *and* $\mathfrak{B} \cong G_2 /\!\!/ H_2$, *then there exist groups* $\hat{G}$ *and* $\hat{H}$ *with* $\hat{G} \supseteq \hat{H}$ *such that* $\mathfrak{A}[\mathfrak{B}] \cong \hat{G} /\!\!/ \hat{H}$.

<u>Proof</u>. Let $X = G_2/H_2 = \{H_2 g : g \in G_2\}$ and let $\hat{G} = G_1^X \circledS_\varphi G_2$, the semi-direct product of G_1^X by G_2, where φ, mapping G_2 into $\mathrm{Aut}(G_1^X)$, is the homomorphism given by $\varphi_g(f) = g^* f$ for all $f \in G_1^X$.

$$\begin{tikzcd} X \arrow[dr, "f"'] & & X \arrow[ll, "g^*"'] \arrow[dl, "\varphi_g(f)"] \\ & G_1 & \end{tikzcd}$$

I.e., $g \in G_2$ induces $g^*: X \longrightarrow X$ by right multiplication, so $\varphi_g(f)(x) = f(xg)$ for $g \in G_2$, $f \in G_1^X$ and $x \in X$. Also, let $\hat{H} = (H_1 \times G_1^{X-\{H_2\}}) \circledS_\varphi H_2$ where

$$\varphi : H_2 \longrightarrow \mathrm{Aut}(\, H_1 \times G_1^{X-\{H_2\}})$$

is defined, as above, by $\varphi_g(f) = g^* f$.

Note that $\hat{H} = \bar{H} \circledS_\varphi H_2$ where $\bar{H} = \{f \in G_1^X : f(H_2) \in H_1\}$. Clearly $\hat{H}$ is a subgroup of $\hat{G}$, so it remains to show that $\mathfrak{A}[\mathfrak{B}] \cong \hat{G} /\!\!/ \hat{H}$.

First we identify $\mathfrak{A}$ with part of $\hat{G} /\!\!/ \hat{H}$. For $g \in G_1$ let $\hat{g} = (f, 1)$ where 1 is the identity element of G_2 and $f \in G_1^X$ is defined by

$$f(H_2 x) = \begin{cases} g & \text{if } H_2 x = H_2 \\ e & \text{if } H_2 x \neq H_2 \end{cases}$$

Then,
$$\begin{aligned} \hat{H}\hat{g}\hat{H} &= (\bar{H} \circledS H_2)(f,1)(\,\bar{H} \circledS H_2) \\ &= (\bar{H} f \circledS H_2)(\bar{H} \circledS H_2) \\ &= (\bar{H} f \bar{H}) \circledS H_2 \end{aligned}$$
where the second equality holds because, for $h \in H_2$, φ_h fixes the "H_2-coordinate" of f. Thus,

(1) $\quad (G_1^X \circledS H_2) /\!\!/ \hat{H} \cong G_1 /\!\!/ H_1$.

Now we consider the elements in $G_2 /\!\!/ H_2$ ($\cong \mathfrak{B}$). For $g \in G_2$ let $\bar{g} = (E, g)$ where E is the identity element of G_1^X. Then

$$\hat{H}\bar{g} = (\,\bar{H} \circledS H_2)\bar{g} = \bar{H} \circledS H_2 g$$

and, for $g \notin H_2$,

$$\hat{H}\bar{g}\hat{H} = (\bar{H} \circledS H_2 g)(\bar{H} \circledS H_2) = G_1^X \circledS (H_2 g H_2)$$

since, for $f_1, f_2 \in \bar{H}$, $(f_1 \cdot f_2^{hg})(x) = f_1(x) f_2(xhg)$ will produce any element of G_1^X. (To see this observe that $g \notin H_2$ means g^* is a permutation of X that moves H_2; so, for all $x \in X$, either $f_1(x)$ or $f_2(xhg)$ can be any element of G_1.) Thus,

(2) $\quad \hat{G} = \bigcup \{G_1^X \circledS b \ : \ b \in G_2 /\!\!/ H_2\}$.

A one-one correspondence between the non-identity elements of $(G_1/\!/H_1)[G_2/\!/H_2]$ and $\hat{G}/\!/\hat{H}$ is introduced as follows: to $a \in (G_1/\!/H_1)^-$ assign the element $\bar{a} \circledS H_2$ where $\bar{a} = \{ f \in G_1^X : f(H_2) \in a \}$ and to $b \in (G_2/\!/H_2)^-$ correlate $G_1^X \circledS b$. In view of (1), to show this correspondence is an isomorphism it is enough to check:

(3) $(\hat{H}\hat{g}_1\hat{H})(\hat{H}\bar{g}_2\hat{H}) = \hat{H}\bar{g}_2\hat{H}$ for $g_1 \in G_1$, $g_2 \in G_2 - H_2$,

(4) $(\hat{H}\bar{g}_2\hat{H})(\hat{H}\hat{g}_1\hat{H}) = \hat{H}\bar{g}_2\hat{H}$ for $g_1 \in G_1$, $g_2 \in G_2 - H_2$, and

(5) $(\hat{H}\bar{g}_1\hat{H})(\hat{H}\bar{g}_2\hat{H}) = G_1^X \circledS (H_2 g_1 H_2 g_2 H_2)$ for $g_1, g_2 \in G_2 - H_2$.

To establish (3), let $\hat{g}_1 = (g_1', 1)$. Then

$$\begin{aligned}(\hat{H}\hat{g}_1\hat{H})\cdot(\hat{H}\bar{g}_2\hat{H}) &= ((\bar{H}g_1'\bar{H}) \circledS H_2)(G_1^X \circledS H_2 g_2 H_2)\\ &= G_1^X \circledS H_2 g_2 H_2\\ &= \hat{H}\bar{g}_2\hat{H}\end{aligned}$$

since, for $h \in H_2$, φ_h fixes the "H_2-coordinate" and permutes all others.

The verification of (4) is easier:

$$(\hat{H}\bar{g}_2\hat{H})(\hat{H}\hat{g}_1\hat{H}) = (G_1^X \circledS H_2 g_2 H_2)((\bar{H}g_1'\bar{H}) \circledS H_2) = G_1^X \circledS H_2 g_2 H_2.$$

Finally we check (5):

$$(\hat{H}\bar{g}_1\hat{H})(\hat{H}\bar{g}_2\hat{H}) = (G_1^X \circledS H_2 g_1 H_2)(G_1^X \circledS H_2 g_2 H_2) = G_1^X \circledS (H_2 g_1 H_2)(H_2 g_2 H_2).$$

It now follows that $G/\!/H \cong \mathfrak{A}[\mathfrak{B}]$ as desired.

We now consider the converses of the properties established in Theorems 2,3,4, and 5. The basic idea for establishing the converses is illustrated by the proof of the following result.

THEOREM 6. *If $\mathfrak{A}[\mathfrak{B}]$ is chromatic, then both $\mathfrak{A}$ and $\mathfrak{B}$ are chromatic.*

Proof. Suppose $\mathfrak{A}[\mathfrak{B}] \cong \mathfrak{M}_{\mathscr{W}}$ for some color scheme $\mathscr{W} = \langle W, C_x \rangle_{x \in C}$. Recall that $C = A^- \cup B^-$. Define a relation $\approx$ on W by

$$w \approx w' \text{ iff } w = w' \text{ or } (w,w') \in C_a \text{ for some } a \in A^-.$$

It is easily seen that $\approx$ is an equivalence relation on W and each $\approx$-block, say $[p] = \{w : w \approx p\}$ for a fixed $p \in W$, inherits the structure of a color scheme from $\mathscr{W}$. The color algebra of this scheme is exactly $\mathfrak{A}$; so $\mathfrak{A}$ is chromatic.

In order to treat $\mathfrak{B}$ we form a new scheme $\mathscr{W}/\!\approx$ on the set $\{ [w] : w \in W \}$ using the elements of B^- as colors. For distinct vertices $[v]$ and $[w]$ set

$$([v],[w]) \in C_b \quad \text{iff} \quad (v,w) \in C_b \quad (\text{in } \mathscr{W}).$$

Since $a_1 b a_2 = b$ holds in $\mathfrak{A}[\mathfrak{B}]$ for $a_1, a_2 \in A$ and $b \in B$, it follows that the assignment of a color to the edge $([v],[w])$ is independent of the $\approx$-representation. It is not hard to check that $\mathscr{W}/\!\approx$ is a color scheme and $\mathfrak{M}_{\mathscr{W}/\approx} \cong \mathfrak{B}$ as desired.

Using the idea above an analysis of the proofs of Theorems 3,4, and 5 give a hint of how to construct their converses. We leave the details to the reader.

THEOREM 7. *If* $\mathfrak{A}[\mathfrak{B}]$ *is a double coset algebra (in* Q^2(Group), Q_s^2(Group) *), then both* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are double coset algebras (in* Q^2(Group), Q_s^2(Group) *respectively).*

4. AN APPLICATION. We conclude with an easy application of the extension construction to the study of relation algebras. There are many non-chromatic polygroups with 4 elements - at least 28 and at most 34. As one example we cite the algebra $\mathfrak{N}_0$ with multiplication table:

	0	1	2	3
0	0	1	2	3
1	1	1	0123	13
2	2	0123	2	23
3	3	13	23	012

In view of the connection between polygroups and integral relation algebras (see [2]) the fact that $\mathfrak{N}_0$ is non-chromatic is just the result of McKenzie [6] that the corresponding relation algebra is non-representable. $\mathfrak{N}_0$ can also be shown to be non-chromatic by a direct argument.

In Section 2 four extensions, $\mathfrak{M}[2]$, $\mathfrak{M}[3]$, $2[\mathfrak{M}]$, and $3[\mathfrak{M}]$ were given that add a new element to a polygroup $\mathfrak{M}$. By Theorems 2 and 6, $\mathfrak{M}$ is chromatic if and only if each extension is chromatic. Starting with $\mathfrak{N}_0$, McKenzie's example above, we can obtain a sequence (in fact many sequences) of non-chromatic polygroups. For example,

$$\mathfrak{N}_1=\mathfrak{N}_0[2],\ \mathfrak{N}_2=\mathfrak{N}_1[2],\ \ldots$$

Again using the connection [2] between polygroups and relation algebras we obtain:

PROPOSITION 8. *For all* $n \geqq 4$ *there exist a non-representable integral relation algebra with* n *atoms.*

REFERENCES

1. Comer, S.D., Multivalued loops and their connection with algebraic logic. Unpublished manuscript, 1969, 173pp.

2. Comer, S.D., Combinatorial Aspects of Relations. Algebra Universalis, in press.

3. Comer, S.D., A Remark on Chromatic Polygroups. Preprint, February 1982.

4. Hall, M., The Theory of Groups, MacMillan, 1959.

5. Higman, D.G., Coherent Configurations. Part I. Ordinary Representation Theory. Geometriae Dedicata 4(1975), 1-32.

6. McKenzie, R., Representations of Integral Relation Algebras. Michigan Math. J., 17(1970), 279-287.

7. Neumann, H., Varieties of Groups, Springer-Verlag, 1967.

The Citadel

Charleston, South Carolina 29409

U.S.A.

A CHARACTERIZATION FOR CONGRUENCE SEMI-DISTRIBUTIVITY

Gábor Czédli *

1. INTRODUCTION. A variety of algebras is said to be congruence-meet-semi-distributive if in the congruence lattices of its algebras the <u>semi-distributive law</u>,

$$(SD_\wedge) \qquad (\forall\alpha)\,(\forall\beta)\,(\forall\gamma)\,(\alpha\wedge\beta = \alpha\wedge\gamma \Rightarrow \alpha\wedge\beta = \alpha\wedge(\beta\vee\gamma)),$$

holds. From the general description of properties that can be characterized by Mal'cev conditions (Taylor [10], Neumann [7]) it follows that there exists a weak Mal'cev condition characterizing congruence meet semi-distributivity of varieties (Jónsson [4, Theorem 2.16]). However, $SD_\wedge$ has seemed the simplest (characterizable) property of congruence lattices for which no concrete weak Mal'cev condition has been known. The aim of this note is to present such a condition and some corollaries to it. (Note that the dual law, $SD_\vee$, has been characterized in [1].)

2. A WEAK MAL'CEV CONDITION. Our Mal'cev conditions will be given by means of certain graphs. First for any lattice term $p = p(\alpha,\beta,\gamma)$ we define a set $\underset{\sim}{G}(p)$ of graphs associated with p. The edges of any $G \in \underset{\sim}{G}(p)$ will be coloured by the variables α, β, and γ, and two distinguished vertices, the so-called <u>left</u> and <u>right</u> <u>endpoints</u>, will have special roles. In figures these endpoints will be always placed on the left-hand side and on the right-hand side, respectively. For all $k \geq 2$ $G_k(p)$ will be a distinguished member of $\underset{\sim}{G}(p)$, but $\underset{\sim}{G}(p)$ will be different from $\{G_k(p) : k \geq 2\}$ in general. Before defining $\underset{\sim}{G}(p)$ we introduce two kinds of operations for graphs. We obtain the parallel connection of graphs G_1 and G_2 by taking disjoint copies of G_1 and G_2 and identifying their left (right, resp.) endpoints (Figure 1). By taking disjoint graphs $H_1, H_2, \ldots, H_\ell$ $(\ell \geq 1)$ such that $H_j \cong G_i$ for $i \equiv j \mod (2)$ and

*This work was supported by NSERC, Canada, Operating Grant A8190.

identifying the right endpoint of H_i and left endpoint of H_{i+1} for $i = 1, 2, \ldots, \ell - 1$ we obtain the serial connection of length ℓ of the graphs G_1 and G_2. (The left endpoint of H_1 and the right one of H_ℓ are the endpoints of the serial connection, cf. Figure 2.)

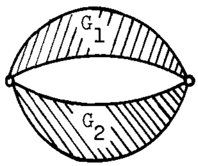


Figure 1

Figure 2

Now, if p is a variable then, for all $k \geq 2$, let $G_k(p)$ be the following graph

which consists of a single edge coloured by p, and let $\underset{\sim}{G}(p)$ be the singleton $\{G_k(p)\}$. Let $\underset{\sim}{G}(p_1 \wedge p_2)$ ($\underset{\sim}{G}(p_1 \vee p_2)$, respectively) be the set of all parallel (serial, resp.) connections of G_1 and G_2 with G_i belonging to $\underset{\sim}{G}(p_i)$. Furthermore let $G_k(p_1 \wedge p_2)$ and $G_k(p_1 \vee p_2)$ be the parallel connection and the serial connection of length k of the graphs $G_k(p_1)$ and $G_k(p_2)$, respectively.

For $m \geq 2$ the smallest equivalence relation of $\{0, 1, \ldots, m\}$ collapsing 0 and m will be denoted by $\alpha(m)$. Similarly, $\beta(m)$ ($\gamma(m)$, respectively) is the smallest equivalence of $\{0, 1, \ldots, m\}$ that collapses $(i, i+1)$ for $0 \leq i < m$, i even (odd, respectively). If $\pi \in \{\alpha, \beta, \gamma\}$ and $j \leq m$ then the smallest member of $\{0, 1, \ldots, m\}$ that is congruent to j modulo $\pi(m)$ will be denoted by $j\pi(m)$ or $j\pi$.

Given a lattice term $p = p(\alpha, \beta, \gamma)$, an integer $m \geq 2$ and a graph $G \in \underset{\sim}{G}(p)$ we associate the following (strong, i.e. finite) Mal'cev condition $U(m, G)$ with G and m:

"For any vertex f_i of G there exists an $(m+1)$-ary term $f_i(x_0, x_1, \ldots, x_n)$ such that for each $\pi \in \{\alpha, \beta, \gamma\}$ and any π-coloured edge connecting, say, f_i and f_j the identity $f_i(x_{0\pi}, x_{1\pi}, \ldots, x_{m\pi}) = f_j(x_{0\pi}, x_{1\pi}, \ldots, x_{m\pi})$ holds (here π abbreviates $\pi(m)$), and for the left and right endpoints f_0 and f_1 the endpoint identities $f_0(x_0, x_1, \ldots, x_m) = x_0$, $f_1(x_0, x_1, \ldots, x_m) = x_m$ are satisfied."

We shall consider the ternary lattice terms $\beta_n = \beta_n(\alpha, \beta, \gamma)$ and $\gamma_n = \gamma_n(\alpha, \beta, \gamma)$, $n = 0, 1, 2, \ldots$, defined by the following induction: $\beta_0 = \beta$, $\gamma_0 = \gamma$, $\beta_{n+1} = \beta \vee (\alpha \wedge \gamma_n)$, $\gamma_{n+1} = \gamma \vee (\alpha \wedge \beta_n)$. Denoting $U(m, G_n(\beta_n))$

by $U(m, n)$ and letting $\underset{\sim}{G}(\beta_\infty)$ be equal to the union of all $\underset{\sim}{G}(\beta_n)$, $2 \leq n < \omega$, we can formulate our main result:

THEOREM. For any variety $\underset{\sim}{V}$ of algebras the following three conditions are equivalent:

(i) $\underset{\sim}{V}$ is congruence meet semi-distributive;

(ii) For any integer $m \geq 2$ there exists an even $n \geq 2$ such that the strong Mal'cev condition $U(m, n)$ holds in $\underset{\sim}{V}$;

(iii) $U(m, G)$ holds in $\underset{\sim}{V}$ for infinitely many $m \geq 2$ and appropriate (depending on m) $G \in \underset{\sim}{G}(\beta_\infty)$.

Moreover (ii) is a weak Mal'cev condition in Jónsson's sense [4], i.e. $U(m, n)$ implies $U(m, n+2)$ for all m, n.

3. PROOF OF THE THEOREM. Since (ii) imples (iii) trivially, (i)$\Rightarrow$(ii) and (iii)$\Rightarrow$(i) have to be shown. While the latter requires almost the same argument that Wille [11] and Pixley [9] used, the implication (i)$\Rightarrow$(ii) needs a different approach.

Given congruences $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ of an algebra A, $a_0, a_1 \in A$, a ternary lattice term p, and $G \in \underset{\sim}{G}(p)$, we say that a_0, a_1 can be connected by the graph G in A if there are further elements $a_i \in A$ for $i \in \{2, 3, \dots, s\}$, where $\{0, 1, \dots, s\}$ is the vertex set of G with endpoints 0 and 1, such that $(a_i, a_j) \in \bar{\pi}$ holds for all $\pi \in \{\alpha, \beta, \gamma\}$ and π-coloured edge of G connecting i and j. The following statement follows from the general description of the join of congruences $\Theta \vee \Psi = \bigcup(\Theta \circ \Psi \circ \Theta \circ \dots$ (k factors): $k < \omega)$ and from reflexivity, thus the proof will be omitted.

Claim 1. Let $A, \bar{\alpha}, \bar{\beta}, \bar{\gamma}, a_0, a_1$, and p be as above. If $(a_0, a_1) \in \in p(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$ then there exists a natural number k_0 such that for all $k \geq k_0$ a_0 and a_1 can be connected by the graph $G_k(p)$ in A. Conversely, if a_0 and a_1 can be connected by some member of $\underset{\sim}{G}(p)$ in A then $(a_0, a_1) \in \in p(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$.

The following assertion will be also needed.

Claim 2. Given a variety $\underset{\sim}{V}$, $m \geq 2$ and an equivalence π of $\{0, 1, \dots, m\}$. Let $\bar{\pi}$ denote the congruence generated by $\{(x_i, x_j) : (i, j) \in \pi\}$ in the free algebra $F_{\underset{\sim}{V}}(x_0, x_1, \dots, x_m)$. If for m-ary $\underset{\sim}{V}$-terms f and g $(f(x_0, x_1, \dots, x_m), g(x_0, x_1, \dots, x_m)) \in \bar{\pi}$ then the identity $f(x_{0\pi}, x_{1\pi}, \dots, x_{m\pi}) = g(x_{0\pi}, x_{1\pi}, \dots, x_{m\pi})$ holds throughout $\underset{\sim}{V}$.

Proof. Extend the map $x_i \mapsto x_{i\pi}$ $(i = 0, 1, \dots, m)$ to an endomorphism φ of $F_{\underset{\sim}{V}}(x_0, x_1, \dots, x_m)$. Since $\bar{\pi} \subseteq \mathrm{Ker}\,\varphi$ we obtain $f(x_{0\pi}, x_{1\pi}, \dots, x_{m\pi}) = f(x_0\varphi, \dots, x_m\varphi) = f(x_0, \dots, x_m)\varphi = g(x_0, \dots, x_m)\varphi = g(x_0\varphi, \dots, x_m\varphi) = g(x_{0\pi}, x_{1\pi}, \dots, x_{m\pi})$, yielding the assertion.

Claim 3. Given congruences $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ of an algebra A, define $\bar{\beta}_\infty = \beta_\infty(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$ and $\bar{\gamma}_\infty = \gamma_\infty(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$ to be $\bigcup(\beta_n(\bar{\alpha}, \bar{\beta}, \bar{\gamma}) : n < \omega)$ and $\bigcup(\gamma_n(\bar{\alpha}, \bar{\beta}, \bar{\gamma}) : n < \omega)$, respectively. Then $\bar{\beta}_\infty$ and $\bar{\gamma}_\infty$ are congruences. Furthermore, denoting $\beta_n(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$ and $\gamma_n(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$ by $\bar{\beta}_n$ and $\bar{\gamma}_n$, respectively, we have $\bar{\beta}_n \subseteq \bar{\beta}_{n+1}$, $\bar{\gamma}_n \subseteq \bar{\gamma}_{n+1}$ for all n and $\bar{\alpha} \wedge \bar{\beta}_\infty = \bar{\alpha} \wedge \bar{\gamma}_\infty$. If $\bar{\alpha} \wedge \bar{\beta} = \bar{\alpha} \wedge \bar{\gamma}$ then $\bar{\beta} = \bar{\beta}_n = \bar{\beta}_\infty$ and $\bar{\gamma} = \bar{\gamma}_n = \bar{\gamma}_\infty$ for all n.

Proof. The inclusions are trivial for $n = 0$. If they hold for $n - 1$ then $\bar{\beta}_n = \bar{\beta} \vee (\bar{\alpha} \wedge \bar{\gamma}_{n-1}) \subseteq \bar{\beta} \vee (\bar{\alpha} \wedge \bar{\gamma}_n) = \bar{\beta}_{n+1}$, and $\bar{\gamma}_n \subseteq \bar{\gamma}_{n+1}$ follows similarly. Therefore $\bar{\beta}_\infty$ and $\bar{\gamma}_\infty$ are congruences. If $(x, y) \in \bar{\alpha} \wedge \bar{\beta}_\infty$ then we have $(x, y) \in \bar{\alpha} \wedge \bar{\beta}_n \subseteq \bar{\alpha} \wedge (\bar{\gamma} \vee (\bar{\alpha} \wedge \bar{\beta}_n)) = \bar{\alpha} \wedge \bar{\gamma}_{n+1} \subseteq \bar{\alpha} \wedge \bar{\gamma}_\infty$, thus $\bar{\alpha} \wedge \bar{\beta}_\infty = \bar{\alpha} \wedge \bar{\gamma}_\infty$ by symmetry. The rest is a trivial induction.

(i)$\Rightarrow$(ii): Suppose $\underset{\sim}{V}$ is a congruence $SD_\wedge$ variety, $m \geq 2$ and consider the congruences $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ of $F_{\underset{\sim}{V}}(x_0, x_1, \ldots, x_m)$ generated by $\{(x_i, x_j) : (i, j) \in \alpha(m)\}$, $\{(x_i, x_j) : (i, j) \in \beta(m)\}$ and $\{(x_i, x_j) : (i, j) \in \gamma(m)\}$, respectively. Let us adopt the abbreviations $\bar{\beta}_n, \bar{\beta}_\infty, \bar{\gamma}_n, \bar{\gamma}_\infty$ from Claim 3. Since $(x_0, x_m) \in \alpha(m) \cap (\beta(m) \circ \gamma(m) \circ \beta(m) \circ \gamma(m) \circ \ldots) \subseteq \bar{\alpha} \wedge (\bar{\beta} \circ \bar{\gamma} \circ \bar{\beta} \circ \bar{\gamma} \circ \ldots) \subseteq \bar{\alpha} \wedge (\bar{\beta} \vee \bar{\gamma}) \subseteq \bar{\alpha} \wedge (\bar{\beta}_\infty \vee \bar{\gamma}_\infty)$ (with $m - 1$ factors occurring), $SD_\wedge$ and Claim 3 yield $(x_0, x_m) \in \bar{\alpha} \wedge \bar{\beta}_\infty$. Therefore there exists an even integer $n \geq 2$ such that $(x_0, x_m) \in \beta_n(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$. Therefore, by Claim 1, there exists $k \geq n$ such that x_0 and x_m can be connected by $G_k(\beta_n)$ in $F_{\underset{\sim}{V}}(x_0, x_1, \ldots, x_m)$. We can assume that $k = n$. (We have $(0, m) \in \alpha(m)$ whence, by repeating the "end-point" elements x_0 and x_m, x_0 and x_m can be connected by $G_k(\beta_{n+2})$, $G_k(\beta_{n+4})$, etc.). Now we have elements a_i in $F_{\underset{\sim}{V}}(x_0, \ldots, x_m)$ associated with the vertices f_i of $G_n(\beta_n)$. But $a_i = f_i(x_0, x_1, \ldots, x_m)$ for some terms f_i whence, by Claim 2, it follows that $U(m, G_n(\beta_n)) = U(m, n)$ holds in $\underset{\sim}{V}$.

(iii)$\Rightarrow$(i): Now suppose $a_0, a_1 \in A \in \underset{\sim}{V}$, $\underset{\sim}{V}$ is a variety satisfying (iii), $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ are congruences of A, $\bar{\alpha} \wedge \bar{\beta} = \bar{\alpha} \wedge \bar{\gamma}$, and $(a_0, a_1) \in \bar{\alpha} \wedge (\bar{\beta} \vee \bar{\gamma})$. Then there are elements $b_0, b_1, \ldots, b_m \in A$ such that $a_0 = b_0$, $a_1 = b_m$, $(b_0, b_m) \in \bar{\alpha}$, $(b_i, b_{i+1}) \in \bar{\beta}$ for i even, and $(b_i, b_{i+1}) \in \bar{\gamma}$ for i odd. From (iii) we have a graph $G \in \underset{\sim}{G}(\beta_\infty)$, and thus $G \in G(\beta_n)$ for some n, such that $U(m, G)$ holds in $\underset{\sim}{V}$. We claim that via assigning $f_i(b_0, b_1, \ldots, b_m) \in A$ to all vertices f_i of G b_0 and b_m are connected by G in A. Really, if two vertices, f_i and f_j, are connected by a π-coloured edge in G, $\pi \in \{\alpha, \beta, \gamma\}$, then $f_i(b_0, b_1, \ldots, b_m) \bar{\pi} f_i(b_{0\pi}, b_{1\pi}, \ldots, b_{m\pi}) = f_j(b_{0\pi}, b_{1\pi}, \ldots, b_{m\pi}) \bar{\pi} f_j(b_0, b_1, \ldots, b_m)$. Hence Claims 1 and 3 yield $(a_0, a_1) = (b_0, b_m) \in \beta_m(\bar{\alpha}, \bar{\beta}, \bar{\gamma}) = \bar{\beta}$, yielding (i).

Finally suppose $U(m, n)$ holds in a variety $\underset{\sim}{V}$ via the terms $f_0, f_1, f_2, \ldots$. To satisfy $U(m, G_n(\beta_{n+2}))$ in $\underset{\sim}{V}$ we can associate the same terms $f_0, f_1, f_2, \ldots$ with the vertices of a subgraph S, $S \cong G_n(\beta_n)$, and associate the projections on x_0 and x_m with the other vertices of $G_n(\beta_{n+2})$. Having $U(m, G_n(\beta_{n+2}))$ satisfied, by repeating terms appropriately one can define terms for $U(m, G_{n+2}(\beta_{n+2})) = U(m, n + 2)$.

4. COROLLARIES. In Jónsson and Rival's paper [5] a sequence of lattice identities ε_n was produced with the property that an arbitrary lattice variety is meet semi-distributive if and only if ε_n holds in it for some $n < \omega$. (Note that the proof of Theorem 6.1 in [5] yields this result, which we cite in a slightly modified form.) Furthermore, Day [2] showed that $\underset{\sim}{K}_n$, the n-th Polin variety, is congruence meet and join semi-distributive, congruence (n+2)-permutable, and ε_{2n} holds in its congruence lattices. (For $n = 2$ Day and Freese [3, Theorem 7.1] have proved more, namely, even ε_2 holds in the congruence lattices of $\underset{\sim}{K}_2 = \underset{\sim}{P}$, the original Polin variety.) Denoting the lattice identity $\alpha\wedge(\beta\vee\gamma)\leq\beta_n$ by ε_n we can present a similar observation.

COROLLARY 1. Given a congruence m-permutable variety $\underset{\sim}{V}$, $\underset{\sim}{V}$ is congruence meet semi-distributive iff there exists $n < \omega$ such that the identity ε_n holds in the congruence lattices of $\underset{\sim}{V}$, or equivalently, iff $U(m, n)$ holds in $\underset{\sim}{V}$ for some $n < \omega$.

<u>Proof.</u> If $\underset{\sim}{V}$ is congruence $SD_\wedge$ then, by our Theorem, $U(m, n)$ holds in it for some n. But what was really shown in the proof of Theorem is that if $U(m, n)$ holds in a variety with m-permutable congruences then its congruence lattices satisfy ε_n. Conversely, if $\alpha\wedge\beta = \alpha\wedge\gamma$ for elements α, β, γ of an arbitrary lattice, then an easy induction yields $\beta_n(\alpha,\beta,\gamma) = \beta$ and $\gamma_n(\alpha,\beta,\gamma) = \gamma$ for all $n<\omega$. Thus ε_n implies $\alpha\wedge(\beta\vee\gamma)\leq\alpha\wedge\beta_n(\alpha,\beta,\gamma) = \alpha\wedge\beta$, the meet semi-distributivity, in any lattice.

It is worth mentioning that the dual statement also holds, i.e. we have the following:

<u>Observation.</u> Let $\underset{\sim}{V}$ be a congruence m-permutable variety of algebras. Then $\underset{\sim}{V}$ is congruence join semi-distributive if and only if there exists an $n < \omega$ such that ε_n^*, the dual of ε_n, holds in the congruence lattices of $\underset{\sim}{V}$.

<u>Proof.</u> By duality, ε_n^* implies join semi-distributivity (in any lattice). Consider the lattice terms $u_n = u_n(\alpha,\beta,\gamma)$ and $v_n = v_n(\alpha,\beta,\gamma)$ defined by the following induction: $u_0 = \alpha\wedge\beta$, $v_0 = \alpha\wedge\gamma$, $u_{n+1} = \alpha\wedge(\beta\vee v_n)$, $v_{n+1} = \alpha\wedge(\gamma\vee u_n)$, and let κ_n denote the identity $\alpha\wedge(\beta\vee\gamma)\leq u_n$. We obtain $u_n = \alpha\wedge\beta_n$ and $v_n = \alpha\wedge\gamma_n$, whence ε_n and κ_n (and thus ε_n^* and κ_n^* as well) are equivalent in any lattice. Now, if $\underset{\sim}{V}$ is m-permutable and congruence join semi-distributive then, by [1, Proposition 1] $U(m, m, \ldots, m)$ (defined there, m occours $n + 1$ times) holds in $\underset{\sim}{V}$ sor some $n<\omega$. Therefore, as it is implicit in [1] (cf. also Pixley [9]), κ_n^* holds in the congruence lattices of $\underset{\sim}{V}$.

Before formulating our last observation we define some (recursively defined) Mal'cev conditions occurring in (iii) more explicitly. Let $G_3(\beta_{m-1}) + G_3(\beta_{m-1}) \in$ $\in \underset{\sim}{G}(\beta_\infty)$ denote the serial connection of length two of two disjoint copies of $G_3(\beta_{m-1})$ for m odd. Then $U(m, G_3(\beta_{m-1}) + G_3(\beta_{m-1}))$ is the following condition (cf. Figure 3 where $m = 3$):

"There exist $(m+1)$-ary terms f_i, f^i, g_i, g^i for $0 \le i \le m-1$ such that, denoting $\pi(m)$ by π and $h(x_{0\pi}, x_{1\pi}, x_{2\pi}, \ldots, x_{m\pi})$ by $h(\pi)$, the following identities

$$f_i(\beta) = f_{i+1}(\beta),\ f^i(\beta) = f^{i+1}(\beta),\ g^i(\beta) = g^{i+1}(\beta),\ g_i(\beta) = g_{i+1}(\beta) \quad \text{for } 0 \le i < m-1,\ i \text{ even},$$

$$f_i(\gamma) = f_{i+1}(\gamma),\ f^i(\gamma) = f^{i+1}(\gamma),\ g^i(\gamma) = g^{i+1}(\gamma),\ g_i(\gamma) = g_{i+1}(\gamma) \quad \text{for } 0 < i < m-1,\ i \text{ odd},$$

$$f_i(\alpha) = f^i(\alpha),\ g^i(\alpha) = g_i(\alpha) \quad \text{for } 0 < i \le m-1,$$

$$f_{m-1}(\beta) = f^{m-1}(\beta),\ g^{m-1}(\beta) = g_{m-1}(\beta),\ f^0(x_0, x_1, \ldots, x_m) = g^0(x_0, x_1, \ldots, x_m),$$

$$f_0(x_0, x_1, \ldots, x_m) = x_0, \text{ and } g_0(x_0, x_1, \ldots, x_m) = x_m$$

hold".

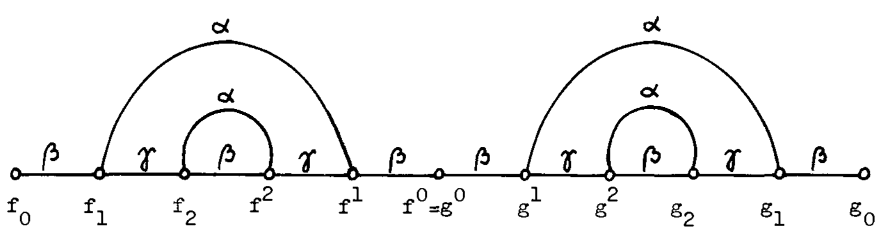


Figure 3

COROLLARY 2 (Papert [8]). The variety of semilattices is congruence meet semi-distributive.

<u>Proof.</u> For $i = 0, 1, \ldots, m-1$ consider the semilattice terms $f_i =$ $= f_i(x_0, x_1, \ldots, x_m) = x_0x_1x_2 \ldots x_i$, $f^i = f_ix_m$, $g_i = x_mx_{m-1}x_{m-2} \ldots x_{m-i}$, and $g^i = x_0g_i$. Since these terms satisfy the identities prescribed in $U(m, G_3(\beta_{m-1})$ $+ G_3(\beta_{m-1}))$ for all odd $m > 1$, our Theorem completes the proof.

Note that essentially these terms from $U(m, G_3(\beta_{m-1}) + G_3(\beta_{m-1}))$ were used by Nation [6] in proving congruence $SD_\wedge$ for semilattices.

Acknowledgement. This work was done during the author's stay at Lakehead University. The author expresses his many thanks to Professor Alan Day for valuable comments and also for providing excellent circumstances to work and to live there.

REFERENCES

[1] G. Czédli, A Mal'cev type condition for the semi-distributivity of congruence lattices, Acta Sci. Math., 43 (1981), 267-272.

[2] A. Day, Polin's non-modular congruence variety - corrigendum, manuscript.

[3] A. Day and Ralph Freese, A characterization of identities implying congruence modularity I, Cand. J. Math., 32 (1980), 1140-1167.

[4] B. Jónsson, Congruence varieties, Algebra Universalis, 10 (1980), 355-394.

[5] B. Jónsson and I. Rival, Lattice varieties covering the smallest non-modular variety, Pacific J. Math., 82 (1979), 463-478.

[6] J.B. Nation, Varieties whose congruences satisfy lattice identities, Ph. D. Thesis, Pasadena (California), 1973.

[7] W. Neumann, On Mal'cev conditions, J. Austral. Math. Soc., 17, 376-384.

[8] D. Papert, Congruence relations in semilattices, London Math. Soc., 39 (1964), 723-729.

[9] A. F. Pixley, Local Mal'cev conditions, Canad. Math. Bull., 15 (1972), 559-568.

[10] W. Taylor, Characterizing Mal'cev conditions, Algebra Universalis 3 (1973), 351-397.

[11] R. Wille, Kongruenzklassengeometrien, Springer-Verlag Lecture Notes in Math., 113, Berlin-Heidelberg-New York, 1970.

JATE, Bolyai Institute

Szeged, Aradi vértanúk tere 1.

HUNGARY 6720

GEOMETRICAL APPLICATIONS IN MODULAR LATTICES

Alan Day(*)

This paper represents the content of lectures given at the meeting on Universal Algebra and Lattice Theory at Puebla, Mexico in January, 1982. It attempts to survey recent important results in modular lattices, due mainly to Freese, Herrmann, and Huhn, that have a strong geometric content in their ideas and proofs. These results (and others) represent a beautiful amalgamation of the classical results of Birkhoff and von Neumann with the newer disciplines (also due in part to Birkhoff) of universal algebra and model theory. Because the roots of the essential ideas lie in geometry, or perhaps more importantly in the lattice interpretation of projective geometry and the coordinatization thereof, we have attempted to present here a short (in fact too short) introductory course in these basic ideas.

We wish to thank Professor Octavio Garcia and his organization committee for the opportunity to present this material, Professor Ralph Freese for his encouragement in putting these notes on paper, and Professor Bjarni Jónsson whose pioneering work and continuing example has been an important inspiration for many of us.

1. PROJECTIVE GEOMETRIES AS MODULAR LATTICES. In [18], Birkhoff proved that finite dimensional projective geometries could be characterized by their lattice of linearly closed subspaces. This characterization is the fundamental link between modular lattices and projective geometries. In this section we describe that linkage for projective planes and present some related results.

DEFINITION. A projective plane is a triple $G = (P, L, I)$ where P and L are disjoint non-empty sets and $I \subseteq P \times L$ is a relation satisfying:

(PP1) For all $p \neq q$ in P there exists a unique ℓ in L such that $pI\ell$ and $qI\ell$. We denote this "line" by $\ell(p, q)$.

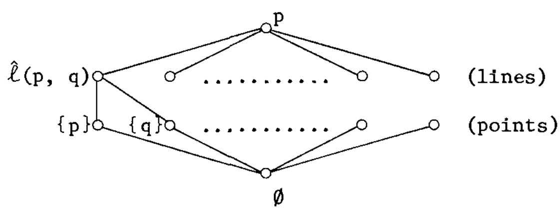
(PP2) For all $\ell \neq m$ in L there exists a p in P such that $pI\ell$ and pIm. (This "point" is also unique in light of (PP1).)

(PP3) There exists distinct p_1, p_2, p_3, p_4 in L satisfying for distinct i, j, k in $\{1, 2, 3, 4\}$, $p_i \not{I} \ell(p_j, p_k)$.

We of course call P the set of points, L the set of lines, and I the incidence relation, p is on ℓ. We could also identify each line with the set of

(*) This research is sponsored in part by an NSERC Operating Grant, A8190.

points incident with the line, namely: $\hat{\ell} = \{p \in P\colon pI\ell\}$, $\ell \in L$. By defining $C \subseteq P$ to be linearly closed if $p, q \in C$ and $p \neq q$ imply $\hat{\ell}(p, q) \subseteq C$, we define $L(G)$, the (closure) system of all linearly closed subsets of P. These subsets are precisely $\{\emptyset, P\} \cup \{\{p\}\colon p \in P\} \cup \{\hat{\ell}\colon \ell \in L\}$ and the Hasse diagram of these subsets looks like:



Alternatively we can let $M(G) = P \cup L \cup \{0, 1\}$ (assuming these sets are disjoint) and define a partial order relation on $M(G)$ by:

$$x \leq y \quad \text{iff} \quad \begin{cases} x = y \\ x = 0 \\ y = 1 \\ x \in P,\ y \in L \ \text{ and } \ xIy\,. \end{cases}$$

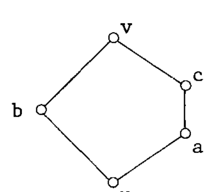
PROPOSITION: $(M(G); \leq)$ is a lattice in which

(a) For $p \neq q$ in P, $p \vee q = \ell(p, q)$.

(b) For $\ell \neq m$ in L, $\ell \wedge m$ is the (unique) point guaranteed by (PP2).

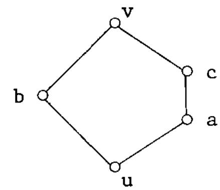
We now wish to characterize the lattices $(M; \vee, \wedge)$ [or $(M; \leq)$] that are produced by projective planes. To do this we need some terminology.

Let $(M; \vee, \wedge)$ be a lattice. $(M; \vee, \wedge)$ is said to be bounded if there exists $0, 1 \in M$ with $0 \leq x \leq 1$ for all $x \in M$. For $x \leq y$ in M, $[x, y] = \{z \in M\colon x \leq z \leq y\}$. If $(M; \vee, \wedge)$ is bounded, $a \in M$ (respectively $c \in M$) is called an atom (resp. coatom) if $[0, a] = \{0, a\}$ (resp. $[c, 1] = \{c, 1\}$). A spanning 3-frame in a bounded lattice $(M; \vee, \wedge)$ is a sequence (x_1, x_2, x_3, x_4) in M satisfying $(F_3 1)$ $\bigvee(p_j\colon j \neq i) = 1$, (all i) and $(F_3 2)$ $p_i \wedge \bigvee(p_k\colon k \neq i, j) = 0$, (all $i \neq j$). Finally a lattice $(M; \vee, \wedge)$ is called modular if M does not contain a sublattice of the form



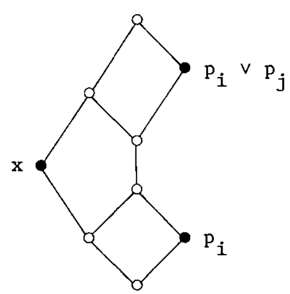
THEOREM. *Projective planes "are" precisely modular lattices* $(M; \vee, \wedge)$ *that contain a spanning 3-frame* (p_1, p_2, p_3, p_4) *of atoms.*

Proof. If $G = (P, L, I)$ is a projective plane, then $(M(G); \vee, \wedge)$ has a spanning 3-frame by (PP3). If $(M(G); \vee, \wedge)$ contained a sublattice of the form

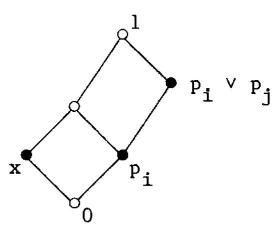


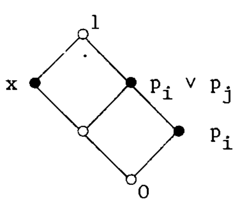
then by the construction of $M(G)$ we would have $u = 0$, $a \in P$, $c \in L$ and $v = 1$. Since $b \in P \cup L$ we obtain contradictions on $b \in P$ by (PP1) and $b \in L$ by (PP2). Therefore $(M(G); \vee, \wedge)$ is also a modular lattice.

Conversely suppose $(M; \vee, \wedge)$ is a modular lattice with a spanning 3-frame of atoms, (p_1, p_2, p_3, p_4). For $i \neq j$ we obtain from modularity that $0 \prec p_i \prec p_i \vee p_j \prec 1$ (where $a \prec b$ means $|[a, b]| = 2$). Now if $x \in M \setminus \{0, 1\}$, there exists $i \neq j = 1, \ldots, 4$ with $x \notin \{0, p_i, p_i \vee p_j, 1\}$. Since the free lattice generated by $\{x, p_i, p_i \vee p_j\}$ is



we have, since M is modular and $0 \prec p_i \prec p_i \vee p_j \prec 1$, only two possible homomorphic images in M; viz





In the first case x is an atom, and in the second, a coatom (again by modularity). Therefore if P is the set of atoms of M and L the set of coatoms, we have $(M; \vee, \wedge) = (M(G); \vee, \wedge)$ for $G = (P, L, <)$. Easy calculations show that $(P, L, <)$ is a projective plane.

For a more detailed analysis, the reader may consult [64]. For his/her own proof, the following results will help.

THEOREM (Dedekind [27]). *Let* $(M; \vee, \wedge)$ *be a lattice; then the following are equivalent:*

(1) $(M; \vee, \wedge)$ *is modular.*

(2) $(M; \vee, \wedge)$ *satisfies:* $(\forall x, y, z \in M)(x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z)$.

(3) $(M; \vee, \wedge)$ *satisfies:* $(\forall x, y, z \in M)((x \wedge z) \vee (y \wedge z) = ((x \wedge z) \vee y) \wedge z))$.

LEMMA. If $(M; \vee, \wedge)$ is a modular lattice and $a, b \in M$, then the intervals $a \wedge b, b]$ and $a, a \vee b$ are isomorphic via the (order) isomorphisms $x \mapsto x \vee a$ and $y \mapsto y \wedge b$.

By defining a spanning n-frame in a (bounded) modular lattice $(M; \vee, \wedge)$ to be $n + 1$ elements $(p_1, \ldots, p_n, p_{n+1})$ satisfying: $(F_n 1)$ $\bigvee(p_j: j \neq i) = 1$, (all i) and $(F_n 2)$ $p_i \wedge \bigvee(p_k: k \neq i, j) = 0$, (all $i \neq j$) , we can by definition or theorem produce:

PROPOSITION. The projective geometries of dimension $n - 1$ "are" precisely those modular lattices with a spanning n-frame *of atoms*.

We should note several items. Firstly Dedekind's result allows one to define modular lattices by means of a lattice equation or identity (part (3)). Secondly the n-frame produces $(n - 1) + 2$ points in general position, an obvious requirement for a projective geometry of dimension $n - 1$. Finally, in order to produce a projective geometry, it is essential that the members of the spanning n-frame be *atoms* of the modular lattice. This last requirement is emphasized by the following important (counter) examples.

EXAMPLE A. The n-frame determined by a ring. Let $(R; +, -, 0, \times, 1)$ be a ring (with identity), and let $(L({}_R R^n); \subseteq)$ be the (complete) lattice of all submodules of the left R-module R^n . We let $\underset{\sim}{e}_0, \ldots, \underset{\sim}{e}_{n-1}$ be the standard basis of R^n , and define:

$$X_i = Re_i, \ i = 0, \ldots, n - 1$$

$$X_n = R(\sum_i^{0,n-1} \underset{\sim}{e}_i) = \{(x, x, \ldots, x): x \in R\} .$$

Easy calculations show that $(X_0, \ldots, X_n)$ is a spanning n-frame in $L({}_R R^n)$. Moreover X_0 is an atom in $L({}_R R^n)$ iff X_i is an atom in $L({}_R R^n)$ for all $i \leq n$ if and only if R is a skewfield (= division ring).

EXAMPLE B. The n-frame determined by an R-module M . Let R be a ring and $(M; +, -, 0, (x \mapsto rx)_{r \in R})$ be a left R-module. Define $(L({}_R M^n), \subseteq)$ to be the (complete) lattice of all submodules of the (bi-) product left R-module, M^n . There exists the canonical coproduct embeddings $\mu_i: M \to M^n$, $i = 1, \ldots, n$, and the canonical diagonal $\Delta: M \to M^n$. We define

$$Y_i = \mathrm{Im}\mu_i,\ i = 1, \ldots, n$$

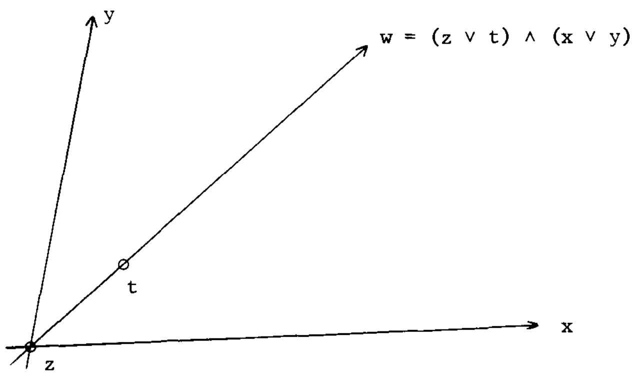
and
$$Y_{n+1} = \mathrm{Im}\Delta\ .$$

Again easy calculations show that $(Y_1, \ldots, Y_{n+1})$ is a spanning n-frame and that Y_1 is an atom in $L({}_RM^n)$ if and only if ${}_RM$ is simple.

2. ELEMENTARY COORDINATIZATION. The classical procedure to coordinatize a projective plane $G = (P, L, I)$ goes as follows:

(1) Take four points (x, y, z, t) in general position (i.e. a spanning 3-frame as guaranteed by (PP3)).

(2) Consider the line $h = x \vee y$ as the "line at infinity" and coordinatize the affine plane, $G_h = (P \setminus \hat{h}, L \setminus \{h\}, I)$ determined by h by means of the three parallel classes of lines: $y \vee z$, the y-axis; $x \vee z$, the x-axis; and $z \vee t$, the coordinatizing diagonal. In pictures we have



Lattice theoretically we have the points of the affine plane defined as complements of h

$$A_h = \{p\colon p \vee h = 1 \text{ and } p \wedge h = 0\}\ .$$

The coordinatizing diagonal, the points on $z \vee t$ save for w, the point at infinity

$$\begin{aligned} D &= \{p \in A_h\colon p \le z \vee t\} \\ &= \{p\colon p \vee w = z \vee t \text{ and } p \wedge w = 0\}\ . \end{aligned}$$

LEMMA. There is a bijection between A_h and $D \times D$ namely $p \mapsto ((z \vee t) \wedge (y \vee p), (z \vee t) \wedge (x \vee p))$ with inverse $(a, b) \mapsto (y \vee a) \wedge (x \vee b)$.

<u>Proof</u>. $w \vee [(z \vee t) \wedge (y \vee p)] = (z \vee t) \wedge (w \vee y \vee p) = z \vee t$ since $w \vee y = h$ and $w \wedge (z \vee t) \wedge (y \vee p) = w \wedge h \wedge (y \vee p) = w \wedge [y \vee (h \wedge p)] = w \wedge y = 0$. Therefore, using $x - y$ symmetry, $p \mapsto ((z \vee t) \wedge (y \vee p), (z \vee t) \wedge (x \vee p))$ is indeed a mapping from A_h into $D \times D$. Similar modular calculations give $(a,b) \mapsto (y \vee a) \wedge (x \vee b)$

as a function from $D \times D$ into A_h .

Now $(y \vee [(z \vee t) \wedge (y \vee p)]) \wedge (x \vee [(z \vee t) \wedge (x \vee p)]) = (y \vee z \vee t) \wedge (y \vee p) \wedge \wedge (x \vee z \vee t) \wedge (x \vee p) = (y \vee p) \wedge (x \vee p) = p \vee (y \wedge h \wedge (x \vee p)) = p \vee (y \wedge [x \vee \vee (h \wedge p)]) = p \vee (y \wedge x) = p$, $(z \vee t) \wedge [y \vee ((y \vee a) \wedge (x \vee b))] = (z \vee t) \wedge (y \vee a) \wedge \wedge (y \vee x \vee b) = a$ and $(z \vee t) \wedge [x \vee ((y \vee a) \wedge (x \vee b))] = b$. Therefore these functions are inverse to each other.

EXAMPLE A (n = 3). By letting $(X, Y, Z, T) = (R\underset{\sim}{e}_1, R\underset{\sim}{e}_2, R\underset{\sim}{e}_0, R(\underset{\sim}{e}_0 + \underset{\sim}{e}_1 + \underset{\sim}{e}_2))$ we have:

(i) $W = R(\underset{\sim}{e}_1 + \underset{\sim}{e}_2)$

(ii) $A_H = \{R(\underset{\sim}{e}_0 + a\underset{\sim}{e}_1 + b\underset{\sim}{e}_2)\colon (a, b) \in R^2\}$

(iii) $\mathcal{D} = \{R(\underset{\sim}{e}_0 + a\underset{\sim}{e}_1 + a\underset{\sim}{e}_2)\colon a \in R\}$.

Proof. Let S be a submodule of ${}_RR^3$ with $S + H = R^3$ and $S \cap H = 0$ (Note $H = R\underset{\sim}{e}_1 + R\underset{\sim}{e}_2$.). Since $\underset{\sim}{e}_0 \in S + H$ there exists an $\underset{\sim}{s}$ in S and $a,b \in R$ such that $\underset{\sim}{e}_0 = \underset{\sim}{s} - (a\underset{\sim}{e}_1 + b\underset{\sim}{e}_2)$. Therefore $R(\underset{\sim}{e}_0 + a\underset{\sim}{e}_1 + b\underset{\sim}{e}_2) \leq S$. But easy calculations show that $R(\underset{\sim}{e}_0 + a\underset{\sim}{e}_1 + b\underset{\sim}{e}_2)$ is a complement of H . Since $L({}_RR^3)$ is modular, we have $S = R(\underset{\sim}{e}_0 + a\underset{\sim}{e}_1 + b\underset{\sim}{e}_2)$.

If $S \in \mathcal{D}$ then $S \leq Z \vee T = Z \vee W = R\underset{\sim}{e}_0 + R(\underset{\sim}{e}_1 + \underset{\sim}{e}_2)$. Therefore $a = b$. That $W = R(\underset{\sim}{e}_1 + \underset{\sim}{e}_2)$ is easily seen.

EXAMPLE B (n = 3). Let $(X, Y, Z, T) = (Y_2, Y_3, Y_1, Y_4)$. Then

(i) $W = \{(0, x, x)\colon x \in M\}$.

(ii) $A_H = \{A_{(\phi,\psi)}\colon \phi, \psi \in \text{End } M\}$ where $A_{(\phi,\psi)} = \{(x, x\phi, x\psi)\colon x \in M\}$.

(iii) $\mathcal{D} = \{A_\phi\colon \phi \in \text{End } M\}$ where $A_\phi = A_{(\phi,\phi)}$.

Proof. Exercise.

In a projective plane, there are three major operations definable on a coordinatizing diagonal that are of interest: multiplication, addition, and the (planar) ternary ring operation. Since the multiplication and addition can be derived from the ternary ring operation, we consider it first.

We wish to construct the line analogous to the "ideal" affine line $Y = Xm + b$. To do so, we need a Y-intercept point (with coordinates $(0, b)$) and a parallel class or slope point on the line at infinity. The first is obtained by intersecting the line through (b, b) parallel with the x-axis with the y-axis. In lattice terms

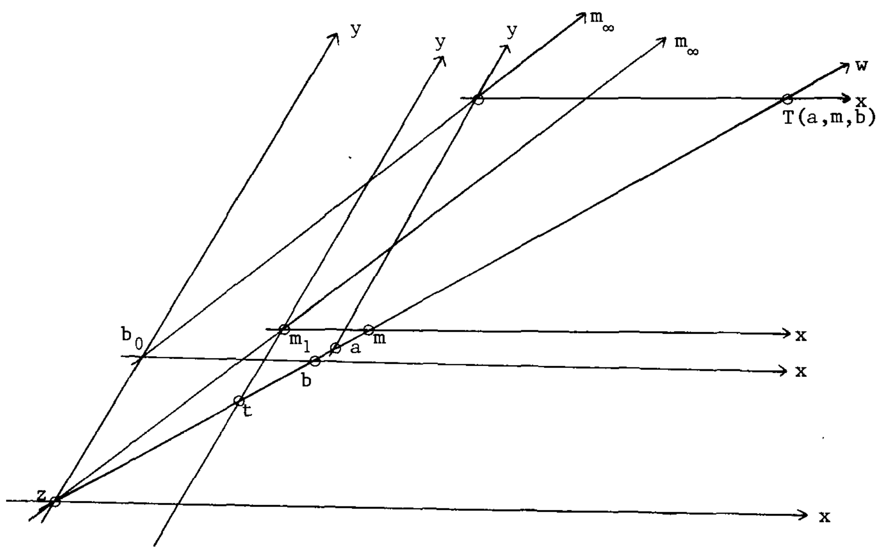
$$b_0 = (y \vee z) \wedge (x \vee b) .$$

The second is formed by finding the infinity point determined by the slope m .

$m_1 = (y \vee t) \wedge (x \vee m)$, the point $(1, m)$

$m_\infty = h \wedge (z \vee m_1)$, the parallel class of lines with slope m .

Our desired line is now $m_\infty \vee b_0$. The reader should show that $z_\infty = x$ (slope zero) and $t_\infty = w$ (unit slope). We now can compute what is supposed to be $am + b$ by going up to the line by $y = a$ (ie. $y \vee a$) and across to the diagonal by $x \vee [(y \vee a) \wedge (m_\infty \vee b_0)]$. In pictures:



In lattice theory, for $a, m, b \in D$

$$T(a, m, b) = (z \vee t) \wedge \{x \vee [(y \vee a) \wedge (b_0 \vee m_\infty)]\}$$
$$a \otimes b = T(a, b, z) = (z \vee t) \wedge \{x \vee [(y \vee a) \wedge (z \vee b_1)]\}$$
$$a \oplus b = T(a, t, b) = (z \vee t) \wedge \{x \vee [(y \vee a) \wedge (b_0 \vee w)]\}$$

LEMMA. $T: D^3 \to D$.

Proof. We must calculate using the modular law.

$$\begin{aligned} w \vee T(a, m, b) &= (z \vee t) \wedge \{w \vee x \vee [(y \vee a) \wedge (b_0 \vee m_\infty)]\} \\ &= (z \vee t) \wedge \{h \vee [a \wedge (y \vee b_0 \vee m_\infty)]\} \\ &= (z \vee t) \wedge (h \vee a) \quad \text{since } y \vee b_0 \vee m_\infty = 1 \\ &= z \vee t \\ w \wedge T(a, m, b) &= w \wedge \{x \vee [h \wedge (y \vee a) \wedge (b_0 \vee m_\infty)]\} \\ &= w \wedge \{x \vee [y \wedge (b_0 \vee m_\infty)]\} \\ &= w \wedge x, \quad \text{since } y \wedge (b_0 \vee m_\infty) = 0 \\ &= 0 \end{aligned}$$

EXAMPLE A ($n = 3$) . Let $A(a) = R(\underset{\sim}{e}_0 + a(\underset{\sim}{e}_1 + \underset{\sim}{e}_2))$ for $a \in R$.

(i) $A(b)_0 = R(\underset{\sim}{e}_0 + b\underset{\sim}{e}_2)$

(ii) $A(m)_\infty = R(\underset{\sim}{e}_1 + m\underset{\sim}{e}_2)$

(iii) $(Y \vee A(a)) \wedge (A(b)_0 \vee A(m)_\infty) = R(\underset{\sim}{e}_0 + a\underset{\sim}{e}_1 + (am + b)\underset{\sim}{e}_2)$

(iv) $T(A(a), A(m), A(b)) = A(am + b)$

(<u>Warning</u>: In performing the above calculations do not make the false assumption that R is a division ring or field! We did not assume $x \neq 0$ and $xy = xz$ implies $y = z$. Such a false assumption would allow one to show $R(a\underset{\sim}{e}_0 + b\underset{\sim}{e}_1 + c\underset{\sim}{e}_2) = [R\underset{\sim}{e}_0 \vee R(b\underset{\sim}{e}_1 + c\underset{\sim}{e}_2)] \wedge [R\underset{\sim}{e}_1 \vee R(a\underset{\sim}{e}_0 + c\underset{\sim}{e}_2)] \wedge [R\underset{\sim}{e}_2 \vee R(a\underset{\sim}{e}_0 + b\underset{\sim}{e}_1)]$. <u>This is not necessarily so!</u>)

EXAMPLE B ($n = 3$). $T(A_\phi, A_\psi, A_\theta) = A_{\phi\psi+\theta}$ where again right hand functional notation is used $x \mapsto x(\phi\psi + \theta) = (x\phi)\psi + (x)\theta$.

We should note that our affine "points" A_h and "coordinatizing diagonal" D depend not only on the chosen spanning 3-frame but also on the order given to the chosen points. There exists projective planes and four points p_1, p_2, p_3, p_4 satisfying (PP3) such that non-isomorphic ternary rings are obtained for different assignments of $\{x, y, z, t\} = \{p_1, p_2, p_3, p_4\}$. (c.f. Demboski [31])

Projective planes provide examples where $\oplus$ and $\otimes$ are not "well behaved". Our examples A and B provide a different type of aberration. In a projective plane two distinct points meet to 0, and join to produce a line. In examples A and B, these properties fall apart.

EXAMPLE A ($n = 3$). $L({}_RR^3)$ is a projective plane if and only if R is a division ring (or skewfield). In general for $a \in R$,

(1) $Z \wedge A(a) = 0$ if and only if $\ell(a) = \{x \in R: xa = 0\} = 0$.

(2) $Z \vee A(a) = Z \vee T$ if and only if there exists $b \in R$ with $ba = 1$.

EXAMPLE B ($n = 3$). (M^3) is a projective plane if and only if ${}_RM$ is a simple R-module. In general for $\phi \in \mathrm{End}({}_RM)$.

(1) $Z \wedge A_\phi = 0$ if and only if ϕ is injective.

(2) $Z \vee A_\psi = Z \vee T$ if and only if ϕ is surjective.

Before exploiting the above question of invertibles, we need to examine the general case of a spanning (n+1)-frame $(x_1, \ldots, x_n, z, t)$ in an arbitrary modular lattice $(M; \vee, \wedge)$. We define:

$$h = \bigvee(x_i : 1 \leq i \leq n)$$
$$A_h = \{p \in M: p \vee h = 1 \text{ and } p \wedge h = 0\}$$
$$w = h \wedge (z \vee t)$$
$$D = \{a \in A_h: a \leq z \vee t\} = \{a \in M: a \vee w = z \vee t \text{ and } a \wedge w = 0\}$$
$$\bar{x}_i = \bigvee(x_j : j \neq i).$$

The affine space A_h, with respect to the "hyperplane at infinity" h can be coordinatized by means of the coordinatizing diagonal D viz:

(i) $p \in A_h \mapsto (a_1, \ldots, a_n)$ where $a_i = (z \vee t) \wedge (\bar{x}_i \vee p)$

(ii) $(a_1, \ldots, a_n) \mapsto \bigwedge(\bar{x}_i \vee a_i : i = 1, \ldots, n) := (1; \underset{\sim}{a})$.

LEMMA. The above functions establish a bijection between A_h and D^n .

For each $i = 1, \ldots, n$, and $y_i = \bar{x}_i \wedge (z \vee t \vee x_i)$, we obtain a 3-frame (x_i, y_i, z, t) spanning the interval $[0, z \vee t \vee x_i]$. For this 3-frame, $w_i = (z \vee t) \wedge (x_i \vee y_i) = w$, and therefore its spanning 3-frame has D as its coordinatizing diagonal. This 3-frame supplies then a planar ternary ring operation on D :

$$T_i(a, m, b) = (z \vee t) \wedge \{x_i \vee [(\bar{x}_i \vee a) \wedge (b_{i0} \vee m_{i\infty})]\}$$

where $b_{i0} = (\bar{x}_i \vee z) \wedge (x_i \vee b)$, $m_{i1} = (\bar{x}_i \vee t) \wedge (x_i \vee m)$ and $m_{i\infty} = h \wedge (z \vee m_{i1})$.

Easy modular lattice calculations will convince the reader that any x', y' satisfying $x' \wedge (z \vee t) = y' \wedge (z \vee t) = 0$ and $(x' \vee y') \wedge (z \vee t) = w$ will produce a ternary operator $T'\colon D^3 \to D$. If $(x', y') \leq (x'', y'')$ in $M \times M$, then $T' = T''$ since both operators produce comparable complements of w in $[0, z \vee t]$. If $n \geq 3$, then $(x_1, y_1) \leq (x_1, \bar{x}_1) \leq (\bar{x}_3, \bar{x}_1) \geq (\bar{x}_3, x_3) \leq (\bar{x}_3, \bar{x}_2) \geq (x_2, \bar{x}_2) \geq (x_2, y_2)$. Therefore all T_i, $i = 1, \ldots, n \geq 3$ are the same ternary operator.

We now state some general results for T, $\oplus$ and $\otimes$. They are phrased in the language of a modular lattice with spanning 3-frame. The above discussions apply to these considerations as well if $n \geq 3$.

LEMMA. $(D; \oplus, z)$ is a loop with left and right difference operators from D to D defined by:

$$c\Delta_r b = (z \vee t) \wedge (y \vee [(x \vee c) \wedge (w \vee b_0)])$$
$$a_\ell\Delta c = (z \vee t) \wedge (x \vee \{(y \vee z) \wedge [w \vee ((y \vee a) \wedge (x \vee c))]\}) .$$

That is: $c = a \oplus b$ iff $a = c\Delta_r b$ iff $b = a_\ell\Delta c$.

As we have seen multiplication need not behave as nicely as addition. We can define $\mathrm{Inv}(D) = \{a \in D\colon z \vee a = z \vee t$ and $z \wedge a = 0\}$, and left and right division functions from D^2 <u>into $[0, z \vee t]$</u> by:

$$c/b = (z \vee t) \wedge [y \vee [(x \vee c) \wedge (z \vee b_1)]]$$
$$a\backslash c = (z \vee t) \wedge [x \vee \{(y \vee t) \wedge [z \vee ((y \vee a) \wedge (x \vee c))]\}] .$$

LEMMA. (1) $a \otimes z = z = z \otimes a$

(2) $z \otimes t = a = t \otimes a$

(3) If $a \in \mathrm{Inv}(D)$ and $b \in D$, $a\backslash b$ and $b/a \in D$

(4) $a \in \mathrm{Inv}(D)$ iff $b \otimes a = t = a \otimes c$ for some $b, c \in D$.

LEMMA. For $b \in D$ and any $p, q \in [0, z \vee t]$

(1) $p \otimes b \leq q$ iff $p \leq q/b$

(2) $b\backslash p \leq q$ iff $p \leq b \otimes q$.

EXAMPLE A $(n = 3)$. For $A(a)$ and $A(b) \in \mathcal{D}$

(i) $A(a)\backslash A(b) = R(a\underset{\sim}{e}_0 + b(\underset{\sim}{e}_1 + \underset{\sim}{e}_2))$

(ii) $A(a)/A(b) = \{x\underset{\sim}{e}_0 + y(\underset{\sim}{e}_1 + \underset{\sim}{e}_2): xa = yb\}$.

EXAMPLE B $(n = 3)$. For A_ϕ and $A_\psi \in \mathcal{D}$

(i) $A_\phi\backslash A_\psi = \{(x\phi, x\psi, x\psi): x \in M\}$

(ii) $A_\phi/A_\psi = \{(x, y, y): x\phi = y\psi\}$.

LEMMA. For $a, b \in D$, $a \vee b = z \vee t$ and $a \wedge b = 0$ if and only if $a\Delta_r b \in \mathrm{Inv}(D)$.

Proof. $z \vee (a\Delta_r b) = z \vee [w \wedge (a \vee b)]$ and $z \wedge (a\Delta_r b) = z \wedge [w \vee (a \wedge b)]$. Therefore $a\Delta_r b \in \mathrm{Inv}(D)$ iff $z \vee [w \wedge (a \vee b)] = z \vee w$ and $z \wedge [w \vee (a \wedge b)] = 0$ iff $w \leq a \vee b$ and $w \geq a \wedge b$ iff $a \vee b = z \vee t$ and $a \wedge b = 0$.

The final result of this section provides a more algebraic description of projective geometries.

THEOREM. *Let* $(M; \vee, \wedge)$ *be a modular lattice; then* $(M; \vee, \wedge)$ *is a projective geometry of dimension* n *if and only if the following properties are satisfied:*

(1) M *has a spanning* $(n+1)$*-frame* $(x_1, \ldots, x_n, z, t)$

(2) M *is generated as a lattice by* $D \cup \{x_1, \ldots, x_n\}$

(3) $D = \{z\} \cup \mathrm{Inv}(D)$.

3. THE ARGUESIAN LAW. It is well known that there exists projective planes that do not satisfy Desargues' Axiom. In [116], Jónsson introduced a lattice identity which precisely reflected Desargues' Axiom. In the last 18 years much work has been done by Jonsson et al (see [119], [125], [128], and [66]). We present in this section a development based more on hindsight than Jónsson's original pioneering work.

DEFINITION 1. A lattice $(L; \vee, \wedge)$ is called Desarguean* if it satisfies the implication

$$\begin{aligned}&[(a_0 \vee b_0) \wedge (a_1 \vee b_1) \leq a_2 \vee b_2] \Rightarrow \\ &\quad \Rightarrow [(a_0 \vee a_1) \wedge (b_0 \vee b_1) \leq [(a_0 \vee a_2) \wedge (b_0 \vee b_2)] \vee \\ &\qquad \vee [(a_1 \vee a_2) \wedge (b_1 \vee b_2)]] .\end{aligned}$$

In order to maintain a geometric flair we call triples, $\underset{\sim}{a} = (a_0, a_1, a_2)$ and $\underset{\sim}{b} = (b_0, b_1, b_2) \in L^3$, <u>triangles</u> in L . <u>We do not assume that these elements of L are atoms!</u> Two triangles in L, $\underset{\sim}{a}$ and $\underset{\sim}{b}$, are called <u>centrally perspective</u> if $(a_0 \vee b_0) \wedge (a_1 \vee b_1) \leq a_2 \vee b_2$. This may be abbreviated as $CP(\underset{\sim}{a}, \underset{\sim}{b})$ or just CP if the meaning is clear. For triangles, $\underset{\sim}{a}$ and $\underset{\sim}{b}$ in L , we write for $i \leq 2$, $c_i = c_i(\underset{\sim}{a}, \underset{\sim}{b}) = (a_j \vee a_k) \wedge (b_j \vee b_k)$ where $\{i, j, k\} = \{0, 1, 2\}$. The triangles are called <u>axially</u> perspective (or $AP(\underset{\sim}{a}, \underset{\sim}{b})$ or just AP) if $c_2 \leq c_0 \vee c_1$. The

* The spelling liberties taken here will be explained later.

Desarguean implication then becomes "centrally perspective triangles are axially perspective".

LEMMA 2. Desarguean lattices are modular.

Proof. Consider the triangles $\underset{\sim}{a} = (x, x \vee z, x)$ and $\underset{\sim}{b} = (x, y, y)$ in a Desarguean lattice $(L; \vee, \wedge)$. They are centrally perspective trivially. Therefore $c_2 \leq c_0 \vee c_1$. This produces for all $x, y, z \in L$,

$$(x \vee y) \wedge (x \vee z) \leq x \vee [y \wedge (x \vee z)] ,$$

an inequality equivalent to modularity.

The pertinent question now is to compare Desarguean (modular) lattices with a spanning 3-frame of atoms and projective planes satisfying Desargues' Axiom. Since Desargues' Axiom for projective planes is usually stated with several inequality assumptions as well as the assumption that the triangles are indeed triangles of points, we must show that in all "degenerate" cases, AP follows from CP and the modular law.

LEMMA 3. Let $(L; \vee, \wedge)$ be a modular lattice and let $\underset{\sim}{a}$ and $\underset{\sim}{b}$ be centrally perspective triangles in L. If $a_i \leq a_j$ or $b_i \leq b_j$ for some $i \neq j$ in $\{0,1,2\}$ then $\underset{\sim}{a}$ and $\underset{\sim}{b}$ are axially perspective.

Proof. By $\underset{\sim}{a} - \underset{\sim}{b}$ symmetry it is enough to consider comparabilities in the triangle $\underset{\sim}{a}$ and by $0 - 1$ symmetry it is enough to consider three cases: $a_0 \leq a_1$, $a_0 \leq a_2$ and $a_2 \leq a_0$.

Case (i). If $a_0 \leq a_1$ then $a_0 \leq a_2 \vee b_2$ by CP. Moreover $c_2 = a_1 \wedge (b_0 \vee b_1)$. Now $c_1 \leq a_0 \vee a_2 \leq a_1 \vee a_2$ gives

$$\begin{aligned} c_0 \vee c_1 &= (a_1 \vee a_2) \wedge (b_1 \vee b_2 \vee c_1) \\ &= (a_1 \vee a_2) \wedge (b_1 \vee b_2 \vee [b_0 \wedge (a_0 \vee a_2 \vee b_2)]) \\ &\geq (a_1 \vee a_2) \wedge (b_1 \vee b_2 \vee [b_0 \wedge (a_1 \vee b_1)]) \quad \text{by CP} \\ &= (a_1 \vee c_2) \wedge (b_2 \vee [(b_1 \vee b_0) \wedge (a_1 \vee b_1)]) \\ &\geq c_2 . \end{aligned}$$

Case (ii) is left for the reader.

Case (iii). If $a_2 \leq a_0$ then using CP and modularity $(a_2 \vee a_1 \vee b_1) \wedge (a_0 \vee b_0) \leq a_2 \vee [(a_1 \vee b_1) \wedge (a_0 \vee b_0)] \leq a_2 \vee b_2$ and

$$\begin{aligned} c_0 \vee c_1 &= c_0 \vee [a_0 \wedge (b_0 \vee b_2)] \\ &= c_0 \vee [a_2 \wedge (b_0 \vee b_2)] \wedge [a_0 \wedge (b_0 \vee b_2)] \\ &= \{(a_1 \vee a_2) \wedge (b_1 \vee b_2 \vee [a_2 \wedge (b_0 \vee b_2)])\} \vee [a_0 \wedge (b_0 \vee b_2)] \end{aligned}$$

$$\begin{aligned}
&= \{(a_1 \vee a_2) \wedge (b_1 \vee [(b_2 \vee a_2) \wedge (b_0 \vee b_2)])\} \vee [a_0 \wedge (b_0 \vee b_2)] \\
&\geq \{(a_1 \vee a_2) \wedge (b_1 \vee [(a_1 \vee a_2 \vee b_1) \wedge (a_0 \vee b_0) \wedge (b_0 \vee b_2)])\} \vee \\
&\qquad \vee [a_0 \wedge (b_0 \vee b_2)] \\
&= \{(a_1 \vee a_2) \wedge (b_1 \vee [(a_0 \vee b_0) \wedge (b_0 \vee b_2)])\} \vee [a_0 \wedge (b_0 \vee b_2)] \\
&= (b_1 \vee [(a_0 \vee b_0) \wedge (b_0 \vee b_2)]) \wedge [a_1 \vee a_2 \vee \{a_0 \wedge (b_0 \vee b_2)\}] \\
&\geq (b_1 \vee b_0) \wedge [a_1 \vee (a_0 \wedge (b_0 \vee b_2 \vee a_2))] \\
&\geq (b_0 \vee b_1) \wedge [a_1 \vee (a_0 \wedge \{b_0 \vee [(a_2 \vee a_1 \vee b_1) \wedge (a_0 \vee b_0)]\})] \\
&= (b_0 \vee b_1) \wedge [a_1 \vee (a_0 \wedge (b_0 \vee a_2 \vee a_1 \vee b_1))] = c_2 \ .
\end{aligned}$$

This last lemma throws out many degenerate substitutions. Our next lemma makes our lattice triangles behave like real geometric triangles.

LEMMA 4. A lattice $(L; \vee, \wedge)$ is Desarguean if and only if centrally perspective triangles, $\underset{\sim}{a}$ and $\underset{\sim}{b}$, satisfying $a_i = (a_i \vee a_j) \wedge (a_i \vee a_k)$ and $b_i = (b_i \vee b_j) \wedge (b_i \vee b_k)$ for $\{i, j, k\} = \{0, 1, 2\}$ are axially perspective.

Proof. Let $\underset{\sim}{a}, \underset{\sim}{b}$ be centrally perspective triangles in a lattice satisfying our (restricted) condition. (A quick check of lemma 2 shows that such a lattice is modular!) Define $a_i' = (a_i \vee a_j) \wedge (a_i \vee a_k)$ and $b_i' = (b_i \vee b_j) \wedge (b_i \vee b_k)$ for $\{i, j, k\} = \{0, 1, 2\}$. Easy checking shows that $\underset{\sim}{a}'$ and $\underset{\sim}{b}'$ satisfy our extra condition.

Now

$$\begin{aligned}
(a_0' \vee b_0') \wedge (a_1' \vee b_1') &= [a_0 \vee (a_1 \wedge (a_0 \vee a_2)) \vee b_0 \vee (b_1 \vee (b_0 \wedge b_2))] \wedge \\
&\quad \wedge [a_1 \vee (a_0 \wedge (a_1 \vee a_2)) \vee b_1 \vee (b_0 \wedge (b_1 \vee b_2))] \\
&= (a_1 \wedge (a_0 \vee a_2)) \vee (b_1 \wedge (b_0 \vee b_2)) \vee (a_0 \wedge (a_1 \vee a_2)) \vee \\
&\quad \vee (b_0 \wedge (b_1 \vee b_2)) \vee [(a_0 \vee b_0) \wedge (a_1 \vee b_1)] \\
&\leq (a_1 \wedge (a_0 \vee a_2)) \vee (b_1 \wedge (b_0 \vee b_2)) \vee (a_0 \wedge (a_1 \vee a_2)) \vee \\
&\quad \vee (b_0 \wedge (b_1 \vee b_2)) \vee (a_2 \vee b_2) \\
&= a_2' \vee b_2' \ .
\end{aligned}$$

Therefore $\underset{\sim}{a}'$ and $\underset{\sim}{b}'$ are centrally perspective triangles satisfying the extra condition. Since $c_i' = c_i$ for $i = 0, 1, 2$, we obtain $AP(\underset{\sim}{a}', \underset{\sim}{b}') = AP(\underset{\sim}{a}, \underset{\sim}{b})$.

THEOREM 5. Let $(M; \vee, \wedge)$ be a projective plane. $(M; \vee, \wedge)$ is a Desarguean lattice if and only if, qua geometry, $(M; \vee, \wedge)$ satisfies Desargues' Axiom.

Proof. Given the usual statement of Desargues' Axiom we have a few more "degenerate" cases to check. Using $\underset{\sim}{a} - \underset{\sim}{b}$ and $0 - 1$ symmetry these cases reduce to: $a_0 \leq b_0 \vee b_2$, $a_2 \leq b_0 \vee b_2$, and $a_0 \leq b_0 \vee b_1$. The ingeneous reader will be able to prove AP from CP and any of the above conditions in a modular lattice! The restriction to a projective plane together with the restrictions that $\underset{\sim}{a}$ and $\underset{\sim}{b}$ are point triangles (lemmata 3 and 4) provide easier methods. Hint: For $\{i,j\} = \{0,1\}$,

$c_i \geq [a_2 \wedge (b_j \vee b_2)] \vee [b_2 \wedge (a_j \vee a_2)]$, therefore $c_0 \vee c_1 = c_0' \vee c_1'$ where $c_i' = c_i \vee [a_2 \wedge (b_i \vee b_2)] \vee [b_2 \wedge (a_i \vee a_2)]$. Compute c_i', $i = 0, 1$ using as well $CP(a, b)$.

Since the modular implication is equivalent to an identity and modular lattices are characterized by the exclusion of the pentagon, it is natural to ask such questions for Desarguean lattice. The first will be answered affirmatively while the second is still an open problem.

LEMMA 6. If $FM(6)$ with free generators $\{x_0, x_1, x_2, y_0, y_1, y_2\}$ the triangles $\langle x_0, x_1, x_2 \vee [x_0 \wedge (x_1 \vee y_1)]\rangle$ and $\langle y_0 \wedge [x_0 \vee ((x_1 \vee y_1) \wedge (x_2 \vee y_2))], y_1, y_2\rangle$ are centrally perspective.

Proof. Compute.

THEOREM 7. *A lattice is Desarguean if and only if it satisfies the identity* $\lambda \leq \rho$ *where*

$$\lambda = (x_0 \vee x_1) \wedge (y_0' \vee y_1)$$
$$\rho = [(x_0 \vee x_2) \wedge (y_0 \vee y_2)] \vee [(x_1 \vee x_2) \wedge (y_1 \vee y_2)] \vee [y_1 \wedge (x_0 \vee x_1)]$$

and $y_0' = y_0 \wedge [x_0 \vee ((x_1 \vee y_1) \wedge (x_2 \vee y_2))]$.

Proof. Since every Desarguean lattice is modular, the identity follows from lemma 6. Conversely if L satisfies the identity, then firstly L is modular. (See lemma 2 for the correct substitution.) Secondly if $\underset{\sim}{a}$ and $\underset{\sim}{b}$ are centrally perspective triangles in L ,

$$b_0' \geq b_0 \wedge [[a_0 \vee [(a_1 \vee b_1) \wedge (a_0 \vee b_0)]] = b_0 \wedge (a_0 \vee a_1 \vee b_1)$$
$$\lambda(\underset{\sim}{a}, \underset{\sim}{b}) \geq (a_0 \vee a_1) \wedge (b_0 \vee b_1) = c_2$$
$$\begin{aligned}\rho(\underset{\sim}{a}, \underset{\sim}{b}) &= c_1 \vee c_0 \vee [b_1 \wedge (a_0 \vee a_1)] \\ &= c_1 \vee [(b_1 \vee b_2) \wedge (a_2 \vee a_1 \vee [a_0 \wedge (a_1 \vee b_1)])] \\ &\leq c_1 \vee [(b_1 \vee b_2) \wedge (a_2 \vee a_1 \vee [a_0 \wedge (a_2 \vee b_2)])] \\ &= c_1 \vee c_0 \vee [b_2 \wedge (a_0 \vee a_2)] \\ &= c_0 \vee c_1 \leq \rho(\underset{\sim}{a}, \underset{\sim}{b}) .\end{aligned}$$

Therefore $c_2 \leq \lambda(a, b) \leq \rho(a, b) = c_0 \vee c_1$.

The Arguesian identity introduced by Jónsson in [118] and proven equivalent to the Desarguean implication in [66] and [128] is not the one presented above. In order to give it and several other equivalent forms, let $a_0, a_1, a_2, b_0, b_1, b_2$ be six variables and define lattice terms

$$p = (a_0 \vee b_0) \wedge (a_1 \vee b_1) \wedge (a_2 \vee b_2)$$
$$c_i = (a_j \vee a_k) \wedge (b_j \vee b_k) \quad \{i, j, k\} = \{0, 1, 2\}$$

and $\quad \bar{c} = c_2 \wedge (c_0 \vee c_1)$.

THEOREM 8. *For a lattice* $(L; \vee, \wedge)$, *the following are equivalent.*

(1) L *is Desarguean*

(2) L *satisfies* $p \leq a_0 \vee [b_0 \wedge (b_1 \vee \bar{c})]$

(3) L *satisfies* $p \leq [a_0 \wedge (a_1 \vee \bar{c})] \vee [b_0 \wedge (b_1 \vee \bar{c})]$

(4) L *satisfies* $p \leq a_0 \vee b_1 \vee \bar{c}$

Proof. Clearly (3) implies (2) and (2) implies (4). Moreover all imply L is modular. To obtain (2) implies (3), use the symmetry of p to deduce

$$p \leq (a_0 \vee [b_0 \wedge (b_1 \vee \bar{c})]) \wedge (b_0 \vee [a_0 \wedge (a_1 \vee \bar{c})])$$
$$= [a_0 \wedge (a_1 \vee \bar{c})] \vee [b_0 \wedge (b_1 \vee \bar{c})]$$ after some calculations using the modular law.

(4) implies (1) is a recent result of Doug Pickering [29]. If $\underset{\sim}{a}$ and $\underset{\sim}{b}$ are centrally perspective then (4) gives us

$$(a_0 \vee b_0) \wedge (a_1 \vee b_1) \leq a_0 \vee b_1 \vee \bar{c} .$$

Joining both sides with $a_0 \vee b_1$ and then meeting with c_2 produces

$$c_2 \leq c_2 \wedge [c_0 \vee c_1 \vee (c_2 \wedge (a_0 \vee b_1))] \leq c_2 .$$

Easy modular calculations and central perspectivity show that

$$c_0 \vee c_1 \vee (c_2 \wedge (a_0 \vee b_1)) = c_0 \vee c_1 \vee [a_0 \wedge (b_0 \vee b_1)] \vee [b_0 \wedge (a_0 \vee a_1)] = c_0 \vee c_1 .$$

Finally we show that for modular lattices, the identity in Theorem 7 is merely an adjustment of (2):

$$p \leq a_0 \vee [b_0 \wedge (b_1 \vee \bar{c})]$$
iff $a_0 \vee p \leq a_0 \vee [b_0 \wedge (b_1 \vee [(a_0 \vee a_1) \wedge (c_0 \vee c_1)])]$

iff $b_0 \wedge [a_0 \vee p_{12}] \leq a_0 \vee [b_0 \wedge (b_1 \vee [(a_0 \vee a_1) \wedge (c_0 \vee c_1)])]$

where $p_{12} = (a_1 \vee b_1) \wedge (a_2 \vee b_2)$

iff $b_0 \wedge [a_0 \vee p_{12}] \leq b_0 \wedge (b_1 \vee [(a_0 \vee a_1) \wedge (c_0 \vee c_1)])$

iff $b_0 \wedge [a_0 \vee p_{12}] \leq b_1 \vee [(a_0 \vee a_1) \wedge (c_0 \vee c_1)]$

iff $b_1 \vee [b_0 \wedge (a_0 \vee p_{12})] \leq b_1 \vee [(a_0 \vee a_1) \wedge (c_0 \vee c_1)]$

iff $(a_0 \vee a_1)\{b_1 \vee [b_0 \wedge (a_0 \vee p_{12})]\} \leq c_0 \vee c_1 \vee [b_1 \wedge (a_0 \vee a_1)]$.

We should note that Jónsson's form of the Arguesian identity has allowed Gratzer and Lakser to produce an identity that holds in every complemented modular lattice, and to provide other proofs of some of the above results. The reader should consult [64; p. 205-214] for these.

Finally, as Jónsson has observed, we have Cartesian coordinates and not Descartesian coordinates. This provides in the author's mind sufficient justification for the appellation "Arguesian". The author's spelling of Desarguean (instead of Desarguesian) has no justification save that it better translates into English usage the French pronunciation of Desargues.

4. FULL COORDINATIZATION RESULTS. The classical coordinatization theorem of projective geometry states that every (finite dimensional) Desarguean projective geometry is coordinatized by a division ring. In lattice theoretical language this would become: every (finite dimensional) complemented, modular, algebraic lattice, L, is isomorphic to $L({}_K V)$ for some (finite dimensional) vector space V over a division ring K. The extensions of this result that concern us will all impose a finite dimensionality condition on the given lattice L. This condition is of course, the existence of a spanning n-frame.

DEFINITION 1. A lattice L is said to be <u>of order n</u> if L possesses a spanning n-frame.

An early restriction on the order of the (modular) lattice under consideration was that $n \geq 4$. This restriction occurred since there exists non-Desarguean projective planes (ie. $n = 3$) and since every (finite-dimensional) projective geometry of dimension ≥ 3 (ie. of order qua lattice, ≥ 4) was Desarguean (qua lattice, Arguesian). When von Neumann obtained the following result, he assumed that L was complemented. Freese noticed that von Neumann really did not use complementation - an important observation for Freese's subsequent results. Artmann obtained another proof of this result that latticizes the geometrical notion of special central collineation.

THEOREM 2 (von Neumann [161], Artmann [6]). *Let* L *be a modular lattice of order* n*, for* $n \geq 4$. *If* $(x_1, \ldots, x_{n-1}, z, t)$ *is a spanning* n*-frame, then* $(D; \oplus, z, \otimes, t)$ *is a ring.*

The companion theorem for Arguesian lattices was proved recently by the author and Douglas Pickering.

THEOREM 3 (Day and Pickering [28]). *Let* L *be an Arguesian lattice of order* n *for* $n \geq 3$. *If* $(x_1, \ldots, x_{n-1}, z, t)$ *is a spanning* n*-frame, then* $(D; \oplus, z, \otimes, t)$ *is a ring.*

The major problems in the above proof were commutativity and associativity of addition. These proofs made essential use of the multiplicative unit, t. Unless alternative proofs are found, a counterexample to Jónsson's question concerning Arguesian lattices and type I-representability may be obtainable by producing a counterexample to these supposed alternative proofs.

The complete coordinatization theorems of von Neumann, Jónsson, Baer-Inaba and Jónsson-Monk will be stated presently. They all state conditions when a modular lattice of order n is isomorphic to a (sub) lattice of $L({}_R R^n)$ for suitable rings R. The von Neumann and Baer-Inaba results for certain modular lattices of order $n \geq 4$ provide proofs that their lattices are indeed Arguesian. As we shall see these deep coordinatization theorems are not needed for that fact.

THEOREM 4 (Day and Pickering [28]). *Let* L *be an Arguesian lattice of order* $n+1$ *for* $n \geq 2$ *and* $(x_1, \ldots, x_n, z, t)$ *a spanning* $(n+1)$*-frame. The function* F *on* $[0, h]$ *defined by* $\underset{\sim}{a} \in F(p)$ *iff* $h \wedge (z \vee (1; \underset{\sim}{a})) \leq p$ *is an (arbitrary) meet preserving map from* $[0, h]$ *into* $L({}_D D^n)$. *If* L *also satisfies* (h - UC) , *then* F *is a lattice homomorphism. If also* $\{h \wedge (z \vee (1; \underset{\sim}{a})) \colon \underset{\sim}{a} \in D^n\}$ *separates elements of* $[0, h]$, *then* F *is a lattice isomorphism onto a sublattice of* $L({}_D D^n)$ *containing all finitely generated submodules.*

The condition (h - UC) is an Upper Complementability condition for $h : p \vee h = 1$ implies there exists $q \in A_h$ with $q \leq p$. It is a condition that holds in any $L({}_R R^{n+1})$ hence it is necessary for any full coordinatization result. It need not be true in our examples of the form $L({}_R M^{n+1})$, where it at least implies a type of self projectivity condition.

We can now present the two main full coordinatization results.

THEOREM 5 (von Neumann [161], Jónsson [118]). *Every complemented modular (resp. Arguesian) lattice of order* n *for* $n \geq 4$ *(resp.* $n \geq 3$*) is isomorphic to the lattice* $\bar{L}({}_R R^n)$ *of all finitely generated submodules of* ${}_R R^n$ *for some regular ring* R .

Outline of Proof. By Frink [51], every complemented modular lattice, L , is a sublattice of a projective geometry. If $n \geq 4$, the dimension of this geometry is greater than equal to 3. Therefore the geometry, qua lattice, and in particular L is Arguesian. Thus Jónsson's result includes trivially(?) von Neumann's.

Given that L is complemented, the $F \colon [0, h] \to L({}_D D^n)$ is a lattice embedding and D is a regular ring. Again since L is complemented, every $p \in L$ is of the form $q \vee (h \wedge p)$ where $q \wedge h = 0$. This allows F to be extended to $G \colon L \to L({}_D D^{1+N})$ as in von Neumann's Case II ([161]).

To present the Baer-Inaba, Jónsson-Monk result we must introduce some less familiar terminology. A ring is said to be completely primary and uniserial if there is a (two-sided) ideal, P , of R such that $L({}_R R) = L(R_R) = \mathrm{Id}(R) = \{R = P^0, P, P^2, \ldots, P^k = \{0\}\}$. An element c of a finite dimensional modular lattice L is called a cycle if $[0, c]$ is a chain. A dual cycle is defined dually. A modular lattice L is called primary if it is finite dimensional, every element is the join of cycles and the meet of dual cycles, and every interval that is not a chain contains at least three atoms. One can easily deduce that a primary lattice of geometric dimension n (see Jónsson-Monk [128]) is a primary lattice possessing a spanning n-frame of cycles and conversely.

THEOREM 6 (Baer-Inaba [14], [113], Jónsson-Monk [128]). *Every primary modular (resp. Arguesian) lattice of order* n *for* $n \geq 4$ *(resp.* $n \geq 3$*) is isomorphic to* *the lattice* $\bar{L}({}_R R^n)$ *of all finitely generated submodules of* ${}_R R^n$ *for some completely primary and uniserial ring* R .

Outline of Proof. By Monk [140], every (modular) primary lattice of order $n \geq 4$ is Arguesian. Therefore Jónsson-Monk subsumes Baer-Inaba. Again, primary Arguesian lattices allow the full effect of Theorem 4, so $F: [0, h] \to L({}_D D^n)$ is a lattice embedding. Since L is primary, D becomes a completely primary and uniserial ring. F is extended to $G: L \to L({}_D D^{1+n})$ by an intricate examination of the properties of cycles. The reader should consult [128] for the (many) details.

It would be of some interest if a common proof could be provided for both the above theorems. This would require the right common generalization of von Neumann regular and completely primary-uniserial rings. This is at present unknown. One seemingly crucial common fact is that for every n and every $\underset{\sim}{a} \in R^n$, $R\underset{\sim}{a}$ is a member of the sublattice of $L({}_R R^n)$ generated by the canonical n-frame and its coordinatizing diagonal.

PROBLEM. For which rings, R , is the above always true?

5. THE ARITHMETIC OF FRAMES. There are many properties of the models $L({}_R R^n)$ and $L({}_R M^n)$ which can be completely interpretted in the general frame model. In this section we will develop some of the more useful results.

In both EXAMPLE A and EXAMPLE B, $n = 3$, we have that the interval [0, T] is precisely the left ideals (resp. submodules) of the ring R (resp. left module M) . In general, if (x, y, z, t) is a spanning 3-frame in a modular lattice L (with $h = x \vee y$, $w = h \wedge (z \vee t)$, A_h and D as before) we can associate with each $p \in [0,t]$, a "left ideal" of D .

DEFINITION. For $p \in [0, t]$,

$$I(p) = \{a \in D: t \wedge (z \vee a) \leq p\} .$$

Easy calculations show that I(p) is close to being a true left ideal (if addition were properly behaved).

LEMMA. For all $p \in [0, t]$, I(p) satisfies

(1) $z \in I(p)$

(2) $a, b \in I(p)$ implies $a \Delta_r b \in I(p)$

(3) $a \in D$ and $b \in I(p)$ imply $a \otimes b \in I(p)$.

Since the map $p \leadsto I(p)$ is not necessarily well behaved, it is sometimes better to consider the elements of [0, t] as the "left ideals" or "submodules". In this case, if $P, Q \leq M$, then $L(P^n), L(Q^n) \leq L(M^n)$ with $P^n \wedge Q^n = (P \wedge Q)^n$ and $P^n \vee Q^n = (P \vee Q)^n$. This process is completely generalized.

LEMMA. The map $\hat{\ }: [0, t] \to L$ defined by $\hat{p} = (x \vee y \vee p) \wedge (x \vee z \vee p) \wedge \wedge (y \vee z \vee p)$ is a lattice embedding with $\hat{0} = 0$, $\hat{t} = 1$ and $t \wedge \hat{p} = p$ for all $p \in [0, t]$.

Proof. Since $(x \vee y \vee p) \wedge (x \vee y \vee q) = x \vee y \vee [p \wedge (x \vee y \vee q) \wedge t] = = x \vee y \vee (p \wedge q)$, we have, using $\{x, y, z\}$-symmetry, that $\hat{\ }$ preserves meets. Noting that $\hat{p} = [x \wedge (y \vee z \vee p)] \vee [y \wedge (x \vee z \vee p)] \vee [z \wedge (x \vee y \vee p)]$ and that $[x \wedge (y \vee z \vee p)] \vee [x \wedge (y \vee z \vee q)] = x \wedge (y \vee z \vee p \vee q)$, we have, again by symmetry, that $\hat{\ }$ preserves joins. Since $t \wedge \hat{p} = p$, $\hat{\ }$ is an embedding. That $\hat{0} = 0$ and $\hat{t} = 1$ follows by the frame properties of (x, y, z, t) .

EXAMPLE B $(n = 3)$. For $U \leq M$ and $P = \{(x, x, x): x \in U\} \leq T$, $\hat{P} = U^3$.

Now $L(U^3) \leq L(M^3)$ and $L((M/U)^3)$ embeds into $[U^3, M^3]$. Moreover both lattices have their own canonical n-frames.

LEMMA. For $p \in [0, t]$, and $\hat{p}$ as previously defined,

(1) $\hat{p} \vee (x, y, z, t)$ is a 3-frame spanning $[\hat{p}, 1]$

(2) $\hat{p} \wedge (x, y, z, t)$ is a 3-frame spanning $[0, \hat{p}]$.

By EXAMPLE B $(n = 3)$, we have $\mathcal{D}(U^3) \cong \mathrm{End}(U)$ and $\mathcal{D}((M/U)^3) \cong \mathrm{End}(M/U)$. Moreover there are easy to find examples in module theory for which there is little relation between these endomorphism rings and the original one $\mathrm{End}(M) \cong \mathcal{D}(M^3)$. If $\phi \in \mathrm{End}(M)$ and U is ϕ-invariant (i.e. $[U]\phi \subseteq U$) , then $\phi|U \in \mathrm{End}(U)$. Moreover U being ϕ-invariant is also the criterion for the completion (commutatively of course) of the diagram

$$\begin{tikzcd}
M \arrow[r, "\phi"] \arrow[d, "\kappa"'] & M \arrow[d, "\kappa"'] \\
M/U \arrow[r, dashed, "\exists\tilde{\phi}"] & M/U
\end{tikzcd}$$

LEMMA. For $p \in [0, t]$ and $a \in D$, the following are equivalent:

(1) $a \wedge \hat{p} \in D[0, \hat{p}]$

(2) $a \vee \hat{p} \in D[\hat{p}, 1]$

(3) $\langle a, w, \hat{p}\rangle$ is a distributive sublattice of L

(4) $t \wedge (z \vee p \otimes a) \leq p$.

Proof. Easy calculations give us that $w \wedge \hat{p} = [(z \wedge \hat{p}) \vee (t \wedge \hat{p})] \wedge [(x \wedge \hat{p}) \vee \vee (y \wedge \hat{p})]$ and $w \vee \hat{p} = [(z \vee \hat{p}) \vee (t \vee \hat{p})] \wedge [(x \vee \hat{p}) \vee (y \vee \hat{p})]$. Therefore (1) is equivalent to $(a \wedge \hat{p}) \vee (w \wedge \hat{p}) = (z \wedge \hat{p}) \vee (t \wedge \hat{p}) = (z \vee t) \wedge \hat{p} = (a \vee w) \wedge \hat{p}$. Similarly (2) is equivalent to $(a \vee \hat{p}) \wedge (w \vee \hat{p}) = \hat{p} = (a \wedge w) \vee \hat{p}$. Therefore (1), (2) and (3) are equivalent. By direct calculation, $t\wedge(z\vee p\otimes a) = t\wedge(z\vee(a\wedge(w\vee p)))$ and

$t \wedge (z \vee p \otimes a) \leq p$ holds if and only if $a \wedge (w \vee p) \leq z \vee p$. Since (3) is also equivalent to $a \wedge (w \vee \hat{p}) \leq \hat{p}$, we obtain that (3) is equivalent with (4).

DEFINITION. For $a \in D$ and $p \in [0, t]$, we say that <u>a lifts modulo p</u> if one of the above equivalent conditions hold.

LEMMA. For $a \in D$ and $p \in [0, t]$, if a lifts modulo p then so does $t \oplus a$ and $a \oplus t$.

<u>Proof.</u> That b lifts modulo p is easily shown to be equivalent to $w \wedge (p \vee b) \leq$ $\leq z \vee p$, and also to $b \wedge (w \vee p) \leq z \vee p$. Therefore if $w \wedge (p \vee a) \leq z \vee p$, we compute

$$\begin{aligned}
w \wedge (p \vee t \oplus a) &= w \wedge (p \vee x \vee [(y \vee t) \wedge (w \vee a_0)]) \\
&= w \wedge (x \vee [(y \vee t) \wedge (p \vee w \vee a_0)]) \\
&= w \wedge (y \vee t \vee [x \wedge (p \vee w \vee [(y \vee z) \wedge (x \vee a)])]) \\
&= w \wedge (t \vee y \vee [x \wedge (y \vee z \vee [(x \vee a) \wedge (p \vee w)])]) \\
&= w \wedge (t \vee [(y \vee x) \wedge (y \vee z \vee [a \wedge (p \vee w)])]) \\
&= w \wedge (t \vee [w \wedge (y \vee z \vee [a \wedge (p \vee w)])]) \\
&= w \wedge (z \vee [a \wedge (p \vee w)]) \\
&\leq w \wedge (z \vee p) \quad \text{by assumption.}
\end{aligned}$$

COROLLARY. If a lifts modulo p then:

(1) in $D[\hat{p}, 1]$, $(a \vee \hat{p}) \oplus (t \vee \hat{p}) = (a \oplus t) \vee \hat{p}$

(2) in $D[0, \hat{p}]$, $(a \wedge \hat{p}) \oplus (t \wedge \hat{p}) = (a \oplus t) \wedge \hat{p}$.

We now are ready to examine particular $p \in [0, t]$ that are "naturally" defined by the coordinatizing diagonal. For any $a \in D$, $p = \mathrm{pr}(a) \equiv t \wedge (z \vee a)$, the "principal ideal generated by a" or $q = \mathrm{ann}(a) \equiv t \wedge (w \vee (z \wedge a))$ are excellent choices and the reader should be able to check the following results.

LEMMA. For $a, b \in D$

(1) a lifts modulo $\mathrm{pr}(b)$ iff $\mathrm{pr}(b \otimes a) \leq \mathrm{pr}(a)$

(2) a lifts modulo $\mathrm{ann}(b)$ iff $\mathrm{ann}(b) \leq \mathrm{ann}(a \otimes b)$

(3) $\mathrm{pr}(a) \leq \mathrm{pr}(b)$ iff $w \vee (a/b) = z \vee t$

(4) $\mathrm{ann}(a) \leq \mathrm{ann}(b)$ iff $w \wedge (a\backslash b) = 0$.

Specializing even further, we can interpret the natural numbers in D via

$$\begin{aligned}
\underset{\sim}{0} &= z \\
(\underset{\sim}{n+1}) &= t \oplus (\underset{\sim}{n})
\end{aligned}$$

and define the characteristic of a 3-frame by:

DEFINITION. A 3-frame (x, y, z, t) in a modular lattice L is said to have characteristic q for $q \in \mathbb{N}$ if $\underset{\sim}{q} = z$.

Our previous lemmata now produce the following important results.

THEOREM. *Let* L *be a modular lattice with spanning* 3-*frame* (x, y, z, t) *and let* $q, r \in \mathbb{N}$; *then:*

(1) $\underset{\sim}{q}$ *lifts modulo* $\mathrm{pr}(\underset{\sim}{r})$

(2) $\hat{\mathrm{pr}}(\underset{\sim}{r}) \vee (x, y, z, t)$ *is a* 3-*frame of characteristic* r

(3) $\hat{\mathrm{ann}}(\underset{\sim}{r}) \wedge (x, y, z, t)$ *is a* 3-*frame of characteristic* r .

We note that everything above works for all n-frames, $n \geq 3$. We state the relevant results found in their full generality in Herrmann-Huhn [94] and Freese [46].

THEOREM. *Let* $\underset{\sim}{x} = (x_1, \ldots, x_{n+1})$ *be an* n-*frame in a modular lattice* L , *spanning the interval* $[u, v]$. *Then for* $\underset{\sim}{y} \in L^{n+1}$ *with* $u \leq y_i \leq x_i$ *for all* i , *the following are equivalent.*

(1) $\underset{\sim}{y}$ *is an* n-*frame*

(2) $\bar{y}_i = \bar{y}_j$ *for all* $i \neq j$

(3) *For some* i *and all* $j \neq i$, $y_j = x_j \wedge (\bar{x}_{ij} \vee y_i)$

(4) *For all* $i \neq j$, $y_j = x_j \wedge (\bar{x}_{ij} \vee y_i)$

Moreover if the above hold and $w = \bar{y}_i$, *then* $\underset{\sim}{y} = w \wedge \underset{\sim}{x}$, *and* $w \vee \underset{\sim}{x}$ *is an* n-*frame spanning the interval* $[w, v]$.

If $n = 3$ and L is not Arguesian then our definition of characteristic seems to depend on the orientation of our 3-frame (although no counter-example is known to the author). If L is Arguesian or $n \geq 4$, then for any permutation $\pi \in \mathrm{Sym}(n+1)$, $x = (x_1, \ldots, x_{n+1})$ has characteristic q if and only if $(x)\pi = (x_{1\pi}, \ldots, x_{(n+1)\pi})$ has characteristic q .

Our final comment in this section concerns our definition of an n-frame. von Neumann defined a spanning homogeneous n-frame to be a family $(a_1, \ldots, a_n; c_{ij}, i \neq j = 1, \ldots, n)$ such that $1 = \bigvee a_i$, $0 = a_i \wedge \bigvee_{j \neq i} a_j$, $c_{ij} = c_{ji}$, $a_i \vee a_j = a_i \vee c_{ij}$, $a_i \wedge c_{ij} = 0$, and $c_{ik} = (a_i \vee a_k) \wedge (c_{ij} \vee c_{jk})$. Our definition of an n-frame is exactly Huhn's definition of an (n-1)-diamond. Herrmann and Huhn in [95] showed that these concepts were indeed definitionally equivalent.

THEOREM. *If* $(a_1, \ldots, a_n; c_{ij}, i \neq j = 1, \ldots, n)$ *is a von Neumann homogeneous spanning* n-*frame in a modular lattice* L , *then* $(a_1, c_{12}, \ldots, c_{n-1,n}, a_n)$ *is a Huhn spanning* (n-1)-*diamond. Conversely if* $(x_1, \ldots, x_{n+1})$ *is a Huhn spanning* (n-1) *diamond, then* $(a_1, \ldots, a_n; c_{ij}; t \neq j = 1, \ldots, n)$ *is von Neumann homogeneous. spanning* n-*frame where*

$$a_i = (\bigvee (x_k;\ k \leq i)) \wedge (\bigvee (x_j:\ j > i)),\ i = 1, \ldots, n$$

$$c_{i,i+1} = x_{i+1} \quad \textit{for} \quad 1 \leq i \leq n-1$$

and for $i < j$, $c_{ij} = c_{ji} = (a_i \vee a_j) \wedge (c_{i,i+1} \vee \cdots \vee c_{j-1,j})$.

Huhn's own results (as well as others) indicate that his concept is more manageable and provides better geometric insight into most applications. We have therefore adopted his concept and von Neumann's numbering in our definition of an n-frame.

6. APPLICATIONS TO THE THEORY OF MODULAR LATTICES. In this section we will try to outline some of the applications of n-frames and coordinatizations to the equational theory of modular lattices. This outline will unfortunately not be exhaustive since, for no other reason, research is continuing. Our main attentions will be focussed on the works of Freese, Herrmann, and Huhn.

One of the principal tools used for these results is the projectivity (in modular lattices) of certain partial lattices. We first formulate the general notions.

DEFINITION. Let $\mathcal{K}$ be a variety of algebras. A configuration in $\mathcal{K}$ is a pair (X, R) where $R \subseteq F_{\mathcal{K}}(X) \times F_{\mathcal{K}}(X)$. An algebra $A \in \mathcal{K}$ <u>has the configuration (X, R) by means of</u> $\alpha: X \to A$ if $R \subseteq \operatorname{Ker} \bar{\alpha}$ where $\bar{\alpha}$ is the unique extension of α, $\bar{\alpha}: F_{\mathcal{K}}(X) \to A$. If there is no chance of confusion we will sometimes say $Y \subseteq A$ is an (X, R) configuration if the $\alpha: X \to A$ such that $Y = \operatorname{Im} \alpha$ is obvious. Finally, a configuration (X, R) in $\mathcal{K}$ is called a <u>projective configuration in $\mathcal{K}$</u> if $F_{\mathcal{K}}(X; R)$, the $\mathcal{K}$-algebra freely generated by the presentation $(X; R)$, is a projective algebra in $\mathcal{K}$.

An easy universal algebraic fact is the following:

LEMMA. Let (X, R) be a configuration in a variety $\mathcal{K}$; then the following are equivalent:

(1) (X, R) is a projective configuration in $\mathcal{K}$.

(2) The canonical $\rho: F_{\mathcal{K}}(X) \twoheadrightarrow F_{\mathcal{K}}(X; R)$ splits.

(3) There exists polynomials $(p_x: x \in X)$ in $F_{\mathcal{K}}(X)$ such that for all $A \in \mathcal{K}$ and $\alpha: X \to A$, A has (X, R) by means of α if and only if for all $x \in X$ $\bar{\alpha}(x) = \bar{\alpha}(p_x)$.

(4) If $\alpha: X \to A$ gives (X, R) in A and $f: B \twoheadrightarrow A$ is a surjective homomorphism then there exists $\beta: X \to B$ giving (X, R) in B with $f \circ \beta = \alpha$.

Since the only configurations (in Mod) we have seen so far are the notions of an n-frame and of an n-frame of characteristic q, the next result should not be surprising.

THEOREM (Huhn [102] and Freese [46]). *An n-frame (resp. an n-frame of characteristic q) is a projective configuration in Mod.*

<u>Proof</u>. We exhibit the polynomials in $FM(n + 1)$ as required by the last lemma. For free variables $x_1, \ldots, x_{n+1}$, define:

$$v = \bigwedge_i \left(\bigvee_{j \neq i} x_j\right)$$

$$u = \bigvee_i \left(\bigwedge_{j\neq i}\left(\bigvee_{k\neq i,j} x_k\right)\right)$$

$$p_i = (u \vee x_i) \wedge v = u \vee (x_i \wedge v) .$$

To obtain an n-frame of characteristic q (possibly orientated if $n = 3$), we first obtain an n-frame. By orientating (w.ℓ.o.g. if $n \geq 4$) this frame as $(x_1, \ldots, x_{n-1}, z, t)$ and for $p = \mathrm{pr}(\underset{\sim}{q}) \leq t$ construct $\hat{p} \vee (x_1, \ldots, x_{n-1}, z, t)$ as the required frame of characteristic q.

Our second important (projective) configuration involves the Hall-Dilworth gluing of modular lattices. This notion's importance has been demonstrated by Hall-Dilworth in producing a modular lattice not embeddable into a complemented modular lattice and by Jónsson first by providing a classification of Arguesian lattices of length $n \leq 4$, [119], and secondly by finding an Arguesian lattice that was not representable as a lattice of subgroups of an Abelian group, [121]. It was Freese in [47] and [48] who applied Hall-Dilworth to frames and by doing so, showed the word problem for $FM(n)$, $n \geq 5$ to be unsolvable.

DEFINITION. Let $\underset{\sim}{x} = (x_1, \ldots, x_{n+1})$ be an n-frame in a modular lattice L spanning the interval $[0_x, 1_x]$. For $I \subseteq \{1, 2, \ldots, n+1\}$ we write

$$x_I = \bigvee(x_i : i \in I)$$

$$\bar{x}_I = \bigvee(x_j : j \notin I) .$$

For $I \subseteq \{1, 2, \ldots, n+1\}$, the <u>lower reduced frame determined by I</u> is $\{x_i : i \in I\} \cup \{x_I \wedge \bar{x}_I\}$ and the <u>upper reduced frame determined by I</u> is $\{x_j \vee x_I : j \notin I\}$.

From our choice of words, the next lemma should be obvious.

LEMMA. If $\underset{\sim}{x} = (x_1, \ldots, x_{n+}$ is an n-frame in a modular lattice L, and $I \subseteq \{1, \ldots, n+1\}$ with $|I| = k$, then the lower (resp. upper) reduced frame determined by I is a frame of order k (resp. $n - k$) spanning the interval $[0_{\underset{\sim}{x}}, x_I]$ (resp. $[x_I, 1_{\underset{\sim}{x}}]$.

We hasten to note that this lemma requires a modified definition of a k-frame for $k = 0, 1$. The obvious modifications are that a <u>0-frame</u> is a point, and a <u>1-frame</u> is the two-element lattice.

DEFINITION. The <u>k-dimensional gluing of an n-frame over an n-frame</u> is the configuration in Mod consisting of:

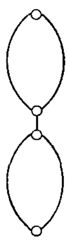
(1) An n-frame $\underset{\sim}{x}$ and an m-frame $\underset{\sim}{y}$.

(2) Sets $I \subseteq \{1, 2, \ldots, n+1\}$ and $J \subseteq \{1, 2, \ldots, m+1\}$ with $|I| = n - k$ and $|J| = k$.

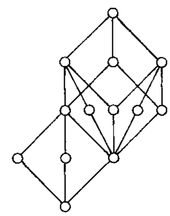
(3) $1_{\underset{\sim}{x}} \vee 0_{\underset{\sim}{y}} = y_J$ and $1_{\underset{\sim}{x}} \wedge 0_{\underset{\sim}{y}} = x_I$.

(4) Under the transposition $[x_I, 1_{\underset{\sim}{x}}] \searrow [0_{\underset{\sim}{y}}, y_J]$, the upper reduced frame determined by I maps onto the lower reduced frame determined by J .

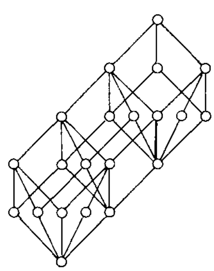
Obviously $k \leq \min\{n, m\}$ and if $k \neq 0$, we may assume that $J = \{1, 2, \ldots, k\}$ and $I = \{k + 2, \ldots, n + 1\}$. Some easy diagrams occur when $k, m,$ and n are small



$k = 0$



$k = 1, n = 2$ and $m = 3$



$k = 2, m = n = 3$

The following result was proven by Freese [47], for $n = m = 4$ and $k = 2$ and by the author for $m = n = k + 1$, [25] and [26].

THEOREM. *The* k*-dimensional gluing of an* m*-frame over an* n*-frame is a projective configuration in Mod. Moreover the* n *and* m*-frames may be given arbitrary characteristics.*

<u>Proof</u> (Sketch). Let $\phi\colon A \twoheadrightarrow B$ be a surjective homomorphism in Mod and let $(\underset{\sim}{x}, \underset{\sim}{y}, I, J)$ be a k-dimensional gluing of the n-frame $\underset{\sim}{y}$ over the n-frame $\underset{\sim}{x}$ in B . Since the case where $k = 0$ is trivial, we assume $k \geq 1$, $I = \{k + 2, \ldots, n+1\}$, $J = \{1, \ldots, k\}$ and

$$x_i \vee 0_{\underset{\sim}{y}} (\vee\, x_I) = \begin{cases} y_i, & i = 1, \ldots, k \\ y_J \wedge \bar{y}_J, & i = k + 1 \end{cases} .$$

Since n-frames are projective configurations, there is an n-frame $\underset{\sim}{u}$ in A with $(\underset{\sim}{u})\phi = \underset{\sim}{x}$, and an m-frame $\underset{\sim}{v}$ in u_I with $(\underset{\sim}{v})\phi = \underset{\sim}{b}$.

Now consider $z_1 = u_1 \wedge v_1, \ldots, z_k = u_k \wedge v_k, z_{k+1} = u_{k+1} \wedge v_J \wedge \bar{v}_J$, $z_{k+2} = u_{k+2}, \ldots, z_{n+1} = u_{n+1}$. We have $0_{\underset{\sim}{u}} \leq z_i \leq u_i$, $i = 1, \ldots, n+1$ and therefore $\underset{\sim}{u}' = (z_1 \wedge \bar{z}_1, \ldots, z_{n+1} \wedge \bar{z}_{n+1})$ is an n-frame with the properties:

(1) $(\underset{\sim}{u}')\phi = \underset{\sim}{x}$

(2) $u_i' \leq v_i \quad i = 1, \ldots, k$

(3) $u_{k+1}' \leq v_J \wedge \bar{v}_J$

(4) $u_i' \leq 0_v$, $i = k+1, \ldots, n+1$ and

(5) $1_{\underset{\sim}{u}'} \leq v_J$.

By letting $\underset{\sim}{u} = \underset{\sim}{u}'$ we now have two pre-image frames that satisfy the necessary order relations.

In order to fix the joins, let $v_i' = 0_{\underset{\sim}{v}} \vee u_i$, for $i = 1, \ldots, k+1$. These v_i' form a "sub" frame of the restricted frame $(v_1, \ldots, v_k, v_J \wedge \bar{v}_J)$ and this can be extended to a "sub"frame $\underset{\sim}{v}' = (v_1', \ldots, v_k', \ldots, v_{m+1}')$ of $\underset{\sim}{v}$ with $(\underset{\sim}{v}')\phi = \underset{\sim}{y}$.

In order to fix the required meets, we could look at the dual lattices and note that the dual of a k-dimensional gluing of an m-frame over an n-frame is a k-dimensional gluing of an n-frame over an m-frame. Alternatively we consider the ^-element generated from $\underset{\sim}{u}$ by $p = u_{k+1} \wedge 0_{\underset{\sim}{v}}$. This <u>is</u>

$$\hat{p} = 1_{\underset{\sim}{u}} \wedge 0_{\underset{\sim}{y}} \wedge \bigwedge_{\ell \in I} (u_1' \vee u_2' \vee \ldots \vee u_{k+1}' \vee u_{I \setminus \{\ell\}})$$

where $u_i' = u_i \wedge 0_{\underset{\sim}{v}}$. The n-frame $\hat{p} \vee \underset{\sim}{u}$ together with the (new) $\underset{\sim}{v}$ have all the desired properties.

The addition of characteristics is left to the reader. He or she may consult Freese [46, Theorem 2.1] on how to do it.

The importance of projective configurations lies in the following facts. Let (X, R) be a projective configuration in a variety K and let V be a subvariety of K . If $\nu\colon F_K(X) \twoheadrightarrow F_V(X)$ is the canonical surjection then we have the commutative diagram:

$$\begin{tikzcd}
F_K(X; R) \arrow[r, tail, "\mu"] \arrow[d, "f"] & F_K(X) \arrow[r, two heads, "\rho"] \arrow[d, "\nu"] & F_K(X; R) \arrow[d, "f"] \\
F_V(X; R) \arrow[r, tail, "\mu'"] & F_V(X) \arrow[r, two heads, "\rho'"] & F_V(X; R)
\end{tikzcd}$$

with $\rho \circ \mu = \text{ident}$ and $\rho' \circ \mu' = \text{ident}$. For any $p, q \in F_K(X; R)$ we then obtain that V satisfies the <u>equation</u> $(\mu(p), \mu(q))$ if and only if all models of (X, R) in V satisfy the (extra) <u>relation</u> $(\mu(p), \mu(q))$. [That is: for all $B \in V$ and all $(X; R)$ configurations $\beta\colon X \to B$, $\beta(\mu(p)) = \beta(\mu(q))$.]

Now Herrmann and Huhn [94] have shown that an n-frame $(n \geq 3)$, x, in a modular lattice is either trivial $[x_1 = x_2 = \ldots = x_{n+1}]$ or non-trivial $[x_i \nleq x_j$ for all $i \neq j]$. From this one can derive that for $k \geq 1$ the k-dimensional gluing of an m-frame, $\underset{\sim}{y}$, over an n-frame $\underset{\sim}{x}$ (with or without specified characteristics) can be really trivial $[x_1 = \ldots = x_{n+1} = y_1 = \ldots = y_{m+1}]$, essentially trivial $[x_1 = \ldots = x_{n+1} < y_1 = \ldots = y_{m+1}]$ or non-trivial [all x_i's are pairwise distinct and all y_j's are pairwise distinct]. By judicious use of $p, q \in F_K(x; R)$, the following results are obtained.

THEOREM (Huhn [103], Bergman [17]). *For any* $n \geq 1$ *the class of all modular lattices not containing a (non-trivial)* (n+1)*-frame is an equational class of modular lattices. Two equivalent defining equations are:*

(1) n-*distributivity:* $x \wedge \bigvee_{i}^{1,n} y_i = \bigvee_{i}^{1,n} (x \wedge \bigvee_{j \neq i} y_j)$

(2) $\bigwedge_{i}^{1,n+1} (\bigvee_{j \neq i}^{1,n+1} x_i) = \bigvee_{i}^{1,n+1} (\bigwedge_{j \neq i}^{1,n+1} (\bigvee_{k \neq i,j}^{1,n+1} x_k))$

This result provides dimension discriminating equations for projective geometries in that:

COROLLARY (Huhn [103]). A projective geometry $G = (P, L, I)$ is of dimension $\leq n - 1$ if and only if $L(G)$ is n-distributive.

THEOREM. *For* $k \geq 1$, $n, m \geq 2$, *the class of all modular lattices containing at most essentially trivial* k*-dimensional gluings of an* m*-frame over an* n*-frame is an equational class.*

In [25], the case where $n = m = k + 1$ was studied and a rather complicated explicit form was given for the so called n-gluing dimension equation, (GD_n).

These equations also provided a dimension discriminating system of varieties that are finer than Huhn's n-distributivity equations. In fact the subdirectly irreducible algebras of maximal possible order in such a variety are, if they are generated by their frame and coordinatizing diagonal, projective geometries. For these results the reader should consult [25].

More importantly, there are the two applications of Freese in [47] and [48].

THEOREM (Freese [47]). *The variety of all modular lattices is not generated by its finite members.*

Proof (Sketch). Take $k = 2$, $m = n = 4$ and let $\underset{\sim}{x}$ be of characteristic p and $\underset{\sim}{y}$ of characteristic q for distinct primes p and q. We examine models of this projective configuration in $K = HSP(Mod_{fin})$. Since the configuration is projective we need only examine models that are subdirect products of finite modular lattices hence only finite models. Now $n = m \geq 4$ will produce two finite rings of characteristic p and q which because of the two-dimensional overlap must have the same cardinality. Therefore the only models of this configuration are (essentially) trivial and we have an equation satisfied by all finite modular lattices.

THEOREM (Freese [48]). *The word problem for* $FM(n)$, $n \geq 5$ *is recursively unsolvable.*

Proof (Sketch). Here Freese again took a special 2-dimensional gluing of 4-frames, the lower of which contained a coded version of a (multiplicative) finitely presented group with an unsolvable word problem. The projectivity of this configuration allowed him to obtain a copy of this configuration in a free modular lattice, and an examination of the necessary generators showed that 5 sufficed.

Recently Herrmann has extended both of these results. After characterizing the free modular lattice generated by an n-frame for $n \geq 4$, he applied this to obtain the following extremely important result.

THEOREM (Herrmann [91]). *An equational class of modular lattices that contains all rational projective geometries,* $L(\mathbb{Q}^n)$, *cannot be both finitely based and generated by its finite dimensional members.*

COROLLARY. Modular lattices and Arguesian lattices are not generated by their finite dimensional members.

In a very recent preprint Herrmann, [93], has also replaced 5 by 4 in Freese's second main result. He used another projective configuration, that of a "skew-frame of type (4, 3) and weak characteristic 3×3" . His main theorem is then that the word problem for $FM(n)$, $n \geq 4$ is recursively unsolvable.

Department of Mathematical Sciences
Lakehead University
Thunder Bay, Ontario
Canada P7B 5E1

REFERENCES.

1. Amemiya, I., On the representation of complemented modular lattices, J. Math. Soc. Japan, 9, 263-279, (1957).
2. Artin, E., Geometric Algebra, Interscience, New York, (1957).
3. Artmann, B., Automorphismen und Koordinaten bei ebenen Verbanden, Mitt. Math. Sem. Giessen, Heft 66, 1-58, (1965).
4. Artmann, B., Bemerkungen zu einem verbandstheoretischen Problem von Skornyakov, Archiv der Mathematik, 18, 226-229, (1967).
5. Artmann, B., Ein Struktursatz fur ebene Verbande, Archiv der Mathematik, 18, 23-32, (1967).
6. Artmann, B., On coordinates in modular lattices, Illinois J. Math., 12, 626-648, (1968).
7. Artmann, B., Hjelmslev planes derived from modular lattices, Can. Jour. Math 21, 76-83, (1969).
8. Artmann, B., Hjelmselv-ebenen mit verfeinerten Nachbarschaftsrelationen, Math. Z., 112, 163-180, (1969).
9. Artmann, B., Uniforme Hjelmslev-ebenen und modulare Verbande, Math. Z., 111, 15-45, (1969).
10. Artmann, B., Hjelmslev-ebenen in projektiven Raumen, Archiv der Mathematik, 21, 304-307, (1970).
11. Artmann, B., Desarguessche Hjelmslev-ebenen n-ter stufe, Mitt. Math. Sem. Giessen, 91, 1-19, (1971).
12. Artmann, B., Geometric aspects of primary lattices, Pacific J. Math., 43, 15-25, (1972).
13. Baer, R., A unified theory of projective spaces and finite Abelian groups, Trans. Amer. Math. Soc., 52, 283-343, (1942).
14. Baer, R., Linear Algebra and Projective Geometry, New York, (1952).
15. Baker, K., Equational classes of modular lattices, Pacific J. Math, 28, 9-15, (1969).
16. Baker, K., Equational axioms for classes of lattices, Bull. Amer. Math. Soc., 77, 97-102, (1971).
17. Bergman, G., On 2-Firs (Weak Bezout Rings) with Distributive Divisor Lattices, Thesis, (1969).
18. Birkhoff, G., Combinatorial relations in projective geometries, Ann. Math., 36 (1935), 743-748.
19. Birkhoff, G., Lattice Theory, 3rd Ed., Amer. Math. Soc. Colloq. Publ., (1967).
20. Crawley, P. and Dilworth, R., Algebraic Theory of Lattices, Prentice-Hall, Englewood Cliffs, New Jersey, (1973).
21. Day, A., Splitting algebras and a weak notion of projectivity, Alg. Univ., 5, 153-162, (1973).
22. Day, A., In search of a Pappian lattice identity, Can. Math. Bull. 24, 187-198, (1981).
23. Day, A., A lemma on projective geometries as modular and/or Arguesian lattices, Can. Math. Bull (in print).
24. Day, A., On some geometric properties defining classes of rings and varieties of modular lattices, Alg. Univ. (in print).
25. Day, A., Dimension equations in modular lattices, Alg. Univ. (in print).
26. Day, A., Equational theories of projective geometries, Colloquium Janos Bolyai Society, Szeged 1980 (in print).
27. Day, A., Herrmann, C. and Wille, R., On modular lattices with four generators, Alg. Univ., 2, 317-323, (1974).
28. Day, A. and Pickering D., The coordinatization of Arguesian lattices, Trans. Amer. Math. Soc. (accepted).
29. Day, A. and Pickering D., A note on the Arguesian lattice identity, Proc. Visegrad Conference on Universal Algebra (1982).
30. Dedekind, R., Uber die drei Moduln erzeugte Dualgruppe, Math. Annalen, 53, 371-403, (1900).
31. Dembowski, P., Finite Geometries, Berlin-Heidelberg-Gottingen, (1958).
32. Dilworth, R., Note on complemented modular lattices, Bull. A. M. S., (1940).
33. Dilworth, R., The structure of relatively complemented modular lattices, Ann. of Math., 51, 348-359, (1950).

34. Dilworth, R. and Freese, R., Generators for lattice varieties, Alg. Univ., 6, 263-267, (1976).
35. Dilworth, R., and Hall, M., The embedidng theorem for modular lattices, Ann. Math., 45, 450-456, (1944).
36. Dlab, V. and Ringel, C., Perfect elements in free modular lattices, Vorabdruck, (1978).
37. Doyen, J. and Herrmann, C., Projective lines and n-distributivity, Colloq. Math. Soc. Janos Bolyai, 14, 45-50, (1976).
38. Drake, D., Coordinatization of H-planes by H-modules, Math. Z., (1970).
39. Freese, R., Congruence lattices of finitely generated modular lattices, preprint.
40. Freese, R., The word problem for modular lattices in six variables, preprint.
41. Freese, R., Subdirectly irreducible modular lattices of width four, Notices Amer. Math. Soc., 17, 1041, (1970).
42. Freese, R., Varieties generated by modular lattices of width four, Bull.Amer. Math. Soc., 78, 447-450, (1972).
43. Freese, R., Breadth two modular lattices, Proc. Univ. of Houston, 409-451, (1973).
44. Freese, R., Planar sublattices of FM(4), Alg. Univ., 6, 69-72, (1976).
45. Freese, R., Some varieties of modular lattices not generated by their finite dimensional members, Colloq. Math. Soc. Janos Bolyai, 17, 133-144, (1977).
46. Freese, R., Projective geometries as projective modular lattices, Trans. Amer. Math. Soc., 251, 329-342, (1979).
47. Freese, R., The variety of modular lattices is not generated by its finite members, Trans. Amer. Math. Soc., 255, 277-300, (1979).
48. Freese, R., Free modular lattices, Trans. Amer. Math. Soc., 261, 81-91, (1980).
49. Fried, E., The amalgamation class of certain classes of projective geometries, in preparation.
50. Fried, E. and Gratzer, G. and Lakser, H., Amalgamation and weak injectives in the equational class of modular lattices, Notices Amer. Math. Soc., 18, 624, (1971).
51. Frink, O., Complemented modular lattices and projective spaces of infinite dimension, Trans. Amer. Math. Soc., 60, 452-467, (1946).
52. Fryer, K. and Halperin, I., Coordinates in geometry, Trans. of the Royal Soc. of Canada, 48, 11-26, (1954).
53. Fryer, K. and Halperin, I., The von Neumann coordinatization theorem for complemented modular lattices, Acta. Sci. Math. Szeged, 17, 450-456, (1956).
54. Fryer, K. and Halperin, I., On the construction of coordinates for non-Desarguean complemented modular lattices, Nederl. Akad. Wetensch Ser. A., 61, 142-161, (1958).
55. Gabriel, P., Unzerlegbare Darstellungen I, Manuscripta Math., 6, 71-103, (1972).
56. Gabriel, P., Unzerlegbare Darstellungen II, Inst. Naz. Di Alta, 11, 81-104, (1973).
57. Gelfand, I. and Ponomarev, V., Problems of linear algebra and classification of quadruples of subspaces in a finite, dimensional vector space, Coll. Math. J. Bolyai, 5, 163-237, (1970).
58. Gelfand, I. and Ponomarev, V., Free modular lattices and their representations, Russian Math. Surveys, 29, 1-56, (1974).
59. Gelfand, I. and Ponomarev, V., Lattices representationes, and algebras connected with them I, Russian Math. Surveys, 31, 67-85, (1977).
60. Gelfand, I. and Ponomarev, V., Lattices, representations, and algebras connected with them II, Russian Math. Surveys, 32, 91-114, (1977).
61. Gleason, A., Finite Fano planes, Amer. Jour. Math., 78, 797-808, (1956).
62. Gratzer, G., Equational classes of lattices, Duke Jour. Math., 33, 613-622, (1966).
63. Gratzer, G., Lattice Theory: First Concepts and Distributive Lattices, W. H. Freeman, (1971).
64. Gratzer, G., Lattice Theory, Freeman, San Francisco, (1971).
65. Gratzer, G. and Wonenburger, M., Some examples of complemented modular lattices, Can. Math. Bull., 5, 111-121, (1962).
66. Gratzer, G. and Lakser, H. and Jónsson, B., The amalgamation property in equational classes of modular lattices, Pacific J. Math., 45, 507-524, (1973).
67. Gross, H., Quadratic forms in infinite dimensional vector spaces, Birkhauser, Boston, (1979).
68. Hall, M., Projective planes, Trans. Amer. Math. Soc., (1943).

69. Hall, M., On the lattice of normal subgroups of a group, AMS Symp. Pure Math., Lattice Theory, (1961).
70. Hall, M. (Jr.), Projective planes and related topics, Calif. Inst. Tech., (1954).
71. Halperin, I., Coordinates in geometry, Trans. of the Royal Soc. of Canada., 48, 11-26, (1954).
72. Halperin, I., On the coordinatization theory of J. von Neumann, Can. Jour. Math., 7, 432-444, (1955).
73. Halperin, I., The von Neumann coordinatization theory for complemented modular lattices, Acta. Sci. Math. Szeged, 20, 203-249, (1956).
74. Halperin, I., Kontinuierliche Geometrien, Bull. Amer. Math. Soc., 64, 386-390, (1958).
75. Halperin, I., On the construction of coordinates for non-Desarguesian projective planes, Proc. of the Royal Netherlands Academy, 61, 142-161, (1958).
76. Halperin, I., A simplified proof of von Neumann's coordinatization theorem, Proc. National Acad. Scie. USA, 47, 1495-1498, (1961).
77. Halperin, I., Complemented modular lattices, Lattice Theory, Proc. Symp. in Pure Math. AMS, 2, 51-64, (1961).
78. Halperin, I., Complemented modular lattices, Algeb. and Topol. Foundations of Geom. Proc. Colloq. Utrecht, 47-55, (1962).
79. Halperin, I. and Amemiya, I., Complemented modular lattices derived from non-associative rings, Acta. Sci. Math. Szeged, 20, 182-201, (1959).
80. Halperin, I., and Amemiya, I., Complemented modular lattices, Can. Jour. Math., 2, 481-520, (1959).
81. Halperin, I., and Amemiya, I., Coordinatization of complemented modular lattices, Proc. Royal Netherlands Acad., 62, 70-78, (1959).
82. Hermes, H., Einfuhrung in die Verbandstheorie, Berlin-Gottingen-Geidelberg, (1955).
83. Herrmann, C., A parameter for subdirectly irreducible modular lattices with 4 generators, to appear Acta. Sci. Math.
84. Herrmann, C., Rahmen und erzeugende Quadrupel in modularen Verbanden, preprint.
85. Herrmann, C., On the equational theory of submodule lattices, Proc. Houston Lattice Theory Conference, 105-118, (1973).
86. Herrmann, C., S-Verklerte Summen von Verbanden, Math. Z., 130, 225-274, (1973).
87. Herrmann, C., Concerning MM Gluhovs paper on the word problem for free modular lattice, Alg. Univ., 5, 445, (1975).
88. Herrmann, C., On modular lattices generated by two complemented pairs, Houston Jour. Math., 2, 513-523, (1976).
89. Herrmann, C., On a condition sufficient for the distributivity of lattices of linear subspaces, Archiv De Math., 33, 235-238, (1979).
90. Herrmann, C., A finitely generated modular ortholattice, Can. Math. Bull., to appear (1980).
91. Herrmann, C., On the Arithmetic of projective coordinate systems, Trans. Amer. Math. Soc., (accepted).
92. Herrmann, C., On elementary Arguesian lattices with four generators, preprint Darmstadt, 1981.
93. Herrmann, C., On the word problem for modular lattices with four generators, preprint Darmstadt, 1982.
94. Herrmann, C. and Huhn, A., Lattices of normal subgroups generated by frames, Colloq. Math. Society Janos Bolyai, 14, 97-136, (1975).
95. Herrmann, C. and Huhn, A., Zum Begriff der Charakteristik modularer Verbande, Math. Z., 144, 185-194, (1975).
96. Herrmann, C. and Huhn, A., Zum Wortproblem fur Freie Untermodulverbande, Archiv Math., 26, 449-453, (1975).
97. Herrmann, C. and Kindersmann, M. and Wille, R., On modular lattices generated by 1+2+2, Alg. Univ., 5, 243-251, (1975).
98. Herrmann, C. and Poguntke, W., The class of sublattices of normal subgroup lattices is not elementary, Alg. Univ., 4, 280-286, (1974).
99. Herrmann, C. and Ringel, C. and Wille, R., On modular lattices with four generators, Notices Amer. Math. Soc., 20, A-418, (1973).
100. Hoffman, A., On the foundations of projective and affine geometry, Trans. Amer.

Math. Soc., 71, 218-242, (1951).
101. Hong, D., Covering relations among lattice varieties, Pacif Jour. Math., 40, 575-603, (1972).
102. Huhn, A., Schwach distributive Verbande I, Acta. Sci. Math., 33, 297-305, (1972).
103. Huhn, A., Weakly distributive lattices, Ph.D. Thesis (1972).
104. Huhn, A., Two notes on n-distributive lattices, Colloq. Math. Soc. Janos Bolyai, (1974).
105. Huhn, A., n-distributivity and some questions of the equational theory of lattices, Coll. Math. Soc. Janos Bolyai, (1975).
106. Huhn, A., On automorphisms of a finitely presented modular lattice, Alg. Univ., 5, 65-71, (1975).
107. Huhn, A., Schwach distributive Verbande II, Acta, Sci. Math, (1977).
108. Hutchinson, G., Modular lattices and abelian categories, J. Alg., 19, 156-184, (1971).
109. Hutchinson, G., Recursively unsolvable word problems of modular lattices, J. Alg., 26, 385-399, (1973).
110. Hutchinson, G., On the representation of lattices by modules, Trans. Amer. Math. Soc., 209, 311-351, (1975).
111. Hutchinson, G., Embedding and unsolvability theorems for modular lattices, Alg. Univ., 7, 47-84, (1977).
112. Hutchinson, G. and Czedli, G., A test for identities satisfied in lattices of submodules, Alg. Univ., 8, 269-309, (1978).
113. Inaba, E., On primary lattices, J. Fac. Sci. Hokkaido Univ., 11, 39-107, (1948).
114. Inaba, E., Some remarks on primary lattices, Nat. Sci. Report of the Ochanomiz Univ., (1951).
115. Jónsson, B., On the representation of lattices, Math. Scand., 1, 193-206, (1953).
116. Jónsson, B., Modular lattices and Desargues theorem, Math. Scand., 2, 295-314, (1954).
117. Jónsson, B., Representations of lattices II, Bull. Amer. Math. Soc., 60, (1954).
118. Jónsson, B., Extensions of von Neumann's coordinatization theorem, Proc. Symp. Pure Math., Vol. II, (1959).
119. Jónsson, B., Arguesian lattices of dimension n<=4, Math. Scand., 7, 133-145, (1959).
120. Jónsson, B., Lattice theoretic approach to projective and affine geometry, Studies in Logic, Amsterdam, (1959).
121. Jónsson, B., Representations of modular lattices and relation algebras, Trans. Amer. Math. Soc., 92, 449-464, (1959).
122. Jónsson, B., Algebras whose congruence lattices are distributive, Math. Scand., 21, 110-121, (1967).
123. Jónsson, B., Equational classes of lattices, Math. Scand., 22, 187-196, (1968).
124. Jónsson, B., The amalgamation property in varieties of modular lattices, Notices Amer. Math. Soc., 18, 400, (1971).
125. Jónsson, B., The class of Arguesian lattices is selfdual, Alg. Univ., 2, 396, (1972).
126. Jónsson, B., Varieties of algebras and their congruence varieties, Proc. Int. Congr. of Math., 315-320, (1974).
127. Jónsson, B., Congruence Varieties, Alg. Univ., (1980).
128. Jónsson, B. and Monk, G., Representation of primary Arguesian lattices, Pacific J. Math., 30, 95-139, (1969).
129. Kleiner, M., On exact representations of partially ordered sets of finite type, Zap. Nauc. Sem. Leningradskooo Otoela (Russian), 24, 42-59, (1972).
130. Klingenberg, W., Projektive und affine Ebenen mit Nachbarelementen, Math. Z., 60, 384-406, (1954).
131. Klingenberg, W., Desarguessche Ebenen mit Nachbarelementen, Abh. Math. Sem. Univ. Hamburg, 20, 97-111, (1955).
132. Kothe, G., Die Theorie der Verbande, J-ber Deutsch Math. Verein, (1937).
133. Lipshitz, L., The undecidability for the word problems of modular lattices and projective geometries, Trans. Amer. Math. Soc., 193, 171-180, (1974).
134. Luck, H., Projektive Hjelmslevraume, Crelles J. Fur Math., 243, 121-158, (1970).
135. Maeda, F., Kontinuierlishe Geometrien, Springer-Verlag, Berlin, (1958).
136. Makkai, M. and McNulty, G., Universal horn systems for lattices of submodules, Alg. Univ., 7, 25-31, (1977).

137. Menger, K., New foundations of projective and affine geometry, Ann. of Math., 37, 456-482, (1936).
138. Mitschke, A. and Wille, R., Freie modulare Verbande FM(DM3), Proc. Lattice Theory Conf. Houston, 383-396, (1973).
139. Mitschke, A. and Wille, R., Finite distributive lattices projective in the class of modular lattices, Alg. Univ., 6, 383-393, (1976).
140. Monk, G., Desargues' law and the representation of primary lattices, Pacific Jour. Math., 30, 175-186, (1969).
141. Nazarova, L., Representation of a tetrad, Izvakad Nauk SSSR Ser. Math., 31, 1361-1378, (1967).
142. Ore, O., Structures and group theory I, Duke Math. Jour., 3, 149-173, (1937).
143. Ore, O., Structures and group theory II, Duke Math. Jour., 4 247-269, (1938).
144. Pickert, G., Projektive Ebenen, Berlin-Gottingen-Heidelberg Springer, (1955).
145. Poguntke, W., Zerlegung von S-verbanden, Math. Z., 142, 47-65, (1975).
146. Rado, F., Non-injective collineations on some sets in Desarguean projective planes, Aequat. Math., (1970).
147. Rado, R., A theorem on abelian groups, Jour. London Math. Soc., 22, 219-226, (1947).
148. Rolf, H., The free modular lattice FM(2+2+2) is infinite, Proc. Amer. Math. Soc., 17, 960-961, (1966).
149. Sauer, G. and Seibert, W. and Wille, R., On free modular lattices over partial lattices with four generators, Proc. Conf. Lattice Theory, 332-382, (1973).
150. Schmidt, E., On finitely generated simple modular lattices, Periodica Math. Hung., 6, 213-216, (1975).
151. Schutzenberger, M., Sur certains axiomes de la theorie des structures, C. R.
152. Schutzenberger, M., Construction du treillis modulaire engendre par 2 elements et une chaine fini, C. R. Acad. Sci. Paris, 235, 926-928, (1952).
153. Skornyakov, L., Complemented Modular Lattices and Regular Rings, Oliver and Boyd, (1964).
154. Suzuki, M., Structure of a Group and the Structure of its Lattice of Subgroups, Berlin, Springer, (1967).
155. Szasz, G., Einfuhrung in die Verbandstheorie, Akademiai Kiado, Budapest, (1962).
156. Takeuchi, K., On free modular lattices, Jap. Jour. Math., 21, 53-65, (1951).
157. Takeuchi, K., On free modular lattices II, Tohoku Math. Jour., 11, 1-12, (1959).
158. Thrall, R. and Duncan, D., A note on free modular lattices, Amer. Jour. Math., 75, 627-632, (1953).
159. Veblen, O. and Young, W., Projective Geometry, Ginn and Company, Boston, 2 Volumes, (1910).
160. von Neumann, J., Algebraic theory of continuous geometries, Proc. Nat. Acad. Sci., 23, 16-22, (1937).
161. von Neumann, J., Continuous Geometry, Princeton Univ. Press, Princeton, N.J., (1960).
162. Wallmman, H., Lattices and topological spaces, Ann. Math., 39, 112-126, (1938).
163. Weller, H., Zusammenhang zwischen Eigenschaften eines Ringes R und Eigenschaften des Verbanden $L(R^3)$, Dissertation, Gießen, (1975).
164. Wille, R., Variety invariants for modular lattices, Can. Jour. Math., 21, 279-283, (1969).
165. Wille, R., Primitive Lange und primitive Weite bei modularen Verbande, Math. Z., 108, 129-136, (1969).
166. Wille, R., Finite Projective Planes and Equational Classes of Modular Lattices, Atta Coll. Intern. Teorie Combinatorie Roma, (1973).
167. Wille, R., On modular lattices generated by finite chains, Alg. Univ., 3, 131-138, (1973).
168. Wille, R., On modular lattices of order dimension two, Proc. Amer. Math. Soc., 43, 287-292, (1974).

SUBDIRECTLY IRREDUCIBLE ALGEBRAS IN MODULAR VARIETIES

Ralph Freese

In a distributive variety generated by a single finite algebra A, every subdirectly irreducible algebra lies in HS(A) by Jónsson's Theorem. In this paper we define the concept of similarity between subdirectly irreducible algebras and show that if A is finite and V(A) is modular then every subdirectly irreducible algebra in V(A) is similar to one in HS(A). The *monolith* μ of a subdirectly irreducible algebra B is the unique atom of Con(B). If μ is nonabelian (definitions below) then the similarity class of B contains only B. Suppose μ is abelian and let α be the *annihilator* of μ (the largest congruence with $[\alpha,\mu] = 0$). Then each μ-block is in a natural way an abelian group. Moreover, by a result of Gumm [5], μ-blocks which lie in the same α-block determine isomorphic groups. Roughly, B is similar to B' (with abelian monolith μ' and annihilator α') if $B/\alpha \cong B'/\alpha'$, the abelian groups inside of corresponding α and α' blocks are isomorphic, and a certain natural action of B/α on these groups is preserved under these isomorphisms. The correspǒnding concept for groups is given in [8].

In the first section we review those parts of the commutator theory which we will need. The second section gives a useful lattice theoretic characterization of similarity and uses it to prove the main result. In the third section we investigate the relation between similarity and the Gumm-Herrmann concept of isotopy. We also show that if θ is a minimal abelian congruence then there is a division ring D such that each θ-block is a vector space over D and the unary algebraic functions of the algebra act densely on these vector spaces. In particular if A is finite and θ is a minimal abelian congruence then each block has prime power order for a fixed prime. The fifth section gives another characterization of similarity.

The author would like to thank Ralph McKenzie for several helpful comments and the NSF for support.

1. PRELIMINARIES. We let V denote a modular variety; i.e., a variety of algebras all of whose congruence lattices are modular. We use $+$ and juxtaposition for the lattice operations. The congruence lattices of members of V have a third operation, the commutator, denote $[\alpha,\beta]$ (see [4] or [5] for a detailed development). The basic properties are

$$[\alpha,\beta] \le \alpha\beta$$

$$[\alpha,\beta] = [\beta,\alpha]$$

$$[\alpha,\bigvee \beta_i] = \bigvee[\alpha,\beta_i]$$

Moreover if f is a homomorphism from A onto B with kernel θ then for $\alpha,\beta \in \mathrm{Con}(A)$

$$[\alpha,\beta] + \theta = f^{-1}[f(\alpha+\theta),f(\beta+\theta)].$$

Using the complete additivity, we define a *residuation* operation $(\alpha : \beta)$, $\alpha,\beta \in \mathrm{Con}(A)$ to be the largest θ with $[\theta,\beta] \le \alpha$.

The commutator can be defined by the following term condition: $[\alpha,\beta]$ is the least congruence γ such that if t is an n+m-ary term $\underset{\sim}{a}^1,\underset{\sim}{a}^2 \in A^n$, $\underset{\sim}{b}^1,\underset{\sim}{b}^2 \in A^m$ and $a_i^1 \;\alpha\; a_i^2$, $i = 1,\dots,n$ and $b_j^1 \;\beta\; b_j^2$, $j = 1,\dots,m$, and $t(\underset{\sim}{a}^1,\underset{\sim}{b}^1) \;\gamma\; t(\underset{\sim}{a}^1,\underset{\sim}{b}^2)$ then $t(\underset{\sim}{a}^2,\underset{\sim}{b}^1) \;\gamma\; t(\underset{\sim}{a}^2,\underset{\sim}{b}^2)$.

By a result of Herrmann and Gumm V has a ternary term $d(x,y,z)$ satisfying

$$d(x,x,z) = z$$

$$d(x,z,z)[\alpha,\alpha]x \quad \text{if} \quad x \;\alpha\; z$$

([4] or [5]). If $a \in A \in V$ and $\theta \in \mathrm{Con}(A)$ we let a/θ denote the block of θ containing a. If θ is an abelian congruence, i.e., $[\theta,\theta] = 0$, then the operations $x + y = d(x,a,y)$, $-x = d(a,x,a)$ for $x,y \in a/\theta$ make a/θ into an abelian group with a as null element. We also require a useful result of Gumm [5].

THEOREM 1.1. *Let* $\alpha \ge \beta$ *in* $\mathrm{Con}(A)$. *The following are necessary and sufficient conditions in order that* $[\alpha,\beta] = 0$. *For any term function* $s(x_1,\dots,x_n)$ *and elements* $x_i \;\beta\; y_i \;\alpha\; z_i$, $i = 1,\dots,n$, *we have* $d(s(\underset{\sim}{x}),s(\underset{\sim}{y}),s(\underset{\sim}{z})) = s(d(x_1,y_1,z_1),\dots,d(x_n,y_n,z_n))$, *and* $x \;\beta\; y$ *implies* $d(x,y,y) = x$.

As a corollary to this theorem note that if γ is abelian γ permutes with all congruences. Indeed, since $[\gamma,\gamma] = 0$, if

$a\ \gamma\ b$ then $a = d(a,b,b)$. Hence if $a\ \gamma\ b\ \theta\ c$ then $a = d(a,b,b)\ \theta\ d(a,b,c)\ \gamma\ d(a,a,c) = c$.

If $\alpha \geq \beta$ and $\gamma \geq \delta$ in a lattice we write $\alpha/\beta \searrow \gamma/\delta$ (and also $\gamma/\delta \nearrow \alpha/\beta$) if $\alpha = \beta + \gamma$ and $\delta = \beta\gamma$. We say α/β and γ/δ are projective if they can be connected by a sequence of such transpositions.

2. SIMILARITY. Let V be a modular variety, $A \in V$, $a,a' \in A$, and θ an abelian congruence on A. Let $\mathrm{Hom}(\theta,a,a')$ be the set of all functions g from a/θ to a'/θ which have the form

$$(1)\quad g(x) = f(x,a,a';c_1,\ldots,c_n) \quad x \in a/\theta$$

where f is a term such that V satisfies the identity

$$(2)\quad f(v,v,v';y_1,\ldots,y_n) = v'.$$

This definition makes it appear that $\mathrm{Hom}(\theta,a,a')$ depends on V as well as A. To see that it does not, let $c_1,\ldots,c_n \in A$ and suppose h is a term such that

$$(2')\quad h(a,a,a';c_1,\ldots,c_n) = a'.$$

Let $f(u,v,v';y_1,\ldots,y_n) = d(h(u,v,v';y_1,\ldots,y_n),h(v,v,v';y_1,\ldots,y_n),v')$ Clearly V satisfies (2) for this f, and the properties of d give that $f(x,a,a';c_1,\ldots,c_n) = h(x,a,a';c_1,\ldots,c_n)$ for all $x \in a/\theta$. Notice that this shows that $\mathrm{Hom}(\theta,a,a')$ *is simply the set of restrictions to* a/θ *of unary algebraic functions which map* a *to* a'.

Let $\alpha = (0:\theta)$ be the annihilator of θ. The θ,α-term condition tells us g is unchanged if we replace each c_i with d_i provided $c_i\ \alpha\ d_i$, $i = 1,\ldots,n$ (for $x \in a/\theta$, of course). Thus we may think of c_i in (1) as an element of A/α. We write

$$(3)\quad g_{aa'}(x) = f(x,a,a';c_1/\alpha,\ldots,c_n/\alpha) \quad x \in a/\theta.$$

We have added the subscripts a and a' to emphasize the domain and range of g.

Since θ is abelian, a/θ is an abelian group with a as zero element and $x + y = d(x,a,y)$. We denote this group $M(\theta,a)$. By Theorem 1.1 each $g \in \mathrm{Hom}(\theta;a,a')$ is a group homomorphism of $M(\theta,a)$ to $M(\theta,a')$.

Let B be another algebra in V with abelian congruence ψ and and let $\beta = (0:\psi)$. Then we define θ in A to be *similar* to ψ

in B if several things occur. First there is an isomorphism

(4) $\sigma : A/\alpha \rightarrowtail\!\!\twoheadrightarrow B/\beta$.

Moreover, for each $a \in A$ and $b \in B$ such that $\sigma(a/\alpha) = b/\beta$ there is an isomorphism

(5) $\tau_{ab} : M(\theta,a) \rightarrowtail\!\!\twoheadrightarrow M(\psi,b)$

satisfying: if $a' \in A$ and $b' \in B$ and $\sigma(a'/\alpha) = b'/\beta$ and $g_{aa'}$ is as in (3) then

(6) $\tau_{a'b'}g_{aa'}(x) = g^{\sigma}_{bb'}\tau_{ab}(x)$ for $x \in a/\theta$

where $g^{\sigma}_{bb'}$ is defined by

(7) $g^{\sigma}_{bb'}(x) = f(x,b,b';\sigma(c_1/\sigma),\ldots,\sigma(c_n/\alpha))$.

Roughly this says that A/α is isomorphic to B/β via σ and that the group determined by a θ-block, $M(\theta,a)$ is isomorphic to the group $M(\psi,b)$ provided a and b correspond under σ. Moreover, (3) defines an "action" between the θ-blocks. Condition (6) says that the isomorphism between $M(\theta,a)$ and $M(\psi,b)$ preserves this action.

Now suppose A and B are subdirectly irreducible with monoliths μ and ν, respectively. Let $\alpha = (0 : \mu)$ and $\beta = (0 : \nu)$. We say that A is *similar* to B and write $A \sim B$ if $A \cong B$ or both μ and ν are abelian and μ in A is similar to ν in B, as defined above. The next theorem gives a useful characterization of similarity. If θ is a completely meet irreducible congruence we let θ^* denote its upper cover.

THEOREM 2.1. *Let* A *and* B *be subdirectly irreducible algebras in* V. *Then* $A \sim B$ *if and only if there is an algebra* $C \in V$ *and* $\gamma,\delta,\eta,\varepsilon \in \mathrm{Con}(C)$, *with* η *and* ε *completely meet irreducible, such that* $A \cong C/\eta$, $B \cong C/\varepsilon$, *and* $\eta^*/\eta \searrow \gamma/\delta \nearrow \varepsilon^*/\varepsilon$. *Moreover, if* $A \sim B$ *then such a* C *can be found among the subalgebras of* $A \times B$ *with* η *and* ε *as the projective kernels.*

Proof. Let μ and ν be the monoliths of A and B and α and β their annihilators. Suppose C is as described in the theorem. If we replace γ with $\gamma' = \gamma + \eta\varepsilon$ and δ with $\delta' = \eta\varepsilon$, we have $\eta^*/\eta \searrow \gamma'/\delta' \nearrow \varepsilon^*/\varepsilon$. Thus we may assume $\gamma \geq \eta\varepsilon$ and $\delta = \eta\varepsilon$. Moreover, by replacing C with C/δ, we may assume $\delta = 0$.

Let $\phi = (\eta : \eta^*)$ and $\phi' = (\varepsilon : \varepsilon^*)$. Then $[\phi,\varepsilon^*] = [\phi,\varepsilon+\gamma] = [\phi,\varepsilon] + [\phi,\gamma] \leq \varepsilon + [\phi,\eta^*]\gamma \leq \varepsilon + \eta\gamma = \varepsilon$. Hence by definition $\phi \leq \phi'$. So by symmetry, $\phi = \phi'$. It follows that $A/\alpha \cong C/\phi \cong B/\beta$. There is no loss of generality in assuming $A = C/\eta$ and $B = C/\varepsilon$. Now $\phi \geq \eta$

and $\phi \geq \varepsilon$ so $\phi \geq \eta + \varepsilon$. Thus $\phi \geq \eta^*$ unless $\eta \geq \varepsilon$. Now if the latter holds then, in fact, $\eta = \varepsilon$, and hence $A = B$, since $\eta > \varepsilon$ implies $\eta \geq \varepsilon^* \geq \gamma$, contradicting $\gamma + \eta = \eta^*$ (which is a consequence of the projectivity). Thus we may assume $\phi \geq \eta^*$ and $\phi \geq \varepsilon^*$. Hence $[\eta^*,\eta^*] \leq \eta$, so μ is an abelian congruence on A. Similarly ν is abelian. Now $[\gamma,\gamma] \leq [\eta^*,\eta^*][\varepsilon^*,\varepsilon^*] \leq \eta\varepsilon = 0$. So γ is an abelian congruence and hence permutes with all congruences of C. For $a \in C$, let $M(\eta^*/\eta,a)$ be the abelian group whose elements are $\{x/\eta : x\,\eta^*\,a\}$ (which is isomorphic to $M(\mu,a/\eta)$). For $a \in C$ define $\tau_a : a/\eta^* \to a/\varepsilon^*$ as follows. If $x \in a/\eta^*$ then since $\eta^* = \eta + \gamma = \eta \circ \gamma$ there is a $y \in C$ with $a\ \gamma\ y\ \eta\ x$. Since $\eta\gamma = 0$, y is unique. Set $\tau_a(x) = y$. Since $\gamma \leq \varepsilon^*$, $y \in a/\varepsilon^*$. Let $\overline{\tau}_a : M(\eta^*/\eta,a) \to M(\varepsilon^*/\varepsilon,a)$ be defined by $\overline{\tau}_a(x/\eta) = \tau_a(x)/\varepsilon$. It is easy to check that if $x\ \eta\ x'$ then $\tau_a(x)\ \gamma\ \tau_a(x')$, from which it follows that $\overline{\tau}_a$ is well-defined.

To see that $\overline{\tau}_a$ is a group homomorphism, suppose, for some $x,x' \in a/\eta^*$, $\tau_a(x) = y$ and $\tau_a(x') = y'$. Then $a\ \gamma\ y\ \eta\ x$ and $a\ \gamma\ y'\ \eta\ x'$. This implies $a = d(a,a,a)\ \gamma\ d(y,a,y')\ \eta\ d(x,a,x')$. Hence $\tau_a(d(x,a,x')) = d(y,a,y')$. Thus $\tau_a(x+x') = \tau_a(x) + \tau_a(x')$, and it follows that $\overline{\tau}_a$ preserves $+$. To see that $\overline{\tau}_a$ is one to one, suppose $\overline{\tau}_a(x/\eta) = \overline{\tau}_a(x'/\eta)$. Let $y = \tau_a(x)$, $y' = \tau_a(x')$. Then we have $y\ \varepsilon\ y'$ and $a\ \gamma\ y\ \eta\ x$ and $a\ \gamma\ y'\ \eta\ x'$. Hence $y\ \gamma\cap\varepsilon\ y'$ so $y = y'$ and hence $x\ \eta\ x'$.

If $y \in a/\varepsilon^*$ then there is an x with $a\ \gamma\ x\ \varepsilon\ y$. Clearly $a\ \gamma\ x\ \eta\ x$, so $\overline{\tau}_a(x/\eta) = x/\varepsilon = y/\varepsilon$. Thus $\overline{\tau}_a$ is onto.

Remark. This proof shows that in general, if we have a projectivity $\alpha/\beta \searrow \gamma/\delta$ and either $[\alpha,\alpha] \leq \beta$ or $[\gamma,\gamma] \leq \delta$, then the other one holds and in this case the groups $M(\alpha/\beta,a)$ and $M(\gamma/\delta,a)$ are isomorphic. This may be thought of as a version of the second isomorphism theorem.

Now suppose f is a term satisfying (2). Then

(8) $\tau_{a'}f(x,a,a';\underset{\sim}{c}) = f(\tau_a x,a,a';\underset{\sim}{c}) \qquad x \in a/\eta^*$

since $a' = f(a,a,a';\underset{\sim}{c})\ \gamma\ f(\tau_a x,a,a',\underset{\sim}{c})\ \eta\ f(x,a,a';\underset{\sim}{c})$.

Now suppose $a,b \in C$ and $a\ \phi\ b$. Define $\tau_{ab} : a/\eta^* \to b/\varepsilon^*$ by $\tau_{ab}(x) = d(\tau_a(x),a,b)$ for $x \in a/\eta^*$. Let $\overline{\tau}_{ab} : M(\eta^*/\eta,a) \to M(\varepsilon^*/\varepsilon,b)$ be defined by $\overline{\tau}_{ab}(x/\eta) = \tau_{ab}(x)/\varepsilon$. It is easy to see that $\overline{\tau}_{ab}$ is well-defined. By Gumm's result (see Proposition 7.2 of [4]) the map $z \mapsto d(z,a,b)$ induces a group isomorphism of $M(\varepsilon^*/\varepsilon,a)$ onto $M(\varepsilon^*/\varepsilon,b)$. It follows that $\bar{\tau}_{ab}$ is an isomorphism of $M(\eta^*/\eta,a)$ onto $M(\varepsilon^*/\varepsilon,b)$. Suppose now that f is a term satisfying (2) and that $a',b' \in C$ with $a' \phi b'$. Note $[\gamma,\phi] \leq [\eta^*,\phi][\varepsilon^*,\phi] \leq \eta\varepsilon = 0$. Hence by Theorem 1.1 and (8) we have for $x \in a/\eta^*$

$$\begin{aligned}
&f(\tau_{ab}(x),b,b';\underset{\sim}{c}) \\
&\quad = f(d(\tau_a(x),a,b),d(a,a,b),d(a',a',b');d(c_1,c_1,c_1),\ldots,d(c_n,c_n,c_n)) \\
&\quad = d(f(\tau_a(x),a,a';\underset{\sim}{c}),f(a,a,a';\underset{\sim}{c}),f(b,b,b';\underset{\sim}{c})) \\
&\quad = d(f(\tau_a(x),a,a';\underset{\sim}{c}),a',b') \\
&\quad = d(\tau_{a'}f(x,a,a';\underset{\sim}{c}),a',b') \\
&\quad = \tau_{a'b'}f(x,a,a';\underset{\sim}{c}).
\end{aligned}$$

It follows that the isomorphism $\bar{\tau}_{ab}$ has the desired properties and thus $A \sim B$.

Conversely suppose $A \sim B$. The case $A \cong B$ is easy to handle. Thus we assume μ and ν are abelian and thus $\alpha \geq \mu$ and $\beta \geq \nu$. Let $D = A/\alpha$ and let h be the natural map $A \to D$ and let $k : B \to D$ with $\ker k = \beta$. Define $C = \{(x,y) \in A \times B : h(x) = k(y)\}$. Let $\gamma \in \mathrm{Con}(C)$ be defined by $(a,b)\ \gamma\ (a',b')$ if $a\ \mu\ a'$, $b\ \nu\ b'$, and $\tau_{ab}(a') = b'$. Clearly γ is reflexive. To see symmetry suppose $(a,b)\ \gamma\ (a',b')$. Let $g_{aa'}(x) = g(x) = d(a,x,a')$ and note $g \in \mathrm{Hom}(\mu,a,a')$ since $a\ \mu\ a'$, $g(a') = d(a,a',a') = a$. Hence by (6) $\tau_{a'b'}g_{aa'}(a') = g_{bb'}\tau_{ab}(a')$. Thus $\tau_{a'b'}(a) = g_{bb'}(b') = d(b,b',b') = b$, proving symmetry.

Suppose $(a,b)\ \gamma\ (a',b')\ \gamma\ (a'',b'')$. Then a, a', and a'' are μ related and b, b', and b'' are ν related. Also $\tau_{ab}(a') = b'$, $\tau_{a'b'}(a'') = b''$, and $\tau_{a'b'}(a) = b$ (by symmetry). Let $g_{a'a}(x) = d(a,x,a')$. It is easy to see that $a'' = g_{a'a}(d(a,a'',a'))$ and $b'' = g_{b'b}(d(b,b'',b'))$. Thus

$$\begin{aligned}
\tau_{ab}(a'') &= \tau_{ab}g_{a'a}d(a,a'',a') \\
&= g_{b'b}\tau_{a'b'}d(a,a'',a') \\
&= g_{b'b}d(b,b'',b') \\
&= b''.
\end{aligned}$$

Suppose $(a,b)\ \gamma\ (a',b')$ and $f(x;y_1,\ldots,y_n)$ is a term. Then $(x,y) \mapsto (f(x;c_1,\ldots,c_n),f(y;d_1,\ldots,d_n))$ is a unary algebraic function on C provided $(c_i,d_i) \in C$; i.e., $h(c_i) = k(d_i)$. As was pointed out earlier $f(x;\underset{\sim}{c}) \in \mathrm{Hom}(\mu,a,f(a;\underset{\sim}{c}))$ and $f(y;\underset{\sim}{d}) \in \mathrm{Hom}(\nu,b,f(b;\underset{\sim}{d}))$. Then by (6)

$$\tau_{f(a;\underset{\sim}{c})f(b;d)}f(x;\underset{\sim}{c}) = f(\tau_{ab}(x);\underset{\sim}{d}).$$

Now setting $x = a'$ we see that γ respects the unary algebraic functions. Hence γ is a congruence.

Let η and ε be the kernels of the natural maps of C onto A and C onto B. Suppose $(a,b)\ \gamma\eta\ (a',b')$. Then $a = a'$; so $b' = \tau_{ab}(a') = \tau_{ab}(a) = b$; amd thus $\gamma\eta = 0$. Clearly $\gamma \le \eta^*$ and $\eta \prec \eta^*$. Hence $\eta + \gamma = \eta^*$. Thus $\eta^*/\eta \searrow \gamma/0$. Similarly $\varepsilon^*/\varepsilon \searrow \gamma/0$, completing the proof.

The next theorem shows that any subdirectly irreducible algebra in V with abelian monolith is similar to one whose monolith equals its annihilator.

THEOREM 2.2. *Let* B *be a subdirectly irreducible member of* V *with abelian monolith. Then there is a subdirectly irreducible algebra* $B' \in V$ *with* $B \sim B'$ *and* $(0 : \mu') = \mu'$ *in* Con(B').

<u>Proof</u>. Let $B(\mu) = \{(a_0,a_1) \in B \times B : a_0\ \mu\ a_1\}$, i.e., μ thought of as a subalgebra of $B \times B$. If $\theta \in \mathrm{Con}(B)$ let $\theta_i \in \mathrm{Con}(B(\mu))$, $i = 0,1$, be defined by $(a_0,a_1)\ \theta_i\ (b_0,b_1)$ if $a_i\ \theta\ b_i$. Let η_i, $i = 0,1$, be the kernels of the projection maps, i.e., $\eta_i = 0_i$. Let $\alpha = (0 : \mu) \in \mathrm{Con}(B)$. It is easy to check that $\mu_0 = \mu_1$ and $\alpha_0 = \alpha_1$ (since $\alpha \ge \mu$) and $\eta_0 + \eta_1 = \mu_0 = \mu_1$. Let $\Delta = \Delta_{\mu,\alpha} \in \mathrm{Con}(B(\mu))$ be the congruence generated by the set of pairs $\{((x,x),(y,y)) : x\ \alpha\ y\}$. If $(a_0\ a_1)\ \alpha_0\ (b_0\ b_1)$ then $a_0\ \alpha\ b_0$. Hence $(a_0\ a_1)\ \eta_0\ (a_0\ a_0)\ \Delta\ (b_0\ b_0)\ \eta_0\ (b_0\ b_1)$. Thus $\eta_0 + \Delta = \alpha_0 = \alpha_1$. Similarly $\eta_1 + \Delta = \alpha_0 = \alpha_1$. Suppose $(a_0\ a_1)\ \Delta\cap\eta_1\ (b_0\ b_1)$. Then $a_1 = b_1$ and it follows from Theorem 4.11 (iv) of [4] $a_0\ [\mu,\alpha]\ b_0$, i.e., $a_0 = b_0$. Thus $\Delta\eta_1 = 0 = \Delta\eta_0$. These facts show

(9) $\alpha_0/\Delta \searrow \eta_1/0 \nearrow \mu_0/\eta_0$.

Let $B' = B(\mu)/\Delta$. To see that B' is subdirectly irreducible we need to show that Δ is completely meet irreducible. Suppose $\beta > \Delta$ in $\mathrm{Con}(B(\mu))$ and that $\beta \not\le \alpha_0 = \alpha_1$. Then $\beta \not\ge \eta_1$ since otherwise $\beta \ge \Delta + \eta_1 = \alpha_0 = \alpha_1$. Hence $\beta\eta_1 = 0$ since $\eta_1 \succ 0$ by (9). Thus $[\beta,\mu_0] = [\beta,\eta_0 + \eta_1] \le \eta_0 + \beta\eta_1 = \eta_0$. Thus $[\alpha_0 + \beta,\mu_0] \le \eta_0$. By the definition of α in Con(B) this means $\beta \le \alpha_0$, which implies $\beta = \alpha_0$, a contradiction. Thus B' is subdirectly irreducible.

Since $B(\mu)/\eta_0 \cong B$, the projectivity (9) and the previous theorem imply B is similar to B'

COROLLARY 2.3. Suppose $V = V(A)$ where A is finite. Then every subdirectly irreducible algebra in V is similar to a finite subdirectly irreducible algebra in V.

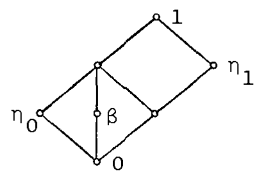
Proof. Let $B \in V$ be subdirectly irreducible. If the monolith μ of B is nonabelian, then $B \in HS(A)$ by the Generalized Jonsson Theorem (see [2]). Thus by the last theorem we may assume $(0 : \mu) = \mu$. So by the Generalized Jonsson Theorem $B/\mu \in HS(A)$. Hence $|B/\mu| \leq |A|$. By Theorem 10.5 of [4] each μ-block contains at most $|A|$ elements. Hence $|B| \leq |A|^2$.

THEOREM 2.4. *If* A *is finite then every subdirectly irreducible algebra in* $V(A)$ *is similar to a subdirectly irreducible algebra in* $HS(A)$.

Proof. Let $B \in V(A)$ be subdirectly irreducible. By the above corollary we may assume B is finite. Thus $B \cong C/\theta$, for some congruence θ, where C is a subdirect product of subdirectly irreducible algebras $A_0, \ldots, A_{k-1} \in HS(A)$. Let $\eta_0, \ldots, \eta_{k-1} \in Con(C)$ be the projection kernels. Since C is finite we may assume that if $\theta_0, \ldots, \theta_{m-1} \in Con(C)$ satisfy (1) $\theta \geq \bigwedge \theta_i$ (2) for each i there is a j with $\theta_i \geq \eta_j$, then $\{\eta_0, \ldots, \eta_{k-1}\} \subseteq \{\theta_0, \ldots, \theta_{m-1}\}$. Now let $\eta_i' = \bigwedge_{j \neq i} \eta_j$. If $\theta\eta_i' \neq 0$, then we can replace η_i with $\eta_i + \theta\eta_i'$, violating the above. Thus $\theta\eta_i' = 0$. Let θ^* be the unique congruence covering θ. Since $\theta \geq \eta_i'$ would violate the condition above, $\theta^* \leq \theta + \eta_i'$, so $\theta^* + \eta_i' = \theta + \eta_i'$. Modularity now implies that $\theta^*\eta_i' \succ 0$. From this it follows easily that $\theta^*/\theta \searrow \theta^*\eta_i'/0$. If $\eta_i \geq \theta^*\eta_i'$ then $\theta^*\eta_i' = \theta^*\eta_i'\eta_i = 0$, a contradiction. Thus since $\theta^*\eta_i' \succ 0$, $\eta_i + \theta^*\eta_i' = \eta_i^*$. Hence $\theta^*/\theta \searrow \theta^*\eta_i'/0 \nearrow \eta_i^*/\eta_i$. Thus we have $B \sim A_i$ for each i.

3. ISOTOPY. Gumm and Herrmann called algebras A and B in V *isotopic* if there is an algebra $C \in V$ with $A \times C \cong B \times C$ via an isomorphism which commutes with the second projection (i.e., one of the form $(a,c) \mapsto (b,c)$). They showed that A is isotopic to B if and only if there is a $C \in V$ a congruence β on $A \times C$ with $(A \times C)/\beta \cong B$ and β a complement of the second projection kernel η_1. In this situation the congruence lattice of $A \times C$ must contain

a homomorphic image of the following lattice.



Combining this lattice theoretic characterization with Theorem 2.1 we have the following.

THEOREM 3.1. *Let* A *and* B *be subdirectly irreducible algebras in* V. *If* A *is isotopic to* B *then* A *is similar to* B. *If* A *and* B *are simple, then* A *is isotopic to* B *if and only if* A *is similar to* B.

4. MINIMAL ABELIAN CONGRUENCES. Now we examine the sets $\mathrm{Hom}(\theta,a,a')$ for θ an abelian congruence. We give $\mathrm{Hom}(\theta,a,a')$ an abelain group structure by defining $g + h$, for $g,h \in \mathrm{Hom}(\theta,a,a')$ to be the function $d(g(x),a',h(x))$, $x \in a/\theta$; $-g$ is the function $d(a',g(x),a')$, and the function $x \mapsto a'$ is the zero. If we recall that when x, y, and z are all in the same θ-block then $d(x,y,z) = x - y + z$ for an abelian group structure on this block, it is easy to verify that $\mathrm{Hom}(\theta,a,a')$ is an abelian group. If $g \in \mathrm{Hom}(\theta,a,a')$, $h \in \mathrm{Hom}(\theta,a',a'')$ then $h \circ g$ is defined by function composition. It is easy to see that both the left and right distributive laws hold for this multiplication. In particular, $\mathrm{Hom}(\theta,a,a)$ is a ring with 1.

Let a_i, $i \in I$, be a system of representatives for the θ-classes. We combine the $\mathrm{Hom}(\theta,a_j,a_i)$ into a matrix ring $\mathrm{Mat}(\theta)$. This consists of all I by I matrices whose (i,j)th entry lies in $\mathrm{Hom}(\theta,a_j,a_i)$ and each column has only finitely many nonzero entries. This is a ring under the usual matrix operations. Form the direct sum abelian group $\sum_{i\in I} M(\theta,a_i)$. This may be thought of as a $\mathrm{Mat}(\theta)$ module (under matrix multiplication, where we think of $\sum M(\theta,a_i)$ as column vectors).

Now consider the case $\theta \succ 0$ (and θ is abelian). It follows easily from Lemma 11 of [3] that $\sum M(\theta,a_i)$ is a simple $\mathrm{Mat}(\theta)$ module. By Schur's Lemma the endomorphism ring of this module is a division ring D and Jacobson Density Theorem says that $\mathrm{Mat}(\theta)$ acts on $\sum M(\theta,a_i)$ as a dense ring of linear transformation. Since $\mathrm{Mat}(\theta)$ includes the transformation which leaves the ith component unchanged (for i fixed) and changes all other components to zero, the subgroup $M(\theta,a_i)$ of $\sum M(\theta,a_j)$ is a D-space. It follows that $\mathrm{Hom}(\theta,a_i,a_i)$ is a dense ring of linear transformations on $M(\theta,a_i)$ and more generally $\mathrm{Hom}(\theta,a_i,a_j)$ is a dense set of linear transformations between $M(\theta,a_i)$ and $M(\theta,a_j)$.

Thus if θ is a minimal abelian congruence then there is a division ring D such that each θ-block is a vector space over D and the hom sets act densely. Note when A is finite this says there is a prime p such that each θ-block has a size p^i with i, but not p, depending on the block.

5. ANOTHER CHARACTERIZATION OF SIMILARITY. In this section we show that canonically associated with subdirectly irreducible algebra A is another subdirectly irreducible algebra $D(A)$ such that $A \sim B$ if and only if $D(A) \cong D(B)$. In fact $D(A)$ is the algebra constructed in the proof of Theorem 2.2. More precisely, if A is subdirectly irreducible with monolith μ and μ is nonabelian, let $D(A) = A$. If μ is abelian and $\alpha = (0 : \mu)$ then set $D(A) = A(\mu)/\Delta_{\mu,\alpha}$. Theorem 2.2 contains the appropriate definitions and shows that $A \sim D(A)$ and that the monolith of $D(A)$ is its own annihilator. Also note from the definition of $\Delta_{\mu,\alpha}$, $\{(x,x)/\Delta : x \in A\}$ *is a subalgebra of* $D(A)$ *which is a transversal for the monolith of* $D(A)$.

THEOREM 5.1. *Let* A *and* B *be subdirectly irreducible algebras in a modular variety. Then* $A \sim B$ *if and only if* $D(A) \cong D(B)$.

Proof. If $D(A) \cong D(B)$ then $A \sim D(A) \sim D(B) \sim B$.

Now suppose $A \sim B$. Then $D(A) \sim D(B)$. Recall the definition of α_0 and α_1 and that $\alpha_0 = \alpha_1$ in $\mathrm{Con}\, A(\mu)$. Also note that α_0/Δ is the monolith of $D(A)$. Thus $D(A)/\mu_{D(A)} \cong A(\mu)/\alpha_0$. Hence, since $D(A) \sim D(B)$, there is an isomorphism $\sigma : A(\mu)/\alpha_0 \cong B(\nu)/\beta_0$, where ν is the monolith of B and $\beta = (0 : \nu)$. If $(x,y)/\Delta \in D(A)$ then $(x,y)\, \alpha_0\, (x,x)$. Let $\sigma((x,x)/\alpha_0) = (u,v)/\beta_0 = (u,u)/\beta_0$. Now define $\rho : D(A) \to D(B)$ by

$$\rho((x,y)/\Delta) = \tau_{(x,x)/\Delta,(u,u)/\Gamma}((x,y)/\Delta)$$

where Γ is the congruence on $B(\nu)$ corresponding to Δ on $A(\mu)$, i.e., $\Gamma = \Delta_{\nu,\beta}$. If $(x,y)\,\Delta\,(x',y')$ then, since $\alpha_0 \geq \Delta$, $(x,x)\,\alpha_0\,(x',x')$; thus $x\,\alpha\,x'$. But then by the definition of Δ, $(x,x)/\Delta = (x',x')/\Delta$. It follows that ρ is well-defined. Similar arguments, combined with the fact that the τ's are isomorphisms, show that ρ is bijective.

To see that ρ is a homomorphism let $f(x_0,x_1,\ldots,x_n)$ be a term and let $(x_0,y_0)/\Delta,(c_1,d_1)/\Delta,\ldots,(c_n,d_n)/\Delta$ be elements of $D(A)$. Then $g((x_0,y_0)/\Delta) = f((x_0,y_0/\Delta),(c_1,d_1)/\Delta),\ldots,(c_n,d_n)/\Delta)$ is in $\mathrm{Hom}(\alpha_0/\Delta,(x_0,x_0)/\Delta,g((x_0,x_0)/\Delta))$. By the invariance described in section 2,

$$g((x_0,y_0)/\Delta) = f((x_0,y_0)/\Delta,(c_1,c_1)/\Delta,\ldots,(c_n,c_n)/\Delta)$$

since $(c_i,d_i)\ \alpha_0\ (c_i,c_i)$. Let $x = f(x_0,c_1,\ldots,c_n)$ and $y = f(y_0,c_1,\ldots,c_n)$; then $f((x_0,y_0)/\Delta,(c_1,c_1)/\Delta,\ldots,(c_n,c_n)/\Delta) = (x,y)/\Delta = g((x_0,y_0)/\Delta)$ and $g((x_0,x_0)/\Delta) = (x,x)/\Delta$. Hence if $\sigma((x,x)/\alpha_0) = (u,u)/\beta_0$ and $\sigma((x_0,x_0)/\alpha_0) = (u_0,u_0)/\beta_0$ then by (6)

$$\begin{aligned}
&\rho f((x_0,y_0)/\Delta,(c_1,d_1)/\Delta,\ldots,(c_n,d_n)/\Delta) \\
&\quad = \rho g((x_0,y_0)/\Delta) \\
&\quad = \tau_{(x,x)/\Delta,(u,u)/\Gamma}\, g_{(x_0,x_0)/\Delta,(x,x)/\Delta}((x_0,y_0)/\Delta) \\
&\quad = g^{\sigma}_{(u_0,u_0)/\Gamma,(u,u)/\Gamma}\, \tau_{(x_0,x_0)/\Delta,(u_0,u_0)/\Gamma}((x_0,y_0)/\Delta) \\
&\quad = g^{\sigma}\rho((x_0,y_0)/\Delta) \\
&\quad = f(\rho(x_0,y_0)/\Delta,\sigma((c_1,c_1)/\alpha_0),\ldots,\sigma((c_n,c_n)/\alpha_0)).
\end{aligned}$$

Of course, in the last expression any element of $\sigma((c_i,c_i)/\alpha_0)$ may be used. Since $\rho((c_i,d_i)/\Delta) \in \sigma((c_i,c_i)/\alpha_0)$, these values may be substituted, proving ρ is a homomorphism.

REFERENCES

1. P. Crawley and R. P. Dilworth, Algebraic Theory of Lattices, Prentice-Hall, Englewood Cliffs, NJ, 1973.
2. R. Freese, On Jónsson's theorem, Algebra Universalis, to appear.
3. R. Freese and R. McKenzie, Residually small varieties with modular congruence lattices, Trans. Amer. Math. Soc., 264(1981), 419-430.
4. R. Freese and R. McKenzie, The commutator, an overview, preprint.
5. H. P. Gumm, An easy way to the commutator in modular varieties, Arch. Math., 34(1980), 220-228.
6. H. P. Gumm and C. Herrmann, Algebras in modular varieties: Baer refinements, cancellation and isotopy, Houston J. Math., 5(1979), 503-523.
7. B. Jónsson, Algebras whose congruence lattices are distributive, Math. Scand., 21(1967), 110-121.
8. Hanna Neumann, Varieties of Groups, Springer-Verlag, Heidelberg, 1967.

A SURVEY OF VARIETIES OF LATTICE ORDERED GROUPS

W. Charles Holland

A *lattice ordered group* is both a group (which I will write multiplicatively) and a lattice in which the group translations are assumed to preserve the lattice operations: $x(y \vee z)w = (xyw) \vee (xzw)$ and dually. Such structures form a straightforward generalization of various structures encountered in analysis, such as the real numbers, function algebras, and vector lattices. In this context, a fruitful example to bear in mind is the group (under pointwise addition) and lattice (under pointwise order) of all real-valued functions on some space. From another standpoint, lattice ordered groups are closely connected with non-commutative algebra because they arise as automorphism groups of chains. More precisely, if Ω is any totally ordered set, then the group $\mathbf{A}(\Omega)$ of all order-preserving permutations of Ω becomes a lattice ordered group under the pointwise order. The main theorem of [8] states that every lattice ordered group can be embedded in $\mathbf{A}(\Omega)$ for some totally ordered set Ω.

Lattice ordered groups are of interest from the standpoint of universal algebra as algebraic objects with two operations and a rich structure, and which are less familiar than rings, though just as firmly based on classical mathematics. Much of the standard background material on lattice ordered groups is contained in any one of [1], [2], [5]; most of the material needed in this paper is also in [6].

By a *variety* of lattice ordered groups is meant the class defined by some set of equations involving (universally quanitfied) variables and the group and lattice operations. Besides the trivial varieties $\mathbf{L}$ of all lattice ordered groups, and $\mathbf{E}$ of the one-element lattice ordered groups, the most studied variety is the abelian variety $\mathbf{A}$ defined by the equation $xy = yx$. More generally, any variety of groups (defined by equations not involving the lattice operations) restricts to a variety of lattice ordered groups, and many of these are quite interesting; for example the lattice ordered groups which are nilpotent of class n have a fairly simple structure which I will say more about later. A word of warning, however: lattice ordered groups are always torsion free, so equations which force the existence of elements of finite order will not be of much interest here. In a similar fashion, one should consider varieties defined by equations not involving the group operations. This turns out to be much less interesting because every lattice ordered group is a distributive lattice, and it is well-known that distributive lattices form the smallest proper variety of lattice. Thus, an equation involving only the lattice operations will either say nothing about a lattice ordered group or will force it to be trivial. A more typical example of a variety is the *representable* variety $\mathbf{R}$ defined by the equation $(x^{-1}(y \vee e)x) \wedge (y^{-1} \vee e) = e$, where e is the identity element of the group. A classical result of Lorenzen [13] shows that $\mathbf{R}$ is the variety generated by all totally ordered groups, and consists of those lattice ordered groups which are subdirect sums of totally ordered groups. Another variety which has received much attention is the *normal valued* variety $\mathbf{N}$ defined by the law $xy \leqslant y^2x^2$ if $x,y \geqslant e$. Although in this form the law is not an equation, it is easily seen to be equivalent to the equation $(x \vee e)(y \vee e)(x \vee e)^{-2}(y \vee e)^{-2} \vee e = e$.

Just as in any type of algebra, the intersection of any collection of varieties (of lattice ordered groups) is a variety, so the set of all varieties is a complete lattice V ordered by containment. This paper is a survey of results concerning the structure of V.

Any lattice ordered group with more than one element contains an element $a > e$. Such an element must generate a subgroup isomorphic (as a group and lattice) to the integers $\mathbb{Z}$. This makes it clear that the variety generated by $\mathbb{Z}$ is the unique smallest proper variety of lattice ordered groups. Weinberg [21] proved the much less obvious fact that this minimal variety is the abelian variety $\mathbf{A}$. It is interesting to paraphrase Weinberg's result in the following way. If the lattice ordered group G satisfies the law $xy = yx$ then G satisfies every law (except those which would trivialize G).

Concerning the other end of V, J. Martinez who did much of the early work on varieties of lattice ordered groups [14], [15], [16] observed that the normal valued variety $\mathbf{N}$ is "very large." I believe his observation simply was that $\mathbf{N}$ contains all the known varieties of interest. In [9] I was able to prove Martinez correct and to obtain a sort of dual to Weinberg's result: $\mathbf{N}$ is the unique largest (proper) variety. This can be stated in paraphrased form: if G satisfies anything then G satisfies $xy \leqslant y^2x^2$ for $x,y \geqslant e$.

At this point it would be worthwhile to take a careful look at a lattice ordered group which is *not* normal valued. Consider the lattice ordered group $\mathbf{A}(\mathbb{R})$ of order-preserving permutations of the real line. Certainly there are members $a,b \in \mathbf{A}(\mathbb{R})$ with $a,b \geqslant e$ such that for the real integers $0,1,2,3,4,5,6$, $0a = 3$, $2a = 4$, $4a = 5$, $0b = 1$, $1b = 2$, and $3b = 6$. Then $0ab = 6 > 5 = 0b^2a^2$, so that $\mathbf{A}(\mathbb{R})$ is not normal valued. The important point is that $\mathbf{A}(\mathbb{R})$ acts highly transitively on $\mathbb{R}$. It can be shown in a similar fashion that any sufficiently transitive subgroup of an ordered permutation group $\mathbf{A}(\Omega)$ fails to satisfy any non-trivial equation. The details are in [9]. McCleary has shown [17] that if G is a lattice ordered group which is not normal valued, then G contains a subgroup which acts highly transitively on an ordered set Ω. It then follows from the previous statements that a non-normal valued G cannot belong to any proper variety, and so $\mathbf{N}$ is the largest proper variety.

Returning again to the bottom of V, since the abelian variety $\mathbf{A}$ is defined by just one equation, it follows from general results in universal algebra that $\mathbf{A}$ must have *covers*--varieties immediately larger than $\mathbf{A}$. In fact, $\mathbf{A}$ cannot be the intersection of any properly descending tower. It is still an open problem to find all the covers of $\mathbf{A}$. However, in [20] Scrimger discovered a large class of them. For each integer $n \geq 2$, there is a lattice ordered group G_n generated by $a,b > e$ such that $(b^{-i}ab^{i}) \wedge a = e$ if $1 \leq i < n$ and $b^{-n}ab^{n} = a$. Then G_n generates the Scrimger variety $\mathfrak{S}_n$. For each prime p, $\mathfrak{S}_p$ covers $\mathbf{A}$, and for different primes p and q, $\mathfrak{S}_p$ and $\mathfrak{S}_q$ are distinct. Moreover, none of the G_n are representable, so $\mathfrak{S}_p \cap \mathfrak{R} = \mathbf{A}$.

The representable variety $\mathfrak{R}$ is not a cover of $\mathbf{A}$; in fact as Hollister showed [11], $\mathfrak{R}$ contains all of the nilpotent varieties, which form an infinite ascending chain. Nevertheless, $\mathfrak{R}$ must contain a cover of $\mathbf{A}$. In [18] Medvedev discovered three representable covers of $\mathbf{A}$. Let M^{+} be the totally ordered group generated by $a,b > e$ with $a^{n} < b^{-1}ab$ for all n (notation: $a \ll b^{-1}ab$). Let $\mathfrak{M}^{+}$ be the variety generated by M^{+}. Similarly, $\mathfrak{M}^{-}$ is defined with $a \ll bab^{-1}$. Finally, $\mathfrak{M}$ is the variety generated by the free nilpotent class 2 group on a,b ordered lexicographically on $a^{i}b^{j}[a,b]^{k}$. Medvedev showed that each of $\mathfrak{M}^{+}$, $\mathfrak{M}^{-}$, and $\mathfrak{M}$ is a cover of $\mathbf{A}$ and that any variety which contains a solvable non-abelian group contains one of these three.

There is just one other known cover of $\mathbf{A}$. In [3] T. Feil observed that there would be another representable cover of $\mathbf{A}$ if there is a non-abelian totally ordered group in which whenever $e \ll x \ll y$, then $x \ll y^{-1}xy$. Recently, G. Bergman (unpublished) has constructed such an order of a free group.

The set V of all varieties also has a semigroup structure related to extension. If $\mathfrak{U},\mathfrak{V} \in V$, we define $\mathfrak{U}\mathfrak{V}$ to be the set of all lattice ordered groups G such that G has a homomorphic image $\bar{G} \in \mathfrak{V}$ with corresponding kernel $N \in \mathfrak{U}$. There is an equivalent way to view the product $\mathfrak{U}\mathfrak{V}$. In [10] it was established that for each variety $\mathfrak{U}$ and lattice ordered group G, there is a unique largest convex subgroup sublattice $\mathfrak{U}(G)$ of G which belongs to $\mathfrak{U}$. The subobject $\mathfrak{U}(G)$ is also normal and is thought of as the $\mathfrak{U}$-radical of G. Then $G \in \mathfrak{U}\mathfrak{V}$ if and only if $(G/\mathfrak{U}(G)) \in \mathfrak{V}$.

What are the idempotents $\mathfrak{V} = \mathfrak{V}^2$ of the semigroup V? These are the varieties which are closed under extension. Two obvious examples are $\mathbf{E}$ and $\mathfrak{L}$. A less obvious example is $\mathbf{N}$ [16]. Since any non-trivial variety contains $\mathbf{A}$, any non-trivial idempotent must contain $\mathbf{A}\mathbf{A} = \mathbf{A}^2, \mathbf{A}^3, \ldots, \mathbf{A}^n$, and hence $\bigvee_n \mathbf{A}^n$. In [7] it was shown that $\bigvee_n \mathbf{A}^n = \mathbf{N}$. Thus, there are no idempotents other than $\mathbf{E}$, $\mathbf{N}$, and

$\mathfrak{L}$. This makes the following notion of dimension useful. For a variety $\mathfrak{V}$, we say $\dim \mathfrak{V} = n$ if $\mathfrak{A}^n \subseteq \mathfrak{V}$ but $\mathfrak{A}^{n+1} \not\subseteq \mathfrak{V}$. Then, except for $\mathfrak{E}$, $\mathfrak{N}$, and $\mathfrak{L}$, every variety has a positive dimension. In [7], we showed that $\dim(\mathfrak{U}\mathfrak{V}) = \dim \mathfrak{U} + \dim \mathfrak{V}$ and $\dim(\mathfrak{U} \vee \mathfrak{V}) = \max(\dim \mathfrak{U}, \dim \mathfrak{V})$. As a consequence, if $\mathfrak{U}$ and $\mathfrak{V}$ are different from $\mathfrak{N}$, then $\mathfrak{U}\mathfrak{V} \neq \mathfrak{N}$ and $\mathfrak{U} \vee \mathfrak{V} \neq \mathfrak{N}$. Thus, $\mathfrak{N}$ is irreducible (in the semigroup V). There are also irreducible varieties of every dimension. From the homomorphism property of dim it follows that every variety (different from $\mathfrak{E}$, $\mathfrak{N}$ or $\mathfrak{L}$) is the product of irreducible varieties. In [7], we showed that the varieties different from $\mathfrak{E}$, $\mathfrak{N}$, or $\mathfrak{L}$ form a free semigroup on the irreducible varieties.

Since there are only a countable number of equations, the number of varieties can be no more than the number of subsets of this countable set, that is $2^{\aleph_0}$. The question of whether this upper bound is achieved remained open until Kopytov and Medvedev [12] modified an argument of Olshansky (for varieties of groups) to show there are $2^{\aleph_0}$ varieties of lattice ordered groups. Reilly [19] found an anti-chain of $2^{\aleph_0}$ varieties, which shows that V is very "broad." And Feil [4] found a chain of varieties isomorphic to the chain of real numbers, showing that V is also very "tall."

It is fairly easy to give a description of Feil's varieties. Let p,q be positive integers with $0 < p,q < 1$. Let $[\![a,b]\!] = |[a,b]| = a^{-1}b^{-1}ab \vee b^{-1}a^{-1}ba$. Then $\mathcal{F}_{p,q}$ is the variety of representable lattice ordered groups which satisfy the inequality $[\![x,[\![x,y]\!]]\!]^p \geqslant [\![x,y]\!]^q$ if $e \leqslant y \leqslant x$. A straightforward computation shows that if $p,q \leqslant r,s$, then $\mathcal{F}_{p,q} \subseteq \mathcal{F}_{r,s}$. To show that the containment is strict if the inequality is, consider, for each real number t, $0 < t < 1$, the totally ordered group $F_t = \mathbb{R} \times \mathbb{Z}$ ordered antilexicographically, with group operation

$$(r_1,n_1)(r_2,n_2) = (r_1 + (t/(t+1))^{n_1} r_2, n_1 + n_2),$$

a splitting extension of the reals by the integers. It is easy to show that $F_t \in \mathcal{F}_{p,q}$ if and only if $t \leqslant p/q$. Finally, for each $0 < t < 1$, let $\mathcal{F}_t = \bigcap_{t \leq p/q} \mathcal{F}_{p/q}$. Then $\{\mathcal{F}_t | 0 < t < 1\}$ is a tower of varieties, ordered (under containment) like the real interval $(0,1)$. In particular, for each irrational t, the variety $\mathcal{F}_t$ cannot be defined by a single equation because it is a proper intersection of infinitely many varieties.

The study of varieties of lattice ordered groups is being actively pursued by many mathematicians. Among the interesting unsolved problems are these two:

1. Find all the covers of the abelian variety.
2. Which varieties satisfy the divisible embedding property--that if G belongs to the variety then G can be embedded in a divisible H in the

variety? It is known that the abelian variety does and the variety of all lattice ordered groups does. It is not known whether the representable variety does.

REFERENCES

1. G. Birkhoff, *Lattice Theory*, Amer. Math. Soc. Colloquium Pub. vol. 25, (1969).

2. A. Bigard, K. Keimel, and S. Wolfenstein, *Groupes et Anneaux Réticulés*, Lecture Notes in Mathematics 608, Springer, (1977).

3. *The Black Swamp Problem Book*, unpublished, original kept at Bowling Green State University.

4. T. Feil, An uncountable tower of ℓ-group varieties, *Algebra Universalis*, 14 (1981), 129-131.

5. L. Fuchs, *Partially Ordered Algebraic Systems*, Addison Wesley (1963).

6. A. M. W. Glass, *Ordered Permutation Groups*, London Math. Soc. Lecture Notes 55, Cambridge U. Press, (1981).

7. A. M. W. Glass, W. C. Holland, S. H. McCleary, The structure of ℓ-group varieties, *Algebra Universalis*, 10(1980), 1-20.

8. W. C. Holland, The lattice ordered group of automorphisms of an ordered set, *Michigan Math. J.*, 10(1963), 399-408.

9. _________, The largest proper variety of lattice ordered groups, *Proc. Amer. Math. Soc.*, 57(1976), 25-28.

10. _________, Varieties of ℓ-groups are torsion classes, *Czech. Math. J.*, 29 (1979), 11-12.

11. H. A. Hollister, Nilpotent ℓ-groups are representable, *Algebra Universalis*, 8 (1978), 65-71.

12. V. M. Kopytov and N. Ja. Medvedev, Varieties of lattice ordered groups, *Algebra and Logic*, 16(1977), 281-285.

13. P. Lorenzen, Über halbgeordnete Gruppen, *Math. Z.*, 52(1950), 483-526.

14. J. Martinez, Free products in varieties of lattice-ordered groups, *Czech. Math. J.*, 22(1972), 535-553.

15. _________, Archimedean-like classes of lattice-ordered groups, *Trans. Amer. Math. Soc.*, 186(1973), 33-49.

16. _________, Varieties of lattice-ordered groups, *Math. Z.*, 137(1974), 265-284.

17. S. H. McCleary, O-primitive ordered permutation groups I, II, *Pacific J. Math.*, 40(1972), 349-372; 49(1973), 431-443.

18. N. Ja. Medvedev, The lattices of varieties of lattice ordered groups and Lie algebras, *Algebra and Logic*, 16(1977), 27-30.

19. N. R. Reilly, A subsemilattice of the lattice of varieties of lattice ordered groups, *Can. J. Math.*, 33(1981), 1309-1318.

20. E. B. Scrimger, A large class of small varieties of lattice ordered groups, *Proc. Amer. Math. Soc.*, 51(1975), 301-306.

21. E. C. Weinberg, Free lattice-ordered groups, *Math. Ann.*, 151(1963), 187-199

Bowling Green State University
Bowling Green, Ohio 43403

ON JOIN-INDECOMPOSABLE EQUATIONAL THEORIES

Jaroslav Ježek

There are various papers devoted to the investigation of the lattice $\mathcal{L}_\Delta$ of equational theories of a given type Δ. For example, if Δ is a large type (a type containing either at least two unary symbols or at least one at least binary symbol), then the following properties of $\mathcal{L}_\Delta$ are known. $\mathcal{L}_\Delta$ has uncountably many coatoms and no atoms; $\mathcal{L}_\Delta$ satisfies no nontrivial lattice identity; every algebraic lattice with only countably many compact elements is isomorphic to an interval in $\mathcal{L}_\Delta$; $\mathcal{L}_\Delta$ has no automorphisms besides the obvious "syntactically defined" ones; any finitely based equational theory of type Δ is definable up to automorphisms in $\mathcal{L}_\Delta$; every non-extreme element of $\mathcal{L}_\Delta$ is a cover of some other element.

An element a of a lattice L is said to be join-indecomposable if it is not the least element of L and cannot be expressed in the form $a=b\vee c$ where $b<a$ and $c<a$. In [3] it is proved that an element of $\mathcal{L}_\Delta$ is join-indecomposable iff it is strongly join-indecomposable (or essentially one-based) and a problem is formulated to characterize those equations (a,b) whose generated equational theory Cn(a,b) is join-indecomposable in $\mathcal{L}_\Delta$. The purpose of this paper is to give a partial solution to this problem. The class $\mathcal{E}$ of all equations of type Δ can be decomposed into four subclasses $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$, $\mathcal{E}_4$ as follows (see Section 1 for the meaning of the symbols $\parallel, \sim, <$):

$$\mathcal{E}_1 = \{(a,b)\in\mathcal{E};\ \mathrm{var}(a)\neq\mathrm{var}(b)\},$$
$$\mathcal{E}_2 = \{(a,b)\in\mathcal{E};\ \mathrm{var}(a)=\mathrm{var}(b)\ \text{ and }\ a\parallel b\},$$
$$\mathcal{E}_3 = \{(a,b)\in\mathcal{E};\ \mathrm{var}(a)=\mathrm{var}(b)\ \text{ and }\ a\sim b\},$$
$$\mathcal{E}_4 = \{(a,b)\in\mathcal{E};\ \mathrm{var}(a)=\mathrm{var}(b)\ \text{ and either }\ a<b\ \text{ or }\ b<a\}.$$

The following will be proved in Section 2:

THEOREM. If $(a,b)\in\mathcal{E}_1$ then Cn(a,b) is join-indecomposable iff Δ contains only nullary symbols. If $(a,b)\in\mathcal{E}_2$ then Cn(a,b) is always join-indecomposable. If $(a,b)\in\mathcal{E}_3$ then Cn(a,b) is join-indecomposable iff b can be obtained from a by a permutation f of variables such that the order of f is a prime power.

As for the equations from $\mathscr{E}_4$, the problem remains open. We have the following

CONJECTURE. If $(a,b) \in \mathscr{E}_4$ then $Cn(a,b)$ is always join-decomposable.

The author was not able to prove it; in Section 3 we prove only three very special cases of this conjecture.

Join-indecomposable equational theories are also considered in [1]. There it is proved that the equational theory of commutative groupoids is join-indecomposable and a categorical characterization of varieties with join-decomposable equational theory is given (these varieties are called approximable in [1]).

1. PRELIMINARIES. The terminology and notation here are the same as in Section 1 of [2]. Throughout this paper, Δ is a fixed type. The set of variables is denoted by V and the algebra of terms (of type Δ) by W_Δ. Endomorphisms of W_Δ are called substitutions. If f is a mapping of a set $M \subseteq V$ into W_Δ, then the mapping $f \cup 1_{V \setminus M}$ can be uniquely extended to a substitution; this substitution will be denoted by $\bar{f}$, but we shall often write $f(t)$ instead of $\bar{f}(t)$. If a,b are two terms, then $a \leq b$ means that $f(a)$ is a subterm of b for some substitution f. We write $a \sim b$ if $a \leq b$ and $b \leq a$ at the same time. If $a \leq b$ and $b \nleq a$, we write $a < b$. If neither $a \leq b$ nor $b \leq a$, we write $a \parallel b$. The length of a term t is denoted by $\lambda(t)$. $var(t)$ is the set of variables contained in t. If t is a term and $u \in V \cup \Delta$, then $P_u(t)$ denotes the number of occurrences of u in t. By an equational theory (of type Δ) we mean a fully invariant congruence of W_Δ, i.e. a set of equations which is closed for consequences. $\mathscr{L}_\Delta$ denotes the lattice of equational theories of type Δ. An equational theory is said to be join-decomposable if it is a join-decomposable element of $\mathscr{L}_\Delta$.

Let an equation (a,b) be given. An equation (c,d) is said to be an immediate consequence of (a,b) if, for some substitution f, d results from c by replacing one occurrence of a subterm $f(a)$ by $f(b)$. By an (a,b)-proof (from a_0 to a_n) we mean a nonempty finite sequence $a_0,\dots,a_n$ of terms such that for every $i \in \{1,\dots,n\}$ either (a_{i-1},a_i) or (a_i,a_{i-1}) is an immediate consequence of (a,b).

For the following it will be useful to have a supply of concrete examples of equational theories.

EXAMPLE 1.1. Let E be the set of equations (a,b) such that $var(a)=var(b)$. Then (obviously) E is an equational theory.

EXAMPLE 1.2. For any $n \geq 1$ let L_n be the set of equations (a,b) such that either $a=b$ or $\lambda(a) \geq n$ and $\lambda(b) \geq n$. Then (obviously) L_n is an equational theory.

EXAMPLE 1.3. For any term t let Y_t be the set of equations (a,b) such that either $a=b$ or $a \not\leq t$ and $b \not\leq t$. Then (obviously) Y_t is an equational theory.

EXAMPLE 1.4. For any $n \geq 1$ and any subset D of Δ let $Z_{n,D}$ be the set of equations (a,b) such that n divides $P_u(b)-P_u(a)$ for all $u \in V \cup D$. Then $Z_{n,D}$ is an equational theory. In fact, it is evident that $Z_{n,D}$ is a congruence of W_Δ; its full invariancy follows from the fact that if t is a term, f a substitution, $x \in V$ and $u \in D$ then

$$P_x(f(t)) = \sum_{y \in var(t)} P_x(f(y))P_y(t),$$
$$P_u(f(t)) = P_u(t) + \sum_{y \in var(t)} P_u(f(y))P_y(t).$$

2. THE EQUATIONS FROM $\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3$.

THEOREM 2.1. Let (a,b) be an equation such that $var(a) \neq var(b)$. Then $Cn(a,b)$ is a join-indecomposable equational theory iff Δ contains only nullary symbols.

Proof. If Δ contains only nullary symbols, then $Cn(a,b)$ is the greatest element of $\mathcal{L}_\Delta$ and it is easy to see that it is join-indecomposable. Now let Δ contain a symbol F of arity $n \geq 1$. It is enough to consider the case when $var(b) \setminus var(a)$ is nonempty. For every term t and every $i \geq 1$ define a term $t^{(i)}$ by induction on i as follows: $t^{(1)}=t$; $t^{(i+1)}=F(t^{(i)},t^{(i)},\dots,t^{(i)})$. For every $i \geq 1$ define two substitutions f_i, g_i as follows: if $x \in var(b) \setminus var(a)$ then $f_i(x)=a^{(i)}$ and $g_i(x)=b^{(i)}$; if x is a variable not belonging to $var(b) \setminus var(a)$ then $f_i(x)=g_i(x)=x$. Evidently, there exist positive integers m,p,q such that $m > \lambda(a)$, $m > \lambda(b)$, $\lambda(f_p(b)) \geq m$, $\lambda(g_q(b)) \geq m$. Put

$$T_1 = Cn(a,f_p(b)),$$
$$T_2 = Cn(f_p(b),g_q(b)),$$
$$T_3 = Cn(g_q(b),b)$$

and consider the equational theories E and L_m (see 1.1 and 1.2). Then $T_1 \subseteq E$, $Cn(a,b) \nsubseteq E$, $T_2 \subseteq L_m$, $Cn(a,b) \nsubseteq L_m$, $T_3 \subseteq E$, $Cn(a,b) \nsubseteq E$ and so T_1, T_2, T_3 are different from $Cn(a,b)$. It is easy to see that $Cn(a,b) = T_1 \vee T_2 \vee T_3$ and so $Cn(a,b)$ is join-decomposable.

LEMMA 2.2. Let (a,b) be an equation such that $var(a)=var(b)$ and $a \parallel b$. Let c be a term such that $(a,c) \in Cn(a,b)$. Then either $c=a$ or $c=b$.

Proof. There exists an (a,b)-proof $u_0, \dots, u_n$ from a to c. It is enough to prove by induction on $i \in \{0, \dots, n\}$ that $u_i \in \{a,b\}$. For $i=0$ it is clear. Let $i \leq n$ and $u_{i-1}=a$. Either (u_{i-1}, u_i) or (u_i, u_{i-1}) is an immediate consequence of (a,b). Since $b \nleq a$, only (u_{i-1}, u_i) can be an immediate consequence of (a,b). There exists a substitution f such that $f(a)$ is a subterm of u_{i-1} and u_i is obtained from u_{i-1} by replacing this subterm by $f(b)$. Evidently $f(a)=u_{i-1}=a$ and $f(x)=x$ for all $x \in var(a)=var(b)$, so that $f(b)=b$ and $u_i=b$. It can be proved similarly that if $u_{i-1}=b$ then $u_i=a$.

THEOREM 2.3. Let (a,b) be an equation such that $var(a)=var(b)$ and $a \parallel b$. Then $Cn(a,b)$ is a join-indecomposable equational theory.

Proof. Suppose $Cn(a,b)=T_1 \vee T_2$ for some equational theories T_1, T_2 different from $Cn(a,b)$. Since $(a,b) \in T_1 \vee T_2$, there exists a sequence $u_0, \dots, u_n$ $(n \geq 0)$ such that $a=u_0$, $b=u_n$ and $(u_{i-1}, u_i) \in T_1 \cup T_2$ for all $i \in \{1, \dots, n\}$. By 2.2 we have $\{u_0, \dots, u_n\} = \{a,b\}$ and so there is an $i \in \{1, \dots, n\}$ such that $\{u_{i-1}, u_i\} = \{a,b\}$. We get $(a,b) \in T_1 \cup T_2$ and so either T_1 or T_2 equals $Cn(a,b)$.

LEMMA 2.4. Let a be a term and f be a permutation of $var(a)$. Let w be a term. Then $(a,w) \in Cn(a,f(a))$ iff $w=f^c(a)$ for some integer c.

Proof. Let $(a,w) \in Cn(a,f(a))$, so that there exists an $(a,f(a))$-proof $u_0, \dots, u_n$ from a to w. It is enough to prove by induction on $i \in \{0, \dots, n\}$ that $u_i=f^c(a)$ for some integer c. For $i=0$ it is clear. Let $i \leq n$ and $u_{i-1}=f^c(a)$. If (u_{i-1}, u_i) is an immediate consequence of $(a,f(a))$ then evidently u_i equals $f^{c+1}(a)$. If (u_i, u_{i-1}) is an immediate consequence of $(a,f(a))$ then $u_i=f^{c-1}(a)$. The converse is evident.

THEOREM 2.5. Let (a,b) be an equation such that $var(a)=var(b)$ and $a \sim b$, so that $b=f(a)$ for some permutation f of $var(a)$. Then $Cn(a,b)$ is a join-indecomposable equational theory iff the order of f is a prime power.

Proof. Denote by n the order of f (the least positive integer such that $f^n=1_{var(a)}$). If $n=1$ then $a=b$ and $Cn(a,b)$ is join-decomposable by definition. Let $n\geq 2$.

Consider first the case $n=p^k$ where p is a prime number and $k\geq 1$. Suppose $Cn(a,b)=T_1\vee T_2$ for some equational theories T_1,T_2 different from $Cn(a,b)$. Since $(a,b)\in T_1\vee T_2$, there exists a finite sequence $u_0,\dots,u_m$ such that $a=u_0$, $b=u_m$ and $(u_{i-1},u_i)\in T_1\cup T_2$ for all $i\in\{1,\dots,m\}$. For every $i\in\{0,\dots,m\}$ we have $(a,u_i)\in Cn(a,b)$ and so $u_i=f^{c_i}(a)$ for some integer c_i by 2.4. Of course, $c_m\equiv 1$ (mod p^k), so that c_m is not divisible by p. Denote by j the least number from $\{0,\dots,m\}$ such that c_j is not divisible by p; we have $j>0$ and c_{j-1} is divisible by p. The equation $(f^{c_{i-1}}(a),f^{c_i}(a))$ and hence also the equation $(a,f^{c_i-c_{i-1}}(a))$ belongs either to T_1 or to T_2. The greatest common divisor of the numbers c_i-c_{i-1} and p^k equals 1 and so there are integers d,e such that $(c_i-c_{i-1})d+p^ke=1$. The equation $(a,b)=(a,f^{(ci-ci-1)d+p^ke}(a))$ belongs either to T_1 or to T_2, since $f^{(ci-ci-1)d+p^ke}=f^{(ci-ci-1)d}$. We get a contradiction.

Now consider the case when n is not a prime power. We can write $n=km$ for some integers $k,m\geq 2$ whose greatest common divisor equals 1. Put $T_1=Cn(a,f^k(a))$ and $T_2=Cn(a,f^m(a))$. It follows from 2.4 that both T_1 and T_2 are proper subtheories of $Cn(a,b)$. There are integers d,e such that $dk+em=1$. The equation $(a,b)=(a,f^{dk+em}(a))$ belongs to $T_1\vee T_2$ and so $Cn(a,b)=T_1\vee T_2$.

3. THE EQUATIONS FROM $\mathcal{E}_4$ - SOME PARTIAL RESULTS.

PROPOSITION 3.1. Let (a,b) be an equation such that $var(a)=var(b)$ and $a<b$. Suppose that $Cn(a,b)$ is a join-indecomposable equational theory. Then (a,b) is a consequence of (a,c) for any c such that (a,c) is a consequence of (a,b) and $a<c$.

Proof. Let $(a,c)\in Cn(a,b)$ and $a<c$. Evidently $Cn(a,b)=Cn(a,c)\vee Cn(c,b)$. We have $Cn(c,b)\subseteq Y_a$ and $Cn(a,b)\nsubseteq Y_a$ (see 1.3) and so $Cn(a,b)\neq Cn(c,b)$. Since $Cn(a,b)$ is join-indecomposable, it follows that $Cn(a,b)=Cn(a,c)$ and so (a,b) is a consequence of (a,c).

PROPOSITION 3.2. Let (a,b) be an equation such that $var(a)=var(b)$; let there exist a permutation f of $var(a)$ such that $f(a)$ is a proper subterm of b. Then $Cn(a,b)$ is a join-decomposable equational theory.

Proof. For every $i \geq 1$ define a term b_i, containing $f^i(a)$ as a proper subterm, as follows: $b_1 = b$; if b_i is already defined, let b_{i+1} be the term obtained from b_i by replacing one occurrence of the subterm $f^i(a)$ by $f^i(b)$. We have $(a,b_i) \in Cn(a,b)$ for all i. Put $c = b_n$ where n is the order of f. Then $(a,c) \in Cn(a,b)$, $var(a) = var(c)$ and a is a proper subterm of c. Define terms $c_1, c_2, \ldots$ as follows: $c_1 = c$; if c_i is already defined, let c_{i+1} be the term obtained from c_i by replacing one occurrence of the subterm a by c. We have $(a,c_i) \in Cn(a,b)$ for all i. We cannot have $P_u(a) = P_u(c)$ for all $u \in V \cup \Delta$, and so there exists an integer $k \geq 2$ which is not a common divisor of the numbers $P_u(c) - P_u(a)$ $(u \in V \cup \Delta)$. For every $i \geq 2$ and for every $u \in V \cup \Delta$ we have $P_u(c_i) = P_u(c_{i-1}) + P_u(c) - P_u(a)$; hence $P_u(c_k) - P_u(a) = k(P_u(c) - P_u(a))$. Consider the equational theory $Z_{k,\Delta}$ (see 1.4). We have $(a,c_k) \in Z_{k,\Delta}$ and $(a,c) \notin Z_{k,\Delta}$, so that (a,c) is not a consequence of (a,c_k); hence (a,b) is not a consequence of (a,c_k). It follows from 3.1 that $Cn(a,b)$ is join-decomposable.

PROPOSITION 3.3. Let (a,b) be an equation such that $var(a) = var(b) = \{x_1, \ldots, x_n\}$ $(n \geq 1)$, $a < b$ and $P_{x_i}(a) \neq P_{x_i}(b)$ for some i. Let there exist a substitution f such that $b = f(a)$. For every $i,j \in \{1, \ldots, n\}$ put $a_{i,j} = P_{x_j}(f(x_i))$ and denote by A the matrix $(a_{i,j})$. If $det(A) \neq 0$ then $Cn(a,b)$ is a join-decomposable equational theory.

Proof. For every term t such that $var(t) \subseteq \{x_1, \ldots, x_n\}$ denote by C_t the matrix $(P_{x_1}(t), \ldots, P_{x_n}(t))$. It is easy to prove $C_{f(t)} = C_t A$. For every $k \geq 1$ denote by $a_{k;i,j}$ the members of A^k. There exists a prime number p such that p does not divide $det(A)$ and p does not divide $P_{x_i}(b) - P_{x_i}(a)$ for some i. There exists an infinite set $N_{1,1}$ of positive integers such that whenever $i,j \in N_{1,1}$ then $a_{i;1,1} \equiv a_{j;1,1}$ (mod p). There exists an infinite subset $N_{1,2} \subseteq N_{1,1}$ such that whenever $i,j \in N_{1,2}$ then $a_{i;1,2} \equiv a_{j;1,2}$ (mod p). We can proceed in this way and construct infinite sets $N_{1,1} \supseteq N_{1,2} \supseteq \ldots \supseteq N_{1,n} \supseteq N_{2,1} \supseteq \ldots \supseteq N_{2,n} \supseteq \ldots \supseteq N_{n,n}$. Let us fix two numbers $k,l \in N_{n,n}$ such that $k > l$. Every member of the matrix $A^k - A^l$ is divisible by p. Put $m = k - l$. Evidently, $(a, f^m(a))$ is a consequence of (a,b) and $a < f^m(a)$. By 3.1 it is enough to show that (a,b) is not a consequence of $(a, f^m(a))$. Consider the equational theory $Z_{p,\emptyset}$ (see 1.4). We have $(a,b) \notin Z_{p,\emptyset}$ and so it is sufficient to prove that p divides any member of $C_{f^m(a)}-C_a=C_aA^m-C_a=C_a(A^m-A^0)$. Denote this matrix by $(d_1,\dots,d_n)$. Since $C_a(A^m-A^0)A^1=C_a(A^k-A^1)$ and p divides any member of A^k-A^1, every member of the matrix $(d_1,\dots,d_n)A^1$ is divisible by p. This means that over the field $\mathbb{Z}_p$ of integers modulo p, the vector $(d_1,\dots,d_n)$ is a solution of a system of linear equations; the determinant of this system equals $\det(A^1)=(\det(A))^1$ and so it is nonzero in $\mathbb{Z}_p$; hence $(d_1,\dots,d_n)$ is the zero vector over $\mathbb{Z}_p$, i.e. p divides all the numbers $d_1,\dots,d_n$.

PROPOSITION 3.4. Let x be a variable and (a,b) be an equation such that $var(a)=var(b)=\{x\}$ and $a<b$; let there exist a substitution f such that f(a) is a subterm of b and $x\in var(f(x))$. Then Cn(a,b) is a join-decomposable equational theory.

Proof. For every $i\geq 1$ define a term b_i, containing $f^i(a)$ as a subterm, as follows: $b_1=b$; if b_i is already defined then b_{i+1} is obtained from b_i by replacing one occurrence of the subterm $f^i(a)$ by $f^i(b)$. We have $(a,b_i)\in Cn(a,b)$ for all i.

Consider first the case $P_x(f(x))\geq 2$. Then $P_x(a)<P_x(b)<P_x(b_2)$, so that (a,b_2) belongs and (a,b) does not belong to the equational theory $Z_{k,\emptyset}$ where $k=P_x(b_2)-P_x(a)$; we can use 3.1.

Now let $P_x(f(x))=1$. We cannot have $P_u(a)=P_u(b)$ for all $u\in\{x\}\cup\Delta$ and so there exists an even number $k\geq 2$ such that for some $u\in\{x\}\cup\Delta$, k+1 does not divide $P_u(b)-P_u(a)$. It is easy to see that

$$P_x(b_k)-P_x(a)=(k+1)(P_x(b)-P_x(a))$$

and

$$P_u(b_k)-P_u(a)=(k+1)(P_u(b)-P_u(a))+\frac{k(k+1)}{2}P_u(f(x))(P_x(b)-P_x(a))$$

for all $u\in\Delta$ and so (a,b_k) belongs to the equational theory $Z_{k+1,\Delta}$. On the other hand, (a,b) does not belong to this theory and so (a,b) is not a consequence of (a,b_k); we can use 3.1.

References

[1] O.C.García and Mario Solay Z.: A classification in varieties of algebras. Universidad Nacional Autónoma de México, Publicaciones Preliminares del Instituto de Matematicas, No.21, 1980, 1-12.

[2] J.Ježek: The lattice of equational theories. Part I: Modular elements. Czechoslovak Math. J. 31, 1981, 127-152.

[3] R.McKenzie: Definability in lattices of equational theories. Annals of Math. Logic 3, 1971, 197-237.

Charles University, Department of Mathematics
Sokolovská 83, 186 00 Praha 8, Czechoslovakia

IDEALFREE CIM-GROUPOIDS AND OPEN CONVEX SETS

Jaroslav Ježek and Tomáš Kepka

A groupoid is said to be a CIM-groupoid (commutative idempotent medial groupoid) if it satisfies the following three identities:

$$xy = yx\ ,$$
$$xx = x,$$
$$xy.zu = xz.yu.$$

Let us remark that in some papers medial groupoids are called abelian or entropic. There are several papers devoted to CIM-groupoids. For example, the lattice of varieties of CIM-groupoids is described (in [4]). The theory of CIM-groupoids is connected with other algebraic theories, e.g. with the theory of modules and with universal algebra. CIM-groupoids are algebraic structures with nice and rather strong properties and there seems to be a possibility of deep structure theorems on CIM-groupoids. For example, consider the problem of classification of all finitely generated CIM-groupoids. It turns out that for any such groupoid G we can define a congruence w_G on G such that G/w_G is a finite semilattice and every block of w_G is a finitely q-generated idealfree CIM-groupoid (this follows from Propositions 2.1 and 1.6 below). Now, in the present paper we classify all finitely q-generated idealfree CIM-groupoids. Although we do not know which of them serve as blocks of w_G for some finitely generated G and it seems to be a difficult task to reconstruct G from the blocks of w_G and from the finite semilattice G/w_G, the solution of the above mentioned problem is at least not beyond hope.

The main result of this paper, the classification of finitely q-generated, idealfree CIM-groupoids, is formulated in Section 5; its proof, together with necessary definitions and partial results, is contained in Sections 1,2,3 and 4.

1. PRELIMINARIES. Let $\mathbb{D}$ designate the set of rational numbers of the form $a2^{-k}$ where a,k are integers. Then $\mathbb{D}$ is a principal ideal domain. For $n \geq 0$ define a binary operation $\circ$ on $\mathbb{D}^n$ by

$$(x_1,\dots,x_n)\circ(y_1,\dots,y_n) = (2^{-1}(x_1+y_1),\dots,2^{-1}(x_n+y_n))$$

and define $n+1$ elements of $\mathbb{D}^n$ as follows:

$$e_{n,0} = (0,0,\dots,0),$$
$$e_{n,1} = (1,0,\dots,0),$$
$$\dots$$
$$e_{n,n} = (0,\dots,0,1).$$

The set $\mathbb{D}^n$ will be considered together with the usual topology and metrics.

PROPOSITION 1.1. Let $n \geq 0$. Then:

(1) $\mathbb{D}^n(\circ)$ is a free CIM-quasigroup and the set $\{e_{n,0},e_{n,1},\dots,e_{n,n}\}$ is its free basis.

(2) The subgroupoid $\mathbb{F}_n$ of $\mathbb{D}^n(\circ)$ generated by $\{e_{n,0},e_{n,1},\dots,e_{n,n}\}$ is a free CIM-groupoid and the set $\{e_{n,0},e_{n,1},\dots,e_{n,n}\}$ is its free basis.

(3) An element $(x_1,\dots,x_n)$ of $\mathbb{D}^n$ belongs to $\mathbb{F}_n$ iff $0 \leq x_1,\dots,x_n$ and $x_i+\dots+x_n \leq 1$.

Proof. See [3].

PROPOSITION 1.2. The varieties of pointed CIM-quasigroups and (unitary) $\mathbb{D}$-modules are equivalent. In more detail: Assign to any pointed CIM-quasigroup $Q(.,/,e)$ a $\mathbb{D}$-module with the underlying set Q by

$$x+y = (xy)/e,$$
$$-x = e/x,$$
$$0 = e,$$
$$2^{-1}x = ex.$$

Conversely, assign to any $\mathbb{D}$-module $M(+,-,0,(rx;\ r\in\mathbb{D}))$ a pointed CIM-quasigroup $M(.,/,e)$ by

$$xy = 2^{-1}(x+y),$$
$$x/y = 2x-y,$$
$$e = 0.$$

In this way we get a pair of mutually inverse bijections between the two varieties; these bijections preserve underlying sets and homomorphisms.

Proof. Easy and well known (it follows e.g. from [2]).

It should be pointed here that quasigroups (considered as algebras with three binary operations) have permutable congruences and that CIM-quasigroups are abelian in the sense of commutator theory.

Let G be a groupoid. For a nonempty subset M of G we denote by $[M]$ the subgroupoid generated by M. A subgroupoid H of G is called q-closed if $a \in H$ whenever $a \in G$, $b \in H$ and either $ab \in H$ or $ba \in H$. A nonempty subset M of G is called q-generating if G is the only q-closed subgroupoid of G containing M. We denote by $\sigma(G)$ the least cardinal number of a generator set of G and by $\sigma_q(G)$ the least cardinal number of a q-generator set of G.

PROPOSITION 1.3. Let G be a cancellative CIM-groupoid. Then there exists a CIM-quasigroup Q such that G is a q-generating subgroupoid of Q. Moreover, Q is determined uniquely up to isomorphism over G. We have $\sigma_q(G) = \sigma_q(Q)$.

Proof. See Theorem 5.3.1 of [6].

By an ideal of a groupoid G we mean a nonempty subset I of G such that $IG \subseteq I$ and $GI \subseteq I$. A groupoid G is said to be idealfree if G is the only ideal of G.

PROPOSITION 1.4. Every idealfree CIM-groupoid is cancellative.

Proof. See Proposition 6.9 of [5].

PROPOSITION 1.5. Let H be a subgroupoid of a finitely q-generated, cancellative CIM-groupoid G. Then H is finitely q-generated and $\sigma_q(H) \leq \sigma_q(G)$. If G is q-generated by H then $\sigma_q(H) = \sigma_q(G)$.

Proof. By 1.3 it is enough to consider the case when H, G are quasigroups. Put $n = \sigma_q(G)$. The quasigroup G can be q-generated by some elements $u_1, \dots, u_n$ such that $u_1 \in H$. Consider H and G as pointed quasigroups, with the point u_1. It follows from 1.2 that the assertion can be translated into the language of $\mathbb{D}$-modules. However, it is well known (see e.g. [7]) that if R is a principal ideal domain, if M is an R-module generated by $n-1$ elements and if N is a submodule of M then N is generated by $n-1$ elements too.

PROPOSITION 1.6. Let H be a subgroupoid of a finitely generated CIM-groupoid G. Then H is finitely q-generated and $\sigma_q(H) \leq \sigma(G)$.

Proof. Put $n = \sigma(G)$. By 1.1 there is a homomorphism of $\mathcal{F}_{n-1}$ onto G. The rest is easy by 1.5.

2. THE CONGRUENCE w_G. For any groupoid G define an equivalence w_G on G as follows: $(a,b) \in w_G$ iff the elements a, b generate

the same ideal of G. In a CIM-groupoid G, the condition $(a,b)\in w_G$ is evidently equivalent to the existence of elements $u_1,\dots,u_n,v_1,\dots,v_m\in G$ $(n,m\geq 0)$ such that $b=(((au_1)u_2)\dots)u_n$ and $a=(((bv_1)v_2)\dots)v_m$.

PROPOSITION 2.1. Let G be a CIM-groupoid. Then:
(1) w_G is a congruence of G.
(2) G/w_G is a semilattice.
(3) Every block of w_G is an idealfree CIM-groupoid.
(4) The natural homomorphism of G onto G/w_G induces an isomorphism of the lattice of ideals of G onto the lattice of ideals of G/w_G.
(5) If G is finitely q-generated then G has a least ideal.
(6) If G is finitely generated and $n=\sigma(G)$ then $\mathrm{Card}(G/w_G)\leq 2^n-1$.

Proof. (1) If $(a,b)\in w_G$ then $b=(((au_1)u_2)\dots)u_n$ and $a=(((bv_1)v_2)\dots)v_m$ for some $n,m\geq 0$ and some elements $u_1,\dots,u_n,v_1,\dots,v_m\in G$. Since CIM-groupoids are distributive, this implies $bc=(((ac.u_1c).u_2c)\dots).u_nc$ and $ac=(((bc.v_1c).v_2c)\dots).v_mc$ for any $c\in G$, so that $(ac,bc)\in w_G$.

(2) In order to prove that $(ab.c,a.bc)\in w_G$ for any $a,b,c\in G$, it is enough to show that if I is an ideal then $ab.c\in I$ iff $a.bc\in I$. However, we have $a.bc=ab.ac=(ab.a)(ab.c)$ and similarly $ab.c=(a.bc)(c.bc)$.

(3) Let H be a block of w_G and $a,b\in H$. We can write $b=(((au_1)u_2)\dots)u_n$ and $a=(((bv_1)v_2)\dots)v_m$. Hence $b=bb=(((ab.u_1b).u_2b)\dots).u_nb$ and $a=aa=(((ba.v_1a).v_2a)\dots).v_ma$. From this it is easy to see that the elements $b,u_1b,\dots,u_nb,a,v_1a,\dots,v_ma$ belong to H and so $(a,b)\in w_H$. Hence $w_H=H\times H$ and H is idealfree.

(4) is obvious.

(5) If G is finitely q-generated then G/w_G is finitely q-generated too. It is easy to see that a semilattice is finitely q-generated iff it contains a least element (with respect to the ordering defined by $x\leq y$ iff $xy=x$).

(6) We have $\sigma(G/w_G)\leq n$; a semilattice with n generators has at most 2^n-1 elements.

3. THE CONGRUENCE t_G. For any groupoid G we define a binary relation t_G on G as follows: $(a,b)\in t_G$ iff the subgroupoid $[a,b]$ is finite. G is said to be a torsionfree groupoid if $t_G=\mathrm{id}_G$, i.e. if any two distinct elements of G generate an infinite subgroupoid. G is said to be a torsion groupoid if $t_G=G\times G$, i.e. if any subgroupoid generated by two elements is finite.

LEMMA 3.1. Let G be a torsion cancellative CIM-groupoid. Then G is a locally finite quasigroup.

Proof. Obviously, G is a quasigroup. The rest is easy (use either 1.2 or the fact that $[u_0,\dots,u_{n+1}]=[u_0,\dots,u_n][u_0,u_{n+1}]$ for any $u_0,\dots,u_{n+1}\in G$).

PROPOSITION 3.2. Let G be a cancellative CIM-groupoid. Then:
(1) t_G is a congruence of G.
(2) Every block of t_G is a locally finite CIM-quasigroup.
(3) G/t_G is a torsionfree, cancellative CIM-groupoid.

Proof. (1) Let $(a,b),(b,c)\in t_G$, $H=[a,b]$ and $K=[b,c]$. Then both H and K are finite and $HK=[a,b,c]$. Consequently, $(a,c)\in t_G$ and we have proved that t_G is an equivalence. However, for $a,b,c\in G$, the map $x\mapsto cx$ is an isomorphism of $[a,b]$ onto $[ca,cb]$ and we see that t_G is a congruence and, moreover, that G/t_G is a cancellative groupoid.

(2) is clear, use 3.1.

(3) Put $H=G/t_G$. As we have proved in (1), H is cancellative; it remains to show that it is torsionfree. For, let $a,b\in G$ be such that $(f(a),f(b))\in t_H$, f being the natural homomorphism of G onto H. Put $K=[a,b]$. Evidently, t_K is just the restriction of t_G to K, and so K/t_K is finite. If A is a block of t_K then A is a locally finite, finitely q-generated quasigroup (use 1.6 and (2)) and therefore A is finite. We have proved that K is finite, i.e. $(a,b)\in t_G$ and $f(a)=f(b)$.

LEMMA 3.3. Let G be a finitely q-generated, cancellative CIM-groupoid. Then:
(1) Every block of t_G is a finite quasigroup.
(2) If G is idealfree then the blocks of t_G are pairwise isomorphic.

Proof. (1) Use 1.5 and 3.2.

(2) Let A,B be two blocks of t_G. Take two elements $a\in A$, $b\in B$. Since G is idealfree, $(a,b)\in w_G$ and so there are elements $u_1,\dots,u_n,v_1,\dots,v_m\in G$ $(n,m\geq 0)$ with $b=(((au_1)u_2)\dots)u_n$ and $a=(((bv_1)v_2)\dots)v_m$. Put $f(x)=(((xu_1)u_2)\dots)u_n$ and $g(x)=(((xv_1)v_2)\dots)v_m$ for all $x\in G$. We have $f(A)\subseteq B$ and $g(B)\subseteq A$. However, f,g are injective and A,B are finite. Hence $f(A)=B$ and A is isomorphic to B.

LEMMA 3.4. Let G be a q-generating, idealfree subgroupoid of a finitely q-generated CIM-quasigroup Q. If A is a block of t_Q

with $A \cap G \neq \emptyset$ then $A \subseteq G$.

Proof. Since G is a q-generating subgroupoid, there exist a limit ordinal number μ and a chain $(G_\alpha)_{\alpha<\mu}$ of subgroupoids of Q with the following properties:

(i) $G_0=G$;

(ii) if $\alpha<\mu$ then $a_\alpha G_{\alpha+1}=G_\alpha$ for some $a_\alpha \in G_\alpha$;

(iii) if $\alpha \leq \mu$ is a limit ordinal then G_α is the union of all G_β with $\beta<\alpha$;

(iv) $G_\mu=Q$.

Evidently, all the subgroupoids G_α are idealfree (in fact, $G_{\alpha+1}$ is isomorphic to G_α and the union of a chain of idealfree groupoids is idealfree); by 1.5 they are all finitely q-generated. Let B be any block of t_G. It is enough to show by transfinite induction that B is a block of t_{G_α} for any $\alpha<\mu$. For $\alpha=0$ this is obvious. If B is a block of t_{G_α}, denote by C the block of $t_{G_{\alpha+1}}$ containing B. Since $x \mapsto a_\alpha x$ is an isomorphism of $G_{\alpha+1}$ onto G_α, it follows from 3.3(2) that C is isomorphic to B. However, both B and C are finite by 3.3(1) and so B=C. The limit case is clear and we are through.

LEMMA 3.5. Let Q be a finitely q-generated CIM-quasigroup. Then $Q \simeq P \times \mathbb{D}^n(\circ)$ for some finite CIM-quasigroup P and some $n \geq 0$.

Proof. Let us fix an element $e \in Q$ and denote by P the block of t_Q containing e, so that (by 3.1 and 1.5) P is a finite quasigroup. Consider P and Q as pointed quasigroups (with the point e) and denote by N,M the corresponding $\mathbb{D}$-modules (see 1.2). Then N is just the torsion part of M. Since M is a finitely generated module over a principal ideal domain, there exists a free submodule K of M such that M is the direct sum of N and K (see [1]). Since K is free, the corresponding CIM-quasigroup is free too, and we can use 1.1.

PROPOSITION 3.6. Let G be a finitely q-generated idealfree CIM-groupoid. Then $G \simeq P \times H$ for some finite CIM-quasigroup P and some finitely q-generated, torsionfree, idealfree CIM-groupoid H. Moreover, P and H are determined uniquely up to isomorphism, since every block of t_G is isomorphic to P and G/t_G is isomorphic to H.

Proof. By 1.3 and 1.4, there is a finitely q-generated CIM-quasigroup Q such that G is a q-generating subgroupoid of Q. By 3.5 it is enough to consider the case $Q=P \times \mathbb{D}^n(\circ)$ for some finite CIM-quasigroup P and some $n \geq 0$. The blocks of t_Q are just the subgroupoids $P \times \{a\}$ ($a \in \mathbb{D}^n$). It follows from 3.4 that $G = P \times H$ for a subgroupoid H of $\mathbb{D}^n(\circ)$; evidently, H is torsionfree, idealfree and (by 1.5) finitely q-generated.

PROPOSITION 3.7. Let G be a finitely q-generated, cancellative, torsionfree CIM-groupoid with $n = \sigma_q(G)$. Then G is isomorphic to a q-generating subgroupoid of $\mathbb{D}^{n-1}(\circ)$.

Proof. By 1.3, G is a q-generating subgroupoid of a CIM-quasigroup Q; Q is torsionfree and $\sigma_q(Q)=n$. By 3.5, $Q \simeq \mathbb{D}^{n-1}(\circ)$.

4. SUBGROUPOIDS OF $\mathbb{D}^n(\circ)$. For every $n \geq 1$ denote by $\mathbb{D}_{(n)}$ the ring of matrices of type (n,n) over $\mathbb{D}$.

PROPOSITION 4.1. (1) Let $n \geq 1$, $a \in \mathbb{D}^n$ and let $A \in \mathbb{D}_{(n)}$. The mapping $f: \mathbb{D}^n \longrightarrow \mathbb{D}^n$ defined by $f(x)=xA+a$ is an endomorphism of $\mathbb{D}^n(\circ)$. This endomorphism is an automorphism of $\mathbb{D}^n(\circ)$ iff A is invertible in $\mathbb{D}_{(n)}$ iff $\det(A) = \pm 2^k$ for some integer k.

(2) Every endomorphism (automorphism, resp.) of $\mathbb{D}^n(\circ)$ is of the form described in (1).

Proof. It is easy.

LEMMA 4.2. Let $n \geq 2$ and let $a_1,\dots,a_n$ be relatively prime integers. Then there are positive integers $b_1,\dots,b_n,m$ such that $b_1a_1+\dots+b_na_n = \pm 2^m$.

Proof. We can assume without loss of generality that $a_1 > 0$ is odd. There are integers $c_1,\dots,c_n$ such that $c_1a_1+\dots+c_na_n=1$; there are positive integers $d_1 > -c_1,\dots,d_n > -c_n$ such that the number $k=d_1a_1+\dots+d_na_n$ is odd and positive. Put $m = \varphi(k)$ (the Euler function). Then k divides 2^m-1. We have $ku+1=2^m$ for some $u \geq 1$ and we can put $b_i=d_iu+c_i$.

LEMMA 4.3. Let $n \geq 1$ and let G be a q-generating subgroupoid of $\mathbb{D}^n(\circ)$. For each $a \in G$ there are elements $b_1,\dots,b_n \in G$ such that the matrix (b_i-a), $i=1,\dots,n$, is invertible in $\mathbb{D}_{(n)}$.

Proof. For $x=(x_1,\dots,x_n)$ and $0 \leq i \leq n$ put ${}^ix=(x_1,\dots,x_i)$. We shall show by induction that for every $0 \leq m \leq n$ there are elements $b_1,\dots,b_m \in G$ and an integer k such that the determinant of the matrix $({}^mb_i-{}^ma)$, $i=1,\dots,m$, equals $\pm 2^k$ (here the determinant of the empty matrix is 1). So, let $1 \leq m \leq n$ and let $b_1,\dots,b_{m-1} \in G$ be such that

$\det({}^{m-1}b_i - {}^{m-1}a) = \pm 2^k$. For every $x \in \mathbb{D}^n$, let $A(x)$ denote the matrix

$$\begin{pmatrix} {}^m b_i - {}^m a \\ {}^m x - {}^m a \end{pmatrix}, \quad i=1,\dots,m-1.$$

Let $p \geq 3$ be a prime number. Denote by H the set of all $x \in \mathbb{D}^n$ such that p divides $\det(A(x))$ in $\mathbb{D}$. It is easy to check that H is a subquasigroup of $\mathbb{D}^n(\circ)$. Moreover, $a+e_{n,m}$ does not belong to H due to the fact that p does not divide $\det({}^{m-1}b_i - {}^{m-1}a)$, $i=1,\dots,m-1$. Since G is q-generating, $G \nsubseteq H$.

Hence for every prime number $p \geq 3$ there exists an element $x \in G$ such that p does not divide $\det(A(x))$ in $\mathbb{D}$. It follows that there are $r \geq 2$ and elements $z_1,\dots,z_r \in G$ such that the numbers $\det(A(z_1)),\dots,\det(A(z_r))$ are relatively prime in $\mathbb{D}$. According to 4.2, $c_1\det(A(z_1))+\dots+c_r\det(A(z_r)) = \pm 2^t$ for some positive integers $c_1,\dots,c_r$ and some integer t. Let s be a positive integer such that $(c_1+\dots+c_r)2^{-s} \leq 1$. Then $(c_1 2^{-s},\dots,c_r 2^{-s}) \in \mathbb{F}_r$ by 1.1. The mapping $(x_1,\dots,x_r) \mapsto a+x_1(z_1-a)+\dots+x_r(z_r-a)$ is a homomorphism of $\mathbb{F}_r(\circ)$ onto the subgroupoid of $\mathbb{D}^n(\circ)$ generated by $a,z_1,\dots,z_r$ and so the element $a+c_1 2^{-s}(z_1-a)+\dots+c_r 2^{-s}(z_r-a)$ belongs to G; denote this element by b_m. Now, $\det(A(b_m)) = c_1 2^{-s}\det(A(z_1))+\dots+ c_r 2^{-s}\det(A(z_r)) = \pm 2^{t-s}$.

LEMMA 4.4. Let $n \geq 1$ and let G be an open subgroupoid of $\mathbb{D}^n(\circ)$. Then G is a q-generating, idealfree subgroupoid of $\mathbb{D}^n(\circ)$. Moreover, G is a convex subset of $\mathbb{D}^n$.

Proof. Clearly, G is a q-generating subgroupoid. Further, let I be an ideal of G, $a \in I$ and $b \in G$. There exists an n-dimensional sphere U with center b such that $U \subseteq G$. Then $b+(a-b)2^{-m} \in U$ for some positive integer m and we have $b-(a-b)2^{-m} \in U$. However, I is an ideal, $b+(a-b)2^{-m} = b\circ(\dots(b\circ a))$ belongs to I and

$$b = (b+(a-b)2^{-m})\circ(b-(a-b)2^{-m}) \in I.$$

We have proved that $I=G$, and hence G is idealfree. It remains to show that G is convex. For, let $a,b \in G$ and let $c \in \mathbb{D}^n$ lie between a and b. There is a neighborhood V of $(0,0,\dots,0)$ in $\mathbb{D}^n$ such that $a+V \subseteq G$ and $b+V \subseteq G$. Obviously, there exists a $t \in \mathbb{D}$ with $0 \leq t \leq 1$ such that $c \in a+t(b-a)+V$. Put $a'=c-t(b-a)$ and $b'=a'+b-a$, so that $a' \in a+V$ and $b' \in b+V$. Then $a',b' \in G$ and $c=a'+t(b'-a')$, so that $c \in G$.

LEMMA 4.5. Let $n \geq 1$ and let G be a q-generating subgroupoid of $\mathbb{D}^n(\circ)$. Denote by I the interior of G, i.e. the set of all

$a \in \mathbb{D}^n$ such that a neighborhood of a is contained in G. Then I is nonempty and it is just the least ideal of G.

Proof. Let $a \in G$ be arbitrary. By 4.3 there are $b_1,\dots,b_n \in G$ such that the matrix $A=(b_i - a)$, $i=1,\dots,n$, is invertible in $\mathbb{D}_{(n)}$. Put $f(x)=xA+a$ for every $x \in \mathbb{D}^n$. Then f is a continuous automorphism of $\mathbb{D}^n(\circ)$ and $f(\mathcal{F}_n) \subseteq G$. Now it is clear that I is nonempty; evidently, I is an ideal of G. On the other hand, I is an open subgroupoid and so I is idealfree by 4.4. The rest is obvious.

PROPOSITION 4.6. Let $n \geq 1$ and let G be a nonempty subset of $\mathbb{D}^n$. The following are equivalent:

(1) G is a q-generating, idealfree subgroupoid of $\mathbb{D}^n(\circ)$;

(2) G is an open convex subset of $\mathbb{D}^n$;

(3) G is an open subgroupoid of $\mathbb{D}^n(\circ)$.

Proof. In 4.4 we have proved (3) $\Rightarrow$ (1) and (3) $\Rightarrow$ (2). The implication (2) $\Rightarrow$ (3) is obvious and (1) $\Rightarrow$ (3) follows from 4.5.

PROPOSITION 4.7. Let $n \geq 1$ and let G_1, G_2 be two nonempty open convex subsets of $\mathbb{D}^n$; let there exist an isomorphism j of $G_1(\circ)$ onto $G_2(\circ)$. Then j can be uniquely extended to an automorphism of $\mathbb{D}^n(\circ)$.

Proof. Let $a \in G_1$. There exists an $m \geq 1$ such that the elements $b_1=a+e_{n,1}2^{-m},\dots,b_n=a+e_{n,n}2^{-m}$ belong to G_1. There are two endomorphisms e,f of $\mathbb{D}^n(\circ)$ such that $e(e_{n,0})=a$, $e(e_{n,1})=b_1,\dots$, $e(e_{n,n})=b_n$, $f(e_{n,0})=j(a)$, $f(e_{n,1})=j(b_1),\dots$, $f(e_{n,n})=j(b_n)$. It follows from 4.1 that e is an automorphism of $\mathbb{D}^n(\circ)$. We have $j(x)=fe^{-1}(x)$ for all $x \in \{a,b_1,\dots,b_n\}$ and so for all x from the subgroupoid H generated by $\{a,b_1,\dots,b_n\}$; evidently, H is just the convex set generated by $\{a,b_1,\dots,b_n\}$. Let us fix an element u from the interior of H. Let $x \in G_1$. There exists an $r \geq 1$ such that the element $v=(((x\circ u)\circ u)\circ\dots)\circ u$ (where u appears r times) belongs to H. We have $j(u)=fe^{-1}(u)$ and $j(v)=fe^{-1}(v)$, so that

$$(((j(x)\circ j(u))\circ j(u))\circ\dots)\circ j(u)=(((fe^{-1}(x)\circ j(u))\circ j(u))\circ\dots)\circ j(u)$$

and consequently $j(x)=fe^{-1}(x)$. We have proved $j \subseteq fe^{-1}$. Since fe^{-1} extends j, it is easy to prove that fe^{-1} is injective and surjective, so that it is an automorphism of $\mathbb{D}^n(\circ)$. The unicity of the extension of j is evident.

5. FORMULATION OF THE MAIN RESULT.

THEOREM. (1) A groupoid G is a finitely q-generated idealfree CIM-groupoid iff there exist a finite CIM-quasigroup P, an integer $n \geq 0$ and a nonempty open convex subset H of $\mathbb{D}^n$ such that $G \simeq P \times H(\circ)$.

(2) Let P_1, P_2 be two finite CIM-quasigroups; let $n, m \geq 0$, let H_1 be a nonempty open convex subset of $\mathbb{D}^n$ and H_2 be a nonempty open convex subset of $\mathbb{D}^m$. Then $P_1 \times H_1(\circ) \simeq P_2 \times H_2(\circ)$ iff $P_1 \simeq P_2$, $n=m$ and $H_2 = j(H_1)$ for an automorphism j of $\mathbb{D}^n(\circ)$. (Automorphisms of $\mathbb{D}^n(\circ)$ are described in 4.1.)

Proof. It is a combination of 3.6,3.7,1.4,4.6,4.7.

COROLLARY. The number of nonisomorphic finitely q-generated idealfree CIM-groupoids is $2^{\aleph_0}$.

R e f e r e n c e s

[1] N.Bourbaki: Éléments de Mathématique. Partie I, Livre II: Algebra, Chapitre VII. Hermann & C^{ie}, Paris.

[2] J.Ježek and T.Kepka: Quasigroups, isotopic to a group. Commentationes Math. Univ. Carolinae 16, 1975, 59-76.

[3] J.Ježek and T.Kepka: Free commutative idempotent abelian groupoids and quasigroups. Acta Univ. Carolinae 17/2, 1976, 13-19.

[4] J.Ježek and T.Kepka: The lattice of varieties of commutative abelian distributive groupoids. Algebra Univ. 5, 1975, 225-237.

[5] J.Ježek, T.Kepka and P.Němec: Distributive groupoids. Rozpravy ČSAV, Řada mat. a přír. věd, 91/3, 1981 (Praha, Academia), 3-94.

[6] J.Ježek and T.Kepka: Medial groupoids. Rozpravy ČSAV, Řada mat. a přír. věd (to appear).

[7] O.Zariski and P.Samuel: Commutative algebra I. D.Van Nostrand, Princeton 1958.

Charles University, Department of Mathematics
Sokolovská 83, 186 00 Praha 8, Czechoslovakia

FINITE FORBIDDEN LATTICES

Ralph McKenzie*

ABSTRACT. Let L be any finite simple lattice of at least three elements, whose co-atoms intersect to 0. One principal result of the paper is that L is not dual isomorphic to the lattice of subvarieties of any locally finite variety. A second principal result is that these statements are equivalent: (i) L is isomorphic to the congruence lattice of a finite algebra with one basic operation; (ii) L is isomorphic either to the subspace lattice of a finite vector space, or for some permutation σ of a finite domain, to the lattice of equivalence relations invariant under σ.

INTRODUCTION. Lattices isomorphic to the congruence lattice of an algebra are called *algebraic*, and have been characterized abstractly. Interesting questions arise when we ask about representations in special classes of algebras. The simplest questions of this sort, concerning the number and the type of operations required to represent a lattice, have been the source of interesting and serendipitous results, for instance the discovery of innocuous conditions on an algebraic lattice which force every representing algebra to have rather well behaved operations.

"It is a trivial fact that, while representing lattices as congruence lattices of algebras, we can confine ourselves to unary algebras." (Quoted from Pálfy, Pudlák [9].) Indeed, this is true in the sense that, for every algebra, there exists a unary algebra having the same universe and the same congruence lattice. And the quoted authors make good use of this fact. On the other hand, algebras whose operations are unary are not widely important in mathematics. And so a major theme in recent investigations of congruence lattices has been the elucidation of the influence that the "shape" of a congruence lattice can have on the structure of n-ary operations, $n \geq 2$, that preserve all the congruences. The discovery that deep influences of this sort exist is a belated but spectacular by-product of work on the simplest of special representation problems, the problem of characterizing abstractly the algebraic lattices that are isomorphic to the congruence lattice of an algebra having just one binary operation.

*Research supported by National Science Foundation grant MCS-8103455.

In [1], Freese, Lampe, and Taylor prove that for L the lattice of subspaces of an infinite dimensional vector space over an uncountable field F, if A is any algebra whose congruence lattice is isomorphic to L, then every operation of A satisfies a quasi-identity called the "term condition" (which is strongly suggestive of linear operations), and A must have at least $\kappa = |F|$ many operations. (Lampe described, in 1977, a class of lattices that force the term condition, and Freese and Taylor modified his result to include these subspace lattices.) Taylor [14] uses Lampe's discovery to construct a countable algebraic lattice that is not representable as the congruence lattice of any semigroup.

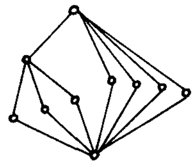
As a consequence of the mentioned result, and another result of Lampe's, the sought-after characterization for congruence lattices of algebras with one binary operation now seems very remote. He proved, in [4], that any algebraic lattice whose unit element is compact (and this is true of every finite lattice) can be represented as the congruence lattice of an *infinite* algebra with one binary operation.

This paper is the outcome of a long-standing interest in the characterization of lattices that can be represented as the congruence lattice of a *finite* algebra with one binary operation. The naive expectation that all finite lattices must admit such a representation is shown here to be false. But our main contribution is to show that the shape of the congruence lattice can force the operations of a finite algebra to satisfy the term condition, and in fact, to satisfy an even stronger quasi-identity. This paper, like [9], also clarifies some of the obstacles which make it so difficult to construct finite algebras with prescribed congruence lattices. At this moment, it remains unknown if every finite lattice is isomorphic to the congruence lattice of a finite algebra. (We shall return to this question a few paragraphs later.)

In 1969, we had shown that for every finite algebra A, there are finite algebras B and C with $Con\ A \cong Con\ B \cong Con\ C$, and such that B has just four unary operations, and C has only a binary operation and a unary operation. These proofs can be found in [2; Theorem 4.7.2] and in [5; §§1-2]. It remains unknown today whether the four unary operations can be replaced by three, or by two.

One of the more striking results in this paper is the description of a congruence lattice of two unary operations on a finite set (in fact, of two permutations), which is not isomorphic to the congruence lattice of any finite algebra with one operation (n-ary, for any n). Below is pictured such a lattice.

Sub A_4



The alternating group on four letters, A_4, can be represented as a group of 12 permutations on a 12-element set U. This group is generated by two permutations f and g. The congruence lattice of the algebra $\langle U,f,g\rangle$ is isomorphic to the lattice of subgroups of A_4. It is a consequence of the result stated in our Abstract, and the work in §5 (Theorem 5.3 and Exercise 5.4), that this lattice has the property claimed for it.

Loosely speaking, the argument developed in this paper runs parallel to the one in Freese, Lampe, Taylor [1]; but the details are completely different. Our starting point is the idea of Pálfy, Pudlák [9], that is, to consider the minimal algebras with a given congruence lattice. Unlike them, however, we admit any finite algebra with a given congruence lattice, and we consider the family of all subsets of that algebra on which minimal algebras are induced. We find that certain abstract properties of the congruence lattice of a finite algebra, in fact the properties stated in our Abstract, imply a kind of pseudo-geometric structure to the family of minimal sets. Algebras possessing this structure are said to have *tame minimal sets*. Surprisingly, every finite simple algebra has tame minimal sets (Corollary 1.10).

Through the vehicle of tame minimal sets, an additional property of the congruence lattice is found to imply that an algebra satisfies what we call the "strong term condition" (Theorem 2.10, Theorem 2.11). A complete structural analysis of finite algebras with one operation, having tame minimal sets and satisfying the strong term condition, is given in §4. This leads in §5 to the second result of the Abstract (Theorem 5.3). The first result of the Abstract, which is Theorem 3.6, was totally unexpected; it is an easy corollary of the other results.

The first manuscript of this paper was written in December 1981. This one is being written in December 1982. During the year we learned of two new results, and these have led to improvements in the theorems we had earlier announced.

The first is the result in P.P.Pálfy's paper [8], reproduced here as Theorem 1.5, which characterizes minimal algebras. This has allowed us to replace everywhere in our paper the adjective "Arguesian" by "isomorphic to the subspace lattice of a vector space," and tends to put all of our results in a clearer light. The second new result, obtained by my student David Hobby, is that the subspace lattice of a finite vector space of dimension greater than one, if it is isomorphic to the congruence lattice of a finite algebra A, forces A to satisfy the term condition (but not the strong term condition). The theorems in §3 about forbidden lattices of subvarieties have been sharpened by incorporating Hobby's result.

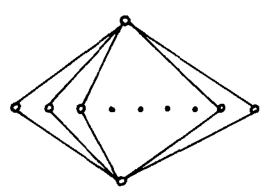
Since it incorporates the results of Pálfy and Hobby, not proved here, this paper is not self-contained. The paper is so structured, with occasional comments to the reader, that the earlier results, which are in effect fully proved here, can be delineated.

We should like to acknowledge a substantial contribution made by W.A.Lampe to this work, both by his presence in Berkeley at the time the results were obtained, and by his careful reading of the first manuscript, which led to many improvements.

We close the introduction with some commentary on the most challenging open problem in the present-day theory of finite lattices. Is every finite lattice isomorphic to the congruence lattice of a finite algebra? (Only in 1976 did we learn, thanks to Pudlák and Tuma [11], that every finite lattice is isomorphic to a *sublattice* of the congruence lattice of some finite algebra.) In the last real advance made on this problem, Pálfy and Pudlák in [9] examined minimal finite unary algebras having a given abstract congruence lattice, and were able to show, assuming some properties of the lattice stronger than those stated in our Abstract, that each of the unary operations must be constant or a permutation. They then constructed, for every finite lattice, a finite lattice satisfying their conditions and having the given lattice as an interval sublattice. In this way they proved: Every finite lattice is isomorphic to the congruence lattice of a finite algebra *iff* every finite lattice is isomorphic to the congruence lattice of a transitive set of permutations on a finite set, or equivalently, is isomorphic to an interval in the lattice of subgroups of a finite group.

The problem of finite representation remains unsolved, and thanks to the work just cited, it seems more interesting and challenging than ever. P. Goralčik proposed to consider the lattices of height 2 as test cases for the problem. M_n is easily representable if $n = 1+p^k$ (p a prime), as the subspace, or congruence, lattice of a 2-dimensional vector space over the Galois field of order p^k.

M_n



n atoms

For all other values of $n > 11$, it is unknown whether M_n has a finite congruence representation. For $n = 7$ or 11, the question has just recently been answered. Partial results for $n = 7$ were given in [3], [7], and [12]. Then Walter Feit (1982, unpublished) found an M_7 interval at the top of $Sub\ A_{31}$, and an M_{11} interval at the top of the subgroup lattice of an alternating group of a larger prime degree. For all $n > 2$, M_n satisfies the hypotheses of our Abstract, and this paper gives new information regarding finite non-unary algebras satisfying $Con\ A \cong M_n$. (As was mentioned earlier, for $n = 1+p^k$, the main result, that A satisfies the term condition, is due to D.Hobby.)

NOTATION. *Algebras*, written usually as $A = \langle A, f_i (i \in I)\rangle$, consist of a non-void set A paired with an indexed family of finitary operations over A. All algebras encountered *are implicitly assumed to be finite*, and all operations are finitary. (The set A is finite, and every f_i is n-ary for some n satisfying $0 < n < \omega$.) This implicit assumption is behind every result in the paper, and all theorems carry the assumption, unless explicitly stated otherwise. *Non-indexed algebras* $\langle A,F\rangle$, F a set of operations over A, will also be called algebras. For both kinds of algebras, the set A is called the universe, or base set, or underlying set, and the f_i (or the $f \in F$) are called the basic operations of the algebra.

The definition of the congruence lattice, *Con* $A = \langle \mathrm{Con}\, A, \vee, \wedge\rangle$, is the usual one, for both kinds of algebras. Its elements are the congruences of A, i.e. the equivalence relations over the base set of A which are preserved by each of the basic operations of the algebra. Isomorphism of indexed algebras is the usual notion. (Two isomorphic indexed algebras must have the same similarity type.) An isomorphism of non-indexed algebras, written $\pi\colon \langle A,F\rangle \cong \langle B,G\rangle$, is a bijection π of A onto B such that $\pi(F) = G$. (For an n-ary operation f on A, πf is defined by $(\pi f)(b_0,\ldots,b_{n-1}) = \pi(f(\pi^{-1}b_0,\ldots,\pi^{-1}b_{n-1}))$.)

By a *permutation group*, we shall always mean an algebra $\langle A,F\rangle$ such that F is a group of permutations of A, i.e. F is closed under composition and inverse and contains the identity permutation. Two permutation groups, in this sense, are isomorphic (as non-indexed algebras) iff the abstract groups admit an isomorphism induced by a bijection of the base sets. Sym A denotes the *set* of all permutations of the set A.

The *clone of term operations* of an algebra A, denoted by Clo A, is the smallest set of operations on A which contains the projections and the basic operations of A and is closed under composition. By a *clone*, we mean the clone of some algebra. (Although algebras are finite, the set of operations of an algebra need not be finite, and not all clones are finitely generated.) The *clone of polynomial operations* of an algebra A, written as Pol A, is the clone over A generated by the set of basic operations of the algebra and the constant unary operations (functions) from A into A. $\mathrm{Clo}_n A$ is the set of n-ary term operations of A; while $\mathrm{Pol}_n A$ is the set of n-ary polynomial operations of A. (Notice: Our definition is quite contrary to Grätzer's usage, in which the term operations are called "polynomials," and our polynomial operations are called "algebraic operations." Our usage is an innovation of the Darmstadt school of universal algebraists. Our notation for the two important clones of an algebra is also unconventional.)

It is well-known, and trivial, that for any indexed or non-indexed algebra A, the algebras $\langle A, \mathrm{Clo}\, A\rangle$, $\langle A, \mathrm{Pol}\, A\rangle$, and $\langle A, \mathrm{Pol}_1 A\rangle$ each have the same congruence lattice as does A. The last algebra in the list is a *mapping monoid*, i.e. it is of the form $\langle A,F\rangle$, F a set of functions from A into A closed under composition and containing the identity function.

Given an algebra A and a set $X \subseteq {}^2A$, the congruence relation generated by X, or $\mathrm{Cg}_A(X)$, is the smallest congruence of A that includes X. The least and largest congruences of A are written as 0_A and 1_A. The identity function on A is id_A. ${}^AB$ denotes the set of all functions from A into B. For $\alpha \in {}^AB$, and for

$U \subseteq A$, $\alpha|_U$ is the restriction of α to U. For $\alpha \in {}^{n}A A$ an n-ary operation on A, $n > 1$, and for $U \subseteq A$, $\alpha|_U$ is defined to be $\alpha|{}^{n}U$, and is called the restriction of α to U. For F a set of operations on A and for $U \subseteq A$, $F|_U$ is the set of all $f|_U$ such that $f \in F$ and U is closed under f.

Now let $A = \langle A, \ldots \rangle$ be any algebra. Every nonvoid subset U of A is the base set of an algebra which we call an *induced algebra* of A. It is the algebra $A|_U = \langle U, (\text{Pol } A)|_U \rangle$. Observe that $(\text{Pol } A)|_U$ is a clone over U and it contains the constant functions from U into U.

1. TAME MINIMAL SETS

The property called "tame minimal sets," a property actually of mapping monoids, is the central new idea of this paper. It is very useful here, and (after the first manuscript of this paper was written) had a key role in a short proof of the Givant-Palyutin theorem characterizing categorical quasi-varieties of countable type, in [6]. First we define the minimal sets of a mapping monoid.

Definition 1.1. (1) Let $A = \langle A, F \rangle$ be a mapping monoid. A subset $B \subseteq A$ will be called a *minimal set* of A iff $B = \alpha(A)$ for some $\alpha \in F$, $|B| > 1$, and $\beta(A) < B$, $\beta \in F$, implies that $|\beta(A)| = 1$. (Here "$<$" denotes proper inclusion.) The set of all minimal sets of A will be denoted by $M(A)$.

(2) Let A be an algebra. We put $M(A) = M(\langle A, \text{Pol}_1 A \rangle)$, and call the members of this set the *minimal sets* of A.

Observe that $M(A)$ is nonvoid if $|A| > 1$, since we assume that A is finite. Observe also that if the algebra $A = \langle A, F \rangle$ is a mapping monoid, then (1) and (2) give the same minimal sets, since $\text{Pol}_1 A$ is the union of F and the set of constant functions, in this case. We define the property of tame minimal sets in such a way that it looks innocuous and, possibly, ill-named. The definition makes it relatively easy to prove in specific instances that an algebra has tame minimal sets. But the proposition following the definition shows that it is quite a strong notion.

Definition 1.2. We say that a mapping monoid $A = \langle A, F \rangle$ satisfies TMS (or has *tame minimal sets*) iff there exists $B \in M(A)$ such that

i) (*density*) for all $x, y \in A$, $x \neq y$, there is some $\alpha \in F$ such that $\alpha(x), \alpha(y) \in B$, $\alpha(x) \neq \alpha(y)$.

ii) (*connectedness*) for all $x, y \in A$ there are $\alpha_0, \ldots, \alpha_n \in F$ for some n with $x \in \alpha_0(B)$, $y \in \alpha_n(B)$, and $\alpha_i(B) \cap \alpha_{i+1}(B) \neq \emptyset$ for all $i < n$.

An algebra A satisfies TMS iff $\langle A, \text{Pol}_1 A \rangle$ does.

Again, the two definitions will be found to agree for algebras that are mapping monoids. 1.2(ii) is clearly equivalent to $Cg_A(^2B) = 1_A$. 1.2(i) implies that $\theta \cap {}^2B > 0_B$ for each $\theta > 0_A$ in Con A.

PROPOSITION 1.3. *If a mapping monoid* $A = \langle A,F\rangle$ *satisfies TMS then the following hold.*

(1) *For any pair of minimal sets* B,C *there are* $\lambda,\mu \in F$ *with* $\mu\lambda|_B = id_B$ *and* $\lambda\mu|_C = id_C$ *and* $\mu(A) = B$ *and* $\lambda(A) = C$.

(2) *For each* $B \in M(A)$ *there is an* $e = e^2 \in F$ *with* $e(A) = B$.

(3) *For all* $x,y \in A$ *and* $B \in M(A)$, *if* $x \neq y$, *then for some* $\alpha \in F$ *we have* $\alpha(A) = B$ *and* $\alpha(x) \neq \alpha(y)$.

(4) *Each* $B \in M(A)$ *satisfies 1.2(i) and 1.2(ii).*

(5) *If* $\emptyset < U < A$ *then for some* $B \in M(A)$, $U \cap B \neq \emptyset \neq B - U$.

(6) *For* $B \in M(A)$ *and* $\alpha \in F$, $\alpha|_B$ *is one-to-one or constant.*

(7) *For each* $B \in M(A)$ *we have* $M(A) = \{\alpha(B): \alpha \in F \text{ and } \alpha|_B \text{ is one-to-one}\}$.

(8) *If* $\alpha \in F$ *is not constant, then* α *is one-to-one on some minimal set.*

Remark: (2) and (3) above may suggest that the α in (3) can be taken to be idempotent. However, there is a three element counterexample to this.

Proof. We wish to point out two elementary principles of minimal sets. The first, and essentially obvious, one is that if $\beta,\gamma \in F$ and $\beta(A) \in M(A)$ then $\beta\gamma$ is constant or $\beta\gamma(A) = \beta(A)$.

Suppose B and C are minimal sets, $\beta \in F$, and $\beta(A) = B$. The second elementary principle is that if β is not constant on C then β maps C onto B. This follows easily from the first elementary principle by choosing any $\gamma \in F$ with $\gamma(A) = C$.

Suppose that B and C are minimal sets. A major part of the work in proving (1) will be to show that there are $\beta,\gamma \in F$ with $\beta(A) = B$ and $\gamma(A) = C$, which have the additional properties that β is not constant on C and γ is not constant on B.

Let B_0 be a minimal set of A satisfying (i) and (ii) of 1.2. First we find an idempotent $e_0 \in F$ with $B_0 = e_0(A)$. In general, if $f: X \to X$ and X is finite then some power of f is idempotent. There is some $\alpha \in F$ with $B_0 = \alpha(A)$. (Why not just let e_0 = some idempotent power of α? The idempotent powers of α may be constant.) Pick x,y such that $\alpha(x) \neq \alpha(y)$. Applying (ii) to these elements we find that there must be some $\alpha_i \in F$ such that α is not constant on $\alpha_i(B_0)$, i.e. $\alpha\alpha_i$ is not constant on B_0. So $\alpha\alpha_i\alpha$ and $\alpha\alpha_i$ are not constant on A. By the first elementary principle we have $\alpha\alpha_i(A) = \alpha(A) = \alpha\alpha_i\alpha(A)$. Thus for $k \geq 1$, $(\alpha\alpha_i)^k(A) = \alpha(A) = B_0$. We choose e_0 to be some idempotent power of $\alpha\alpha_i$, and so we have $e_0(A) = B_0$.

Now we are ready to establish (1). Let $B \in M(A)$. It suffices to consider only the case when $C = B_0$. Suppose that $B = \beta(A)$. Since β is not constant, by the argument above, using (ii) for B_0, we obtain $\varepsilon \in F$ with β not constant on $\varepsilon(B_0)$.

Pick $u \neq v$ in B and (by 1.2(i) applied to B_0) a $\delta \in F$ with $\delta u \neq \delta v$ and $\delta u, \delta v \in B_0$. So $e_0\delta$ is not constant on B. Thus by the two elementary principles, $e_0\delta$ maps both A and B onto B_0, and $\beta\varepsilon$ maps A and B_0 onto B. Now by finiteness, we have that $\beta\varepsilon|_{B_0}$ and $e_0\delta|_B$ are bijections. So $\beta\varepsilon e_0\delta|_B$ is a permutation of B. Let e be an idempotent power of $\beta\varepsilon e_0\delta$. Clearly $e|_B = \mathrm{id}|_B$. Let $\lambda = e_0\delta$. Then e factors as $\mu\lambda$ for a certain μ such that $\mu(A) = B$ and μ maps B_0 one-to-one onto B. For $x \in B_0$ we have $\mu\lambda\mu x = e\mu x = \mu x$. This implies that $\lambda\mu x = x$, since μ is one-to-one on B_0. So these mappings have the desired properties. This establishes both (1) and (2). Using $C = B_0$, (3) follows from (1) and (2). To establish (4) we need only that 1.2(ii) holds for each $B \in M(A)$. Again using $C = B_0$ and (1) we obtain the desired result.

To finish (6) and (7) it is enough to show for $\alpha \in F$ and $B \in M(A)$ that $\alpha|_B$ is one-to-one or constant and if not constant then $\alpha(B) \in M(A)$. Using (2) we have $\alpha(B) = \alpha(e(A)) = \alpha e(A)$. Let $\alpha|_B$ be not constant. Then $\alpha(B) = \alpha e(A)$ contains a minimal set C. By (1), $|C| = |B|$. So $\alpha(B) = C$, which is minimal, and $\alpha|_B$ is one-to-one (by finiteness).

Statement (5) follows from (6), (7) and (ii) for B_0, by choosing $x \in U$ and $y \notin U$. A similar argument yields (8). □

Definition 1.4. If B is a minimal set of an algebra A, the induced algebra $A|_B = \langle B, (\mathrm{Pol}\, A)|_B \rangle$ will be called a *minimal algebra* of A.

That the minimal algebras of any algebra are very restricted in kind is the content of a beautiful theorem due to P.P.Pálfy.

THEOREM 1.5 (Pálfy). *Let* B *be a minimal set of an algebra* A, $|B| > 2$. *If* $A|_B$ *has an operation that is not essentially unary, then a vector space* V, *over a finite field, can be defined with underlying set* B *such that* $(\mathrm{Pol}\, A)|_B = \mathrm{Pol}\, V$.

Proof. It is obvious that $(\mathrm{Pol}\, A)|_B$ is what Pálfy [8] calls a *permutational clone*, that is, every unary member of the clone is a permutation or constant, and all the constant functions are present. This, then, is the main result of [8]. □

Let us observe that if A has tame minimal sets, and if the minimal sets of A are 2-element sets, then A must be a simple algebra. For if θ is a congruence satisfying $0_A < \theta$, and if B is a minimal set satisfying 1.2(i) and 1.2(ii), then $\theta \cap {}^2B > 0_B$ by 1.2(i); thus, if $|B| = 2$, then $\theta \supseteq {}^2B$ and so $\theta = 1_A$ by 1.2(ii). We shall see in Corollary 1.10 that every simple algebra does have tame minimal sets, although the minimal sets of a simple algebra can certainly have more than two elements. But the algebras that truly concern us in this paper are not simple, and Theorem 1.5 yields important information about them.

PROPOSITION 1.6. *Suppose that the algebra* A *has tame minimal sets. Then any two minimal algebras of* A *are isomorphic.*

Proof. This follows easily from (1) of Proposition 1.3. □

In section 2 we shall find a nice necessary and sufficient condition in order that the minimal algebras of an algebra, which has tame minimal sets, be essentially unary. In this section, we are about to demonstrate that TMS can sometimes be inferred from a knowledge of the abstract congruence lattice of an algebra. Let us pause to introduce some examples of algebras having tame minimal sets.

Suppose that A is functionally complete, or just that $\mathrm{Pol}\,A$ contains every 1-ary operation on the base set A. Then, obviously, $M(A)$ is the set of all 2-element subsets of A, and it is clear that TMS holds. For a trivial example, every 2-element algebra satisfies TMS. (However, 1-element algebras, by our definition, do not.) A harder example: a finite lattice L satisfies TMS iff it is simple, i.e. $Con\ L \cong 2$. (The reader can puzzle this out. We shall soon see that every simple algebra has TMS.) A vector space, V, satisfies TMS (at least if $|V| > 1$) because $M(V) = \{V\}$.

The next lemma and at least part of the idea for 1.8 and 1.9 come from [9]. The lemma is valid for infinite algebras as well as for finite ones.

LEMMA 1.7. *Let* A *be an algebra,* $e = e^2 \in \mathrm{Pol}_1 A$, $B = e(A)$. *For* $\theta \in \mathrm{Con}\ A$, *put* $\pi_B\theta = \theta \cap {}^2B$. *Then* π_B *is a lattice homomorphism of* $Con\ A$ *onto* $Con\ A|_B$.

Proof. Let $F = \mathrm{Pol}_1 A$. Note that $F|_B = \mathrm{Pol}_1(A|_B)$ and $F|_B$ is identical with $\{e\alpha|_B\colon \alpha \in F\}$. The lattices involved in this lemma are $Con\ A = Con\langle A,F\rangle$ and $Con\ A|_B = \mathrm{Con}\langle B,F|_B\rangle$.

Now $\pi_B\theta$ is trivially a congruence of $A|_B$, if θ is a congruence of A. And π_B trivially preserves meets. For each $\psi \in \mathrm{Con}\ A|_B$ define

$$\hat{\psi} = \{(x,y) \in {}^2A\colon \text{for all } \alpha \in F,\ (e\alpha(x),e\alpha(y)) \in \psi\}.$$

Thus $\hat{\psi} \in \mathrm{Con}\ A$. It is easily seen that $\pi_B\hat{\psi} = \psi$ (since $e(x) = x$ for $x \in B$) and, further, that for all $\theta \in \mathrm{Con}\ A$, $\pi_B\theta \leqslant \psi$ iff $\theta \leqslant \hat{\psi}$. That π_B is onto and preserves joins follows easily from these facts. □

THEOREM 1.8. *An algebra* A *satisfies TMS iff the following condition holds. There is an idempotent* $e \in \mathrm{Pol}_1 A$ *such that* $B = e(A)$ *is a minimal set of* A *and for all* $\theta \in \mathrm{Con}\ A$:

i) $\theta > 0_A$ *implies* $\pi_B\theta > 0_B$,

ii) $\theta < 1_A$ *implies* $\pi_B\theta < 1_B$.

Proof. Let $B = e(A)$, $e = e^2$ a unary polynomial of A, and suppose that $B \in M(A)$. We shall show for such a B that 1.2(i) $\iff$ 1.8(i) and 1.2(ii) $\iff$ 1.8(ii). This theorem will then follow from 1.3(2).

First, if 1.2(i) holds then for any $\theta > 0_A$, say $(x,y) \in \theta$, $x \neq y$, we have $(\alpha x, \alpha y) \in \pi_B\theta - 0_B$ for some α. Thus 1.8(i) holds. Conversely, if 1.8(i) holds and $x \neq y$ in A, let $\theta = Cg_A(x,y) > 0_A$. Choose $(u,v) \in \pi_B\theta - 0_B$. There are elements $u = s_0, \ldots, s_n = v$ and unary polynomial functions $\alpha_0, \ldots, \alpha_n \in \mathrm{Pol}_1 A$ with $\{\alpha_i(x), \alpha_i(y)\} = \{s_i, s_{i+1}\}$. $e = e^2$ and $u, v \in B$ imply $e(u) = u$ and $e(v) = v$. Then $u \neq v$ implies that for some i, $e\alpha_i(x) \neq e\alpha_i(y)$. Since $e(A) = B$, this gives 1.2(i).

Second, 1.2(ii) is clearly equivalent to $Cg_A({}^2B) = 1_A$ which is equivalent to 1.8(ii). □

THEOREM 1.9. *If the congruence lattice* L *of a nontrivial algebra* A *satisfies the following two conditions, then* A *satisfies TMS.*

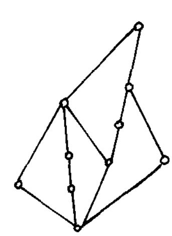
(1) For each $x < 1$ *and* $y > 0$ *in* L, $Cg_L(x,1) = Cg_L(y,0) = 1_L$.

(2) For every meet preserving function ϕ *from* L *into* L *such that* $x < \phi(x)$ *for all* $x < 1$ *in* L, *it is the case that* $\phi(0) = 1$.

Notice that the conditions of the theorem hold for any finite simple lattice whose co-atoms intersect to 0. So we have the following corollary.

COROLLARY 1.10. *Let* A *be a simple algebra, or more generally, a semi-simple algebra whose congruence lattice is simple. Then* A *satisfies TMS.*

There are many finite lattices which satisfy 1.9(1) and 1.9(2), are not simple, and whose co-atoms do not intersect to 0. Here is an example:



Proof of 1.9. Let A be a finite nontrivial algebra (i.e. $|A| > 1$) and let $Con\ A = L$ satisfy the two conditions. Put $F = \mathrm{Pol}_1 A$ and put $I = \{e \in F\colon e^2 = e\}$. We search for an $e \in I$ to demonstrate that the condition of 1.8 holds. There are some non-constant functions in I, for example id_A is one. Let B be a minimal (under $\subseteq$) member of $\{e(A)\colon e \in I$ and e not constant$\}$. And choose $e \in I$ with $e(A) = B$. By Lemma 1.7, π_B is a homomorphism of L onto $Con\ A|_B$ (which is not a trivial lattice, since $|B| > 1$). Thus 1.9(1) yields 1.8(i) and 1.8(ii) for this B. All we need, to get TMS by 1.8, is to prove that $B \in M(A)$.

So let C be some member of $M(A)$ that is contained in B. We hope $C = B$. Suppose instead that $C \subsetneq B$. Let $K = \{\alpha \in F: \alpha(A) \subseteq C\}$. K includes all α such that $\alpha(A) = C$, of which there is at least one. Let $\alpha, \beta \in K$. We claim that $\alpha\beta$ is constant. Suppose it is not. The minimality of C implies that $\beta(A) = \alpha\beta(A) = \alpha(A) = C$ and so $\alpha(C) = C$. Thus $\alpha^k(A) = C$ for all $k \geq 1$. In particular, the idempotent power of α has C as range. The choice of B, and C, implies this is impossible. So we have proved that $K \cdot K$ consists entirely of constant functions. Now for any $\theta \in \operatorname{Con} A$ define

$$\phi(\theta) = \{(x,y) \in {}^2A: \text{ for all } \alpha \in K, (\alpha x, \alpha y) \in \theta\} \quad .$$

Obviously, $K \cdot F \subseteq K$, implying that $\phi(\theta) \in \operatorname{Con} A$. Just as obviously, $\phi(\theta) \geq \theta$ and ϕ is a meet preserving mapping of L into L. Since $K \cdot K$ consists only of constant functions, $\phi(\phi(\theta)) = 1_A$ for all θ, and this implies that $\phi(\theta) > \theta$ for all $\theta < 1_A$ Now by 1.9(2), $\phi(0_A) = 1_A$. This simply means that every member of K is constant, and so $|C| = 1$. This contradicts $C \in M(A)$. So $B = C \in M(A)$. □

The following fact seems noteworthy, although it will not be needed or proved in this paper. (The proof is easy.) The notation used is from the proof of Lemma 1.7.

PROPOSITION 1.11. *Let A satisfy TMS and let $\theta \in \operatorname{Con} A$. Then A/θ satisfies TMS iff $\theta < 1_A$ and for some (or for every) $B \in M(A)$, $\theta = \widehat{\pi_B\theta}$.*

One can define β-minimal sets, where β is a congruence of an algebra A, and define a property we would call *tame β-minimal sets*. When $\beta = 1_A$, the two concepts are identical with the ones we have been studying. If β is the monolithic congruence of a subdirectly irreducible algebra A, then it can be proved that A has tame β-minimal sets. These ideas will be developed in a future paper.

2. THE GLOBAL INFLUENCE OF MINIMAL ALGEBRAS

In the previous section, we described some properties of the congruence lattice of an algebra which imply a property of the mapping monoid of unary polynomial functions of the algebra. The implied property, which we named "tamed minimal sets," can be thought of as a kind of pseudo-geometry of minimal sets under translations by polynomial functions.

Now for an algebra A satisfying TMS, there are just two possibilities. Either a minimal algebra of A is essentially unary, or it has an operation depending on more than one variable (and by 1.6 this is independent of the choice of the minimal algebra). In this section, we show that if the second possibility holds for A, then this reflects back to the congruence lattice, implying that *Con A* can be mapped homomorphically onto the lattice of subspaces of a nontrivial vector space; while the first possibility is equivalent to a remarkable and very useful property holding for all the polynomial operations of A, of any rank.

Thus the minimal algebras of A exert a global influence, which is seen here acting in one of two directions, either back upon the congruence lattice, or forward upon the full clone of polynomial operations of A.

The property of clones that we are aiming for is simple to state, but we shall approach it in gradual steps. Recall that a *quasigroup* is an algebra $\langle A,\cdot\rangle$ with one binary operation, such that for any $a,b \in A$, the equations $x\cdot b = a$, $b\cdot y = a$ have unique solutions x and y. A *quasigroup with 0* is an algebra $\langle A,\cdot\rangle$ such that for some element $u \in A$, $A-\{u\}$ is non-empty, $\langle A-\{u\}, \cdot|_{A-\{u\}}\rangle$ is a quasi-group, and $u\cdot a = a\cdot u = u$ for all $a \in A$. A 2-element *semi-lattice* is any algebra isomorphic to $\langle\{0,1\},\cdot\rangle$ where $\cdot$ is ordinary multiplication. (This is the same as a 2-element quasi-group with 0.) An algebra $B = \langle B,\dots\rangle$ is said to be a *reduct* of an algebra $A = \langle A,\dots\rangle$ if $B = A$, and every basic operation of B is among the basic operations of A. (Under this definition, non-indexed algebras can be reducts of indexed algebras, and vice-versa.)

Exercise 2.1. Let $A = \langle A,\cdot\rangle$ be a quasi-group (assumed finite, of course). Show that $\mathrm{Clo}\,A$ has a ternary operation $p(x,y,z)$ such that the equations $p(x,x,y) = y = p(y,x,x)$ are identities of A, and consequently *Con A* is a modular lattice of commuting equivalence relations. If A is a quasi-group with 0 then, again, *Con A* is a modular lattice of commuting equivalence relations.

Exercise 2.2. Show that if a clone of operations on a set A contains all the constant functions, and is not essentially unary, i.e. if it contains an operation that depends on at least two variables, then it contains a binary operation that depends on both variables. Stronger, if an operation $f(x_1,\dots,x_n)$ on A depends on at least two variables, then for some $1 \leqslant i < j \leqslant n$ and for some $a_1,\dots,a_n \in A$, the operation $g(x,y) = f(a_1,\dots,\overset{i}{x},\dots,\overset{j}{y},\dots,a_n)$ depends on both of its variables.

THEOREM 2.3. *If* A *satisfies TMS then the following are equivalent.*

(1) Each minimal algebra of A *is polynomially equivalent to a vector space, or each minimal algebra of* A *has exactly two elements and has a 2-element semi-lattice as reduct.*

(2) Each minimal algebra of A *has a quasi-group or quasi-group with* 0 *as reduct.*

(3) Some (equivalently, every) minimal algebra of A *is not essentially unary*

(4) For some $n > 1$ *there exists an* n*-ary polynomial operation* f *of* A *(what Grätzer calls an algebraic operation), which depends on at least two variables, and a set* $B \in M(A)$ *such that* $f({}^nA) \subseteq B$.

Remark: The statement of the theorem is encumbered by our desire to simultaneously get the strongest possible versions of later results, avoid reproving Pálfy's Theorem 1.5, and keep our paper as nearly self-contained as possible. The strongest versions depend on the equivalence of (1) and (4), which depends on Theorem 1.5. Slightly weaker versions, which we will sometimes point out, use the equivalence of (2) and (4), for which we give now a complete, self-contained proof.

Proof. We assume that A satisfies TMS. The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are trivial. And (3) $\Rightarrow$ (4) is easy; if $B \in M(A)$, and $f \in \mathrm{Pol}_n A$ is such that $f(^nB) \subseteq B$, and $f|_B$ depends on at least two variables, then, choosing $e = e^2 \in \mathrm{Pol}_1 A$ with $e(A) = B$ (by 1.3(2)), we have that range $ef \subseteq B$ and ef is not essentially unary.

Our proof that (2) implies (1) is short, using Theorem 1.5. Let (2) hold, so that the minimal algebras are not essentially unary. By Theorem 1.5, either each minimal algebra has its clone, $(\mathrm{Pol}\ A)|_B$, identical to the polynomial clone of a vector space, or else the minimal sets are 2-element sets. Suppose the latter. Let B be any minimal set, and $C = (\mathrm{Pol}\ A)|_B$.

Recall that 2-element semi-lattices and 2-element quasi-groups with 0 are the same thing. So we can assume that C does not contain the binary operation of a quasi-group with 0, but does contain the operation of a quasi-group. Since $|B| = 2$, and C contains the two constant functions, it is easy to see that C contains the polynomial clone of a 2-element vector space V. Now it is known that $\mathrm{Pol}\ V$ is a maximal clone. So either $C = \mathrm{Pol}\ V$, or C contains all possible operations. In either event, we get that (1) holds. Thus (1) and (2) are equivalent.

Now we prove that (4) implies (2), which will give the equivalence of (2), (3) and (4). Let f be an n-ary polynomial operation of A, $f(^nA) \subseteq B$, $B \in M(A)$, and f not essentially unary. By Exercise 2.2, we can arrange that $n = 2$. We now choose $c,d \in A$ such that $g(x) = f(x,d)$ and $h(x) = f(c,x)$ are not constant on A. Then, by 1.3(8) and 1.3(7), we choose $\alpha_0, \alpha_1 \in \mathrm{Pol}_1 A$ so that $g(\alpha_0(x))$ and $h(\alpha_1(x))$ are one-to-one on B. We define, for any $x,y \in A$,

$$(f_0)^y(x) = f_0(x,y) = f(\alpha_0(x),y) \quad ,$$
$$(f_1)_x(y) = f_1(x,y) = f(x,\alpha_1(y)) \quad .$$

Thus $(f_0)^d$ and $(f_1)_c$ are permutations of B.

Consider first the case when $(f_0)^y$ and $(f_1)_x$ are permutations of B for all $x,y \in A$. In this case, $f(\alpha_0(x),\alpha_1(y))$ restricted to B is obviously a quasi-group operation. Thus $A|_B$ (and, by 1.6, every minimal algebra of A) has a quasi-group reduct. So we are done, in this case.

Consider now the case when $(f_0)^y$ fails to be one-to-one on B, for some $y \in A$. (The symmetric assumption for $(f_1)_x$ yields a symmetric argument.) Then by 1.3(5) and 1.3(6) we can assume that there is $D \in M(A)$ with $d,d' \in D$, and $(f_0)^d$ is a permutation on B, while $(f_0)^{d'}$ is constant on B (take $U = \{y : (f_0)^y|_B \text{ is one-to-one}\}$ in

1.3(5), and use that every unary polynomial function is one-to-one or constant on B, by 1.3(6)). Choosing $\alpha_2 \in \mathrm{Pol}_1 A$ with $\alpha_2(B) = D$, we now define $q(x,y) = f(\alpha_0(x),\alpha_2(y))$ for $x,y \in B$. This q is a binary operation of the minimal algebra $A|_B$. We define (for $x,y \in B$)

$$q_x(y) = q(x,y) = q^y(x) \quad ,$$

and we note that each q_x, and each q^y, is either constant or a permutation of B. Letting $v,v' \in B$ be such that $\alpha_2(v) = d$, $\alpha_2(v') = d'$, we have that

$$q^v = (f_0)^d|_B \text{ is one-to-one} \quad ,$$
$$q^{v'} = (f_0)^{d'}|_B \text{ is constant} \quad .$$

We set 0 = the only value of $q(x,v')$; and set u' = the x such that $q(x,v) = 0$. Now $q(u',v) = 0 = q(u',v')$, implying that $q_{u'}$ is constant. For $u \in B-\{u'\}$, we have $q(u,v) \neq q(u',v) = 0 = q(u,v')$, implying that q_u is a permutation. Again, letting $w \in B-\{v'\}$, and choosing any $u \in B-\{u'\}$, $q(u,w) \neq q(u,v') = 0 = q(u',w)$, implying that q^w is a permutation.

So we have

$$q(u',y) = 0 = q(x,v') \text{ for all } x,y \in B \quad ;$$
$$q_u \text{ and } q^w \text{ are permutations when } u \neq u',\ w = v' \quad .$$

If $u' = 0 = v'$, then it follows from the above that $\langle B,q\rangle$ is a quasi-group with 0, as desired. If $u' \neq 0 \neq v'$, then there are $a \neq v' \neq b$ such that $q(0,a) = u'$, $q(0,b) = v'$. For the operation $\bar{q}(x,y) = q(q(x,a),q(y,b))$ it is easy to see that $\langle B,\bar{q}\rangle$ is a quasi-group with 0. If, say, $u' = 0 \neq v'$, then choose $a \neq 0$ with $q(a,0) = v'$, and set $\bar{q}(x,y) = q(x,q(a,y))$. Again, $\langle B,\bar{q}\rangle$ is a quasi-group with 0. This finishes the argument. □

Notice that the second alternative of statement (1) in the theorem can hold only if A is a simple algebra, while the first alternative implies that the minimal algebras of A do not have quasi-groups with 0 as reducts. Thus the last paragraphs of the proof yield this additional result.

PROPOSITION 2.4. *Suppose that A satisfies TMS and is not simple. Let $B \in M(A)$ and $f \in \mathrm{Pol}_2 A$. Then either f^y is one-to-one on B for all $y \in A$, or f^y is constant on B for all $y \in A$.*

We now consider algebras satisfying TMS which do not satisfy the equivalent statements of Theorem 2.3. Here is a property of operations that characterizes this situation.

Definition 2.5. An n-ary operation f on a set A is said to *satisfy TC** (or *the strong term condition*) iff for each i, $0 \leq i < n$, and for all $u,v,a_0 b_0 c_0,\dots,a_{n-1},b_{n-1},c_{n-1} \in A$, the following implication holds:

$$f(a_0,\dots,a_{i-1},u,a_{i+1},\dots,a_{n-1}) = f(b_0,\dots,b_{i-1},v,b_{i+1},\dots,b_{n-1}) \rightarrow$$
$$f(c_0,\dots,c_{i-1},u,c_{i+1},\dots,c_{n-1}) = f(c_0,\dots,c_{i-1},v,c_{i+1},\dots,c_{n-1}) \quad .$$

We say that a clone C over A satisfies TC* iff every $f \in C$ satisfies TC*; and that an algebra $A = \langle A,\dots\rangle$ satisfies TC* iff Pol A satisfies TC*.

This property can also be defined rather differently.

LEMMA 2.6. *An* n-*ary operation* f *over* A *satisfies TC* iff there exist equivalence relations* $R_0^f,\dots,R_{n-1}^f$ *over the set* A *(uniquely determined by* f) *such that for all* $\bar{a},\bar{b} \in {}^nA$,

$$f(\bar{a}) = f(\bar{b}) \leftrightarrow \bigwedge_0^{n-1} (a_i,b_i) \in R_i^f \quad .$$

The proof of this lemma is quite easy, and we omit it. TC* is related to the term condition studied in [1] and [14], which we now define.

Definition 2.7. An n-ary operation f on a set A is said to *satisfy TC* (or the *term condition*) iff for each i, $0 \leq i < n$, and for all $u,v,a_0,b_0,\dots,a_{n-1},b_{n-1} \in A$, the following bi-implication holds:

$$f(a_0,\dots,a_{i-1},u,a_{i+1},\dots,a_{n-1}) = f(b_0,\dots,b_{i-1},u,b_{i+1},\dots,b_{n-1}) \leftrightarrow$$
$$f(a_0,\dots,a_{i-1},v,a_{i+1},\dots,a_{n-1}) = f(b_0,\dots,b_{i-1},v,b_{i+1},\dots,b_{n-1}) \quad .$$

We say that a clone C over A satisfies TC iff every $f \in C$ satisfies TC; and that an algebra $A = \langle A,\dots\rangle$ satisfies TC iff Pol A satisfies TC.

Exercise 2.8. TC* implies TC, for operations, clones, and algebras. A clone C satisfies TC* (or TC) iff the clone generated by $C \cup \{\text{constants}\}$ does; thus an algebra A satisfies TC* (or TC) iff Clo A (the clone of term operations of A) does.

Notice that unary algebras satisfy TC*. Modules satisfy TC, but a non-trivial module cannot satisfy TC*. From a theorem of C.Herrmann, reproved in [14], it follows that a non-trivial algebra in a congruence modular variety cannot satisfy TC*. The next theorem is very important for us.

THEOREM 2.9. *Suppose that an algebra* A *satisfies TMS. Then the minimal algebras of* A *are essentially unary iff* A *satisfies TC*.*

Proof. Let A satisfy TMS. Suppose, first, that A satisfies TC*. Then each minimal algebra $A|_B$ obviously satisfies TC^*. A quasi-group or quasi-group with 0 evidently cannot satisfy TC^*, if it has more than one element. Thus statement (2) of Theorem 2.3 fails, and consequently (3) fails also. The minimal algebras are essentially unary.

Now suppose that the minimal algebras are essentially unary, and let $f \in \mathrm{Pol}_n A$. Suppose that $u,v \in A$ and $\bar{a},\bar{b},\bar{c} \in {}^{n-1}A$ are such that $f(u,\bar{c}) \neq f(v,\bar{c})$. By Proposition 1.3(3), there are $B \in M(A)$, $\alpha \in \mathrm{Pol}_1 A$ such that $\alpha(A) = B$ and $\alpha f(u,\bar{c}) \neq \alpha f(v,\bar{c})$. By Theorem 2.3 (the equivalence of (3) and (4)), the operation $f'(\bar{x}) = \alpha f(\bar{x})$ is essentially unary. Since $f'(u,\bar{c}) \neq f'(v,\bar{c})$, the one argument that f' depends on must be the first. Thus $f'(u,\bar{a}) = f'(u,\bar{c}) \neq f'(v,\bar{c}) = f'(v,\bar{b})$, implying that $f(u,\bar{a}) \neq f(v,\bar{b})$.

So we have that $f(u,\bar{a}) = f(v,\bar{b}) \rightarrow f(u,\bar{c}) = f(v,\bar{c})$. The same argument works for each of the n arguments of f, showing that f satisfies TC^*. □

If P is any property of algebras, we shall say that a lattice L *forces* P provided that for every algebra A, $\mathit{Con}\ A \cong L$ implies A has the property P. (Recall that "lattice" means "finite lattice," and "algebra" means "finite algebra" in this paper.)

THEOREM 2.10. *Let L be any lattice such that the two conditions of Theorem 1.9 hold for L, and for no non-trivial vector space V is $\mathit{Sub}\ V$ a homomorphic image of L. Then L forces TC^*.*

Proof. If L is a 1-element lattice, it certainly forces TC^*. Suppose that L satisfies our hypotheses, has more than one element, and $\mathit{Con}\ A \cong L$. Then by Theorem 1.9, A satisfies TMS. Let B be any minimal set of A. By Proposition 1.3(2) and Lemma 1.7, we have a lattice homomorphism of $\mathit{Con}\ A$ onto $\mathit{Con}\ A|_B$. Thus $A|_B$ cannot be polynomially equivalent to a vector space. (The congruence and subspace lattices of a vector space are isomorphic.) Also, $|B| > 2$, because $|B| = 2$ would imply that A is simple, i.e. $L \cong 2$; but then L would be isomorphic to $\mathit{Sub}\ V$ for a 2-element V. So statement (1) of Theorem 2.3 fails for A, and A satisfies TC^*, by Theorems 2.3 and 2.9. □

We proceed to note some immediate consequences, and some easy extensions, of the last theorem.

THEOREM 2.11. *Let L be any simple lattice, not isomorphic to the subspace lattice of a vector space, such that the co-atoms of L intersect to 0. Then L forces TC^*. Moreover, if A is any algebra and $\mathit{Con}\ A \cong L$, then every homomorphic image of A satisfies TC^*.*

Proof. It is obvious from the remark after Theorem 1.9 that the hypotheses on L in this theorem imply those in the last theorem. Thus L forces TC^*.

Now let $Con\ A \cong L$ and $\theta \in \mathrm{Con}\ A$. It must be shown that for every $f \in \mathrm{Pol}_n A$ and $u,v \in A$, $\bar{a},\bar{b},\bar{c} \in {}^{n-1}A$, that $f(u,\bar{c}) \not\equiv_\theta f(v,\bar{c})$ implies $f(u,\bar{a}) \not\equiv_\theta f(v,\bar{b})$. So suppose that $(f(u,\bar{c}),f(v,\bar{c})) \notin \theta$. Choose a minimal set B of A. Since $Con\ A$ is simple, π_B is an isomorphism in Lemma 1.7. Thus $\theta = \widehat{\pi_B\theta}$. So there exists an $\alpha \in \mathrm{Pol}_1 A$, $\alpha(A) \subseteq B$, such that $\alpha f(u,\bar{c}) \not\equiv_\theta \alpha f(v,\bar{c})$. By 2.3 and 2.9 (and because A satisfies TC*), αf is essentially unary. Then the computation in the proof of Theorem 2.9 shows that $f(u,\bar{a}) \not\equiv_\theta f(v,\bar{b})$. □

It follows from the last theorem that the lattice E_n of all equivalence relations on an n-element set, $n \geq 4$, forces TC*, and so does the dual of E_n. Likewise, the height two lattices M_n, for $n \geq 3$, n not the successor of a prime power, force TC*. A simple observation allows us to greatly extend the class of lattices known to force TC*.

By an *interval* in a lattice L we mean a sublattice whose universe is of the form $u/v = \{x \in L\colon v \leq x \leq u\}$ for some $v \leq u$ in L. Such a sublattice will simply be denoted as u/v.

THEOREM 2.12. *Each of these conditions implies that* L *forces TC*.*

(1) $L \cong L_0 \times \dots \times L_k$ *and* L_i *forces TC* for* $i = 0,\dots,k$.

(2) In L *there exist* $v_0,\dots,v_k$ *such that* $\bigwedge_0^k v_i = 0$ *and the lattice* $1/v_i$ *forces TC* for* $i = 0,\dots,k$.

Proof. (1) implies (2), so we focus our attention on (2). Suppose that $v_0,\dots,v_k$ in L satisfy (2), and that $Con\ A \cong L$. So we have $\theta_0,\dots,\theta_k$ in $Con\ A$ satisfying (2). This means that A is a subdirect product of the algebras A/θ_i, and since $Con\ A/\theta_i \cong 1/\theta_i$, these algebras satisfy TC*. Now this theorem follows from the easy observation that subdirect products preserve the satisfaction of TC*. □

We conclude this section with two remarks. The first remark is that results somewhat weaker than Theorems 2.10 and 2.11, but not depending on Theorem 1.5 for their proof, are obtained by replacing the class of subspace lattices of vector spaces by the class of congruence lattices of algebras having a quasi-group or quasi-group with 0 as a reduct. (By Exercise 2.1, this is still a quite restricted class of lattices.)

The second remark is that although M_n, for $n = 1 + p^k$, p a prime, certainly does not force TC*, it has recently been proved by David Hobby that every M_n, $n \geq 3$, forces TC.

3. LATTICES OF SUBVARIETIES

In this section, we find that some remarkable conclusions about the lattices of subvarieties of locally finite varieties of algebras are easy consequences of results in the last section. Perhaps the most remarkable fact, following from Hobby's result mentioned at the close of that section, is that for no locally finite variety V is $L(V) \cong M_\lambda$, $\lambda \geq 3$.

In this section, we do not follow the convention that all mentioned algebras are finite. However, the phrase "L forces P" will continue to have the same meaning as in the last section, namely, that L is a finite lattice such that for every finite algebra A, $Con\ A \cong L$ implies that A satisfies the property P.

Recall that a variety V of algebras is termed *locally finite* iff the V-free algebras $F_V(n)$ are finite for all finite n. $L(V)$ denotes the lattice of all subvarieties of V. The dual of a lattice L is denoted by L^∂. It is well known that $L(V)^\partial$ is isomorphic to the lattice of all fully invariant congruences of $F_V(\omega)$. (A congruence $\theta \in$ Con A is *fully invariant* iff $(x,y) \in \theta$ implies $(s(x),s(y)) \in \theta$, for all endomorphisms s of A and for all $x,y \in A$.) The lattice of fully invariant congruences of an algebra A will be denoted by *I-Con A*.

If a variety V is finitely generated, i.e. if $V = V(A)$ for some finite algebra A, then V is locally finite. If $L(V)$ is finite, and if V is locally finite, then V is finitely generated (since $V = \bigvee_{n<\omega} V(F_V(n))$ and $V(F_V(1)) \leq V(F_V(2)) \leq \ldots$) However, $L(V)$ is not always finite, for finitely generated V.

LEMMA 3.1. *Let V be any variety such that $L(V)$ is finite. For large* $n < \omega$, *$L(V)^\partial$ is isomorphic to the lattice I-$Con\ F_V(n)$.*

Proof. Since $L(V)$ is finite, there is n such that whenever $W,W' \in L(V)$ and $W' \nleq W$, there is an n-variable identity that is valid in W and not valid in W'. Let $L = I\text{-}Con\ F_V(n)$. For each $W \in L(V)$, let θ_W be the smallest congruence θ on $F_V(n)$ satisfying $F_V(n)/\theta \in W$. Then $\theta_W \in L$; θ_W is the kernel of the natural homomorphism of $F_V(n)$ onto $F_W(n)$. By the choice of n, $\theta_W = \theta_{W'}$ iff $W = W'$. Moreover, $\theta_W \subseteq \theta_{W'}$ iff $W' \leq W$. To see that $W \mapsto \theta_W$ is onto L, let θ be any member of L, and let $W = V(F_V(n)/\theta)$. Now $\theta_W \subseteq \theta$, obviously. If $\theta_W < \theta$, then any pair $(u,v) \in \theta - \theta_W$ represents an identity that holds in $F_V(n)/\theta$, due to the full invariance of θ, and does not hold in W because it does not hold in $F_V(n)/\theta_W$. This contradicts the definition of W. So we conclude that $\theta = \theta_W$. □

Definition 3.2. Let F be the universe of a V-free algebra, $F_V(n)$, freely generated by elements $x_1,\ldots,x_n$. We define an n+1-ary operation, *sub*, on F. For $\sigma,\mu_1,\ldots,\mu_n \in F$ we put $sub(\sigma,\mu_1,\ldots,\mu_n) = s(\sigma)$ where s is the unique endomorphism of $F_V(n)$ which sends x_i to μ_i, $1 \leq i \leq n$. (More suggestively: $sub(\sigma,\mu_1,\ldots,\mu_n) = \sigma(\mu_1,\ldots,\mu_n)$.) We now form two algebras, $F_V^s(n) = \langle F, sub\rangle$ and $F_V^*(n)$. The latter algebra is $F_V(n)$ with all its operations together with the n+1-ary operation *sub*.

LEMMA 3.3.
i) For any V, I-Con $F_V(n)$ = Con $F_V^*(n)$.
ii) If the fundamental operations in V are all of rank $\leqslant n$, then I-Con $F_V(n)$ = Con $F_V^s(n)$.

Proof. For fixed $\mu_1,\ldots,\mu_n \in F$, $s^{\bar{\mu}}(u) = sub(u,\mu_1,\ldots,\mu_n)$ is an endomorphism of $F_V(n)$. Moreover, every endomorphism has this form, so they are all polynomials (what Grätzer calls algebraic functions) in each of the new algebras. And every operation of $F_V(n)$ having rank $\leqslant n$ can be expressed as $f(\mu_1,\ldots,\mu_m) = sub(\phi,\mu_1,\ldots,\mu_m,x_{m+1},\ldots,x_n)$ with $\phi = f(x_1,\ldots,x_m) \in F$; so all such operations are polynomial operations of $F_V^s(n)$.

Since congruences are closed under all polynomials, the rest of the proof is easy. (It is trivial to see that invariant congruences of $F_V(n)$ are closed under *sub*.) □

LEMMA 3.4. *Suppose that V is a locally finite variety, $L(V)$ is finite, and $L(V)^\partial$ forces TC. Then V is a variety of trivial algebras and $L(V) \cong 1$.*

Proof. Choose $n \geqslant 2$ so large that (by Lemmas 3.1 and 3.3), $L(V)^\partial \cong$ I-Con $F_V(n) \cong$ Con $F_V^*(n)$. $F_V^*(n)$ is a finite algebra, so it must satisfy TC. Let $x_1,\ldots,x_n$ be the free generating elements, in terms of which *sub* was defined. Now $sub(x_1,x_1,x_1,\ldots,x_1) = sub(x_1,x_1,x_2,\ldots,x_2)$. By TC (see Definition 2.7) we can replace x_1 at the first place in this equation by any other member of $F_V(n)$. In particular, replacing by x_2, we obtain the equation $x_1 = x_2$. This simply means that $F_V^*(n)$ is a one-element algebra and $L(V)$ is a one-element lattice. □

THEOREM 3.5. *Let L be any lattice such that for some $u<1$ in L, the interval lattice $1/u$ is finite and forces TC. Then L^∂ is not isomorphic to $L(V)$ for any locally finite variety V.*

Proof. If $L(V) \cong L^\partial$, then for some variety $V' \subseteq V$, $L(V')^\partial \cong 1/u$. So the theorem follows by the preceding lemma. □

That the class of finite lattices satisfying the hypotheses of the last theorem is quite a large class, is amply demonstrated by Theorems 2.10, 2.11, 2.12. However, all the lattices that force TC, by our theorems, also force the stronger TC*. Now D.Hobby has proved that the class of lattices that force TC is a good deal more extensive than the subclass that force TC*. He proved, in particular, that L forces TC whenever L is a finite simple lattice, $|L| \geqslant 3$, and the co-atoms in L intersect to 0. The next two theorems are a consequence of this result of his and Theorem 3.5.

THEOREM 3.6. *Let* L *be any lattice such that for some* u *in* L, *the interval lattice* $u/0$ *is finite and simple and has at least three elements, and* u *is a join of atoms in* L. *There does not exist any locally finite variety* V *with* $L \cong L(V)$.

A variety V is called *equationally complete* iff $|L(V)| = 2$; and called *equationally pre-complete* iff $L(V) \cong M_\lambda$ for some cardinal $\lambda \geqslant 1$.

THEOREM 3.7. *An equationally pre-complete locally finite variety has at most two equationally complete subvarieties.*

Proof. Let V be equationally pre-complete and locally finite, and assume that V has more than two equationally complete subvarieties. Thus $L(V) \cong M_\lambda$ for some cardinal $\lambda \geqslant 3$. By Theorem 3.6, it is forbidden that λ be finite and $\geqslant 3$. So λ is infinite. Let $F = F_V(2)$, a non-trivial finite algebra, V-freely generated by two elements x and y. Let $W_0, W_1, \ldots$ be an infinite list of distinct atoms of $L(V)$. As in the proof of Lemma 3.1, let θ_i be the smallest congruence θ of F with $F/\theta \in W_i$. Now $\theta_i \vee \theta_j = 1_F$ for $i \neq j$, since $F/(\theta_i \vee \theta_j) \cong (F/\theta_i)/((\theta_i \vee \theta_j)/\theta_i) \in W_i \cap W_j$. And $\theta_i \wedge \theta_j = 0_F$, $i \neq j$; for if $(\mu(x,y), \nu(x,y)) \in \theta_i \wedge \theta_j$, then the identity $\mu \approx \nu$ holds in both W_i and W_j, hence in $W_i \vee W_j = V$, and so $\mu(x,y) = \nu(x,y)$.

It is impossible for a finite non-trivial lattice to have an infinite sequence $(\theta_i)_{i<\omega}$ of elements as above. But *Con F* is certainly a finite non-trivial lattice. So we have a contradiction, proving the theorem. □

4. IMPLICATIONS OF TC*

The convention that all mentioned algebras are finite is followed in this section. Our purpose here is to develop a complete description of all algebras $A = \langle A,f \rangle$ which have tame minimal sets, satisfy the strong term condition, and have just one basic operation. It turns out that either f is constant, or $\langle A, \mathrm{Clo}\, A \rangle$ is isomorphic to a [k]-th power of a non-indexed algebra $\langle U,C \rangle$ where C is a clone generated by a single permutation $\sigma \in \mathrm{Sym}\, U$. From this result, coupled with the earlier results, we shall be able to quickly delineate a broad class of finite lattices that cannot be represented as the congruence lattice of a finite algebra with one operation.

Let us recall a few concepts and results relating to clones. Two algebras $A = \langle A, \ldots \rangle$ and $B = \langle B, \ldots \rangle$ are called *equivalent* iff their underlying sets are equal and $\mathrm{Clo}\, A = \mathrm{Clo}\, B$. (This definition makes sense, and we use it, even in case A is an indexed algebra and B is non-indexed.) A and B are called *weakly isomorphic* iff the non-indexed algebras $\langle A, \mathrm{Clo}\, A \rangle$ and $\langle B, \mathrm{Clo}\, B \rangle$ are isomorphic, i.e. iff there is a bijection from A onto B which carries $\mathrm{Clo}\, A$ onto $\mathrm{Clo}\, B$. The *non-indexed product* of A and B is $\langle A, \mathrm{Clo}\, A \rangle \times \langle B, \mathrm{Clo}\, B \rangle = \langle A \times B, C \rangle$ where C consists of all operations on A×B which act co-ordinatewise, and act like a member of $\mathrm{Clo}\, A$

in the first co-ordinate, like a member of Clo$B$ in the second. Notice that C is a clone.

Let $1 \leqslant k < \omega$. The [k]-th power of A is the algebra $\langle {}^kA, C\rangle$ where C consists of all operations f such that, if f is n-ary, there exist $f_0, \ldots, f_{k-1} \in \mathrm{Clo}_{nk} A$ satisfying (for all $\bar{x}^0, \ldots, \bar{x}^{n-1} \in {}^kA$):

(4.1) $$f(\bar{x}^0, \ldots, \bar{x}^{n-1}) = (f_0(\bar{y}), \ldots, f_{k-1}(\bar{y})) \quad , \text{ where}$$
$$\bar{y} = (x_0^0, \ldots, x_{k-1}^0, \ldots, x_0^{n-1}, \ldots, x_{k-1}^{n-1}) = \bar{x}^{0\frown} \bar{x}^{1\frown} \cdots {}^\frown \bar{x}^{n-1} .$$

This non-indexed algebra $\langle {}^kA, C\rangle$ is denoted by $A^{[k]}$.

Three special operations of $A^{[k]}$ are particularly interesting.

(4.2) For $\bar{x}, \bar{y}, \bar{x}^0, \ldots, \bar{x}^k$ in ${}^kA$, define
$$d_k(\bar{x}^0, \ldots, \bar{x}^{k-1}) = (x_0^0, x_1^1, \ldots, x_{k-1}^{k-1}) ,$$
$$p_k(\bar{x}) = (x_{k-1}, x_0, x_1, \ldots, x_{k-2}) ,$$
$$b_k(\bar{x}, \bar{y}) = (y_{k-1}, x_0, \ldots, x_{k-2}) .$$

PROPOSITION 4.3. *Let A, B be algebras, $1 \leqslant k < \omega$.*

(1) If A is an indexed algebra, then $A^{[k]}$ is equivalent to the algebra $({}^kA, d_k, p_k)$ consisting of the ordinary k*-th direct power of A and its operations, together with the operations d_k and p_k. $A^{[k]}$ is also equivalent to $({}^kA, b_k)$.*

(2) $A^{[k]} = \langle A, \mathrm{Clo}\, A\rangle^{[k]}$, and the k*-fold non-indexed power of A is a reduct of $A^{[k]}$.*

(3) $Con(\langle A, \mathrm{Clo}\, A\rangle \times \langle B, \mathrm{Clo}\, B\rangle) \cong Con\, A \times Con\, B$, while $Con\, A^{[k]} \cong Con\, A$.

(4) Any algebra $A' = \langle {}^kA, \ldots\rangle$ with universe ${}^kA$ is equivalent to $A^{[k]}$ iff: the operations d_k and p_k belong to Clo A' *(equivalently, b_k belongs), and* Clo A *is identical with the clone generated by all operations of the form $g(x_0^0, \ldots, x_{k-1}^{n-1}) = \pi f(\bar{x}^0, \ldots, \bar{x}^{n-1})$, where $f \in \mathrm{Clo}_n A'$, n is arbitrary, and π is one of the* k *projections of ${}^kA$ to* A.

Proof. These facts are easily verified, and in any case are well-known. The reader is referred to W.Taylor [13] for more information about [k]-th powers. □

In [5], we used [k]-th powers to show that for any algebra A with finitely many basic operations, $Con\, A$ is congruence representable with a binary and unary operation. In fact, if A has $\leqslant k$ basic operations, and these have rank $\leqslant k$, then $A^{[k]}$ has its clone generated by the binary operation b_k and one unary operation, and $Con\, A \cong Con\, A^{[k]}$ by statement (3) in the above proposition. Here we shall use [k]-th powers for the opposite purpose, to facilitate a proof that one operation does not suffice for congruence lattice representations with finite algebras.

Recall the properties TC* and TC defined in Definitions 2.5 and 2.7. We now have several constructions available for producing algebras satisfying these properties. The next theorem is fairly obvious.

THEOREM 4.4. *The class of algebras satisfying TC* contains all multi-unary algebras, and is closed under weak isomorphism, and under the formation of reducts, direct products (of similar indexed algebras), non-indexed products,* [k]*-th powers, subalgebras, and direct factors. The class of algebras satisfying TC also has these properties.*

Among the simplest examples of algebras satisfying TMS and TC* are the permutation groups (algebras of the form $\langle A,G\rangle$ with G a subgroup of Sym A). From them, we get the basic examples for this section.

THEOREM 4.5.
(1) If $F \subseteq \mathrm{Sym}\,A$, $|A|>1$, *and* $1 \leqslant k < \omega$, *then* $\langle A,F\rangle^{[k]}$ *satisfies TMS and TC*.*
(2) If $f \in \mathrm{Sym}\,A$, *and* $1 \leqslant k < \omega$, *then* $\langle A,f\rangle^{[k]}$ *is equivalent to an algebra* $\langle {}^kA,b\rangle$ *with one binary operation.*

Proof. We first tackle (2). Let $f \in \mathrm{Sym}\,A$. We claim that the clone $C = \mathrm{Clo}\,\langle A,f\rangle^{[k]}$ is generated by the operation b defined as

$$b(\bar{x},\bar{y}) = (fy_{k-1},x_0,\ldots,x_{k-2}) \quad .$$

It is obvious that $b\in C$. Defining $q(\bar{x}) = b(\bar{x},\bar{x})$ and $f'(\bar{x}) = q^k(\bar{x})$ (i.e. q iterated k times), we have that $f'((x_0,\ldots,x_{k-1})) = (fx_0,\ldots,fx_{k-1})$; i.e. f' is the basic operation of the direct power algebra ${}^k\langle A,f\rangle$. By Proposition 4.3(1), C is generated by f' together with b_k. Since A is finite, we can choose $n>1$ such that $f^n = \mathrm{id}_A$. Then we can check that $b_k(\bar{x},\bar{y}) = (f')^{n-1}(b(f'(\bar{x}),\bar{y}))$. Thus b generates the entire clone C.

Now we tackle (1). Let $F \subseteq \mathrm{Sym}\,A$, $|A|>1$, $A' = \langle A,F\rangle^{[k]}$. Since the algebra A' depends only on the clone of $\langle A,F\rangle$, we can suppose that F is a subgroup of Sym A. That A' satisfies TC* is a part of Theorem 4.4. To see that A' satisfies TMS we use Definition 1.2, and we put $B = \{(x,\ldots,x)\colon x \in A\}$. B is obviously the range of a polynomial function of A'. We show that B is a minimal set of A' satisfying 1.2(i) and 1.2(ii).

Suppose that $\alpha \in \mathrm{Pol}_1 A'$ and $\alpha({}^kA) \subseteq B$. We wish to show that either $\alpha({}^kA) = B$, or α is constant. We can find $h \in \mathrm{Clo}_n A'$ for some $n\geqslant 1$, and $\bar{a}^1,\ldots,\bar{a}^{n-1} \in {}^kA$, such that α is the function $\alpha(\bar{x}) = h(\bar{x},\bar{a}^1,\ldots,\bar{a}^{n-1})$. Now the clone of A' consists of all operations of the form (4.1). Since $\mathrm{Clo}\langle A,F\rangle$ consists of all operations of the form $t(x_0,\ldots,x_{u-1}) = f(x_j)$ for some $f\in F$ and some $j<u$, we have that $\alpha(\bar{x}) = (f_0(\varepsilon_0),\ldots,f_{k-1}(\varepsilon_{k-1}))$ with each $\varepsilon_j \in \{x_0,\ldots,x_{k-1},a^1_0,\ldots,a^{n-1}_{k-1}\}$ and $f_0,\ldots,f_{k-1} \in F$. The only way it can happen that $\alpha({}^kA) \subseteq B$ and α is not constant,

is if all ε_j are chosen from among the components of $\bar{x}$, and in fact all are the same component of $\bar{x}$. Thus we can assume that $\alpha(\bar{x}) = (f_0(x_j),\dots,f_{k-1}(x_j))$ for a certain $j < k$, and for all $\bar{x}$. Again, $\alpha({}^kA) \subseteq B$ implies $f_0 = \dots = f_{k-1}$, and then clearly $\alpha({}^kA) = B$. So we have proved that $B \in M(A')$.

Let $\bar{u},\bar{v} \in {}^kA$, $\bar{u} \neq \bar{v}$. For some $j < k$, $u_j \neq v_j$. Clearly, $\alpha(\bar{x}) = (x_j,\dots,x_j)$ defines a polynomial function of A' such that $\alpha(\bar{u}) \neq \alpha(\bar{v})$ and $\alpha({}^kA) = B$. Thus 1.2(i) holds for this B.

For each $j < k$ and $a_0,\dots,a_{j-1},a_{j+1},\dots,a_{k-1} \in A$, the operation $\alpha(\bar{x}) = (a_0,\dots,a_{j-1},x_j,a_{j+1},\dots,a_{k-1})$ is in $\mathrm{Pol}_1 A'$. The sets $\alpha(B)$, α of this form, obviously connect ${}^kA$. So 1.2(ii) holds for this B. □

Up to now, we have been preparing the ground to motivate the principal result of this section, Theorem 4.8. Now we begin the proof of it.

Definition 4.6. An n-ary operation f over A is called *δ-injective* iff the function $f_\delta(x) = f(x,\dots,x)$ is one-to-one.

LEMMA 4.7. *Suppose that* $A = \langle A,f\rangle$ *satisfies TMS and TC*. If* f *is not δ-injective, then it is constant.*

Proof. We suppose that f is n-ary and that f_δ is not one-to-one. Let $a \neq b$, $f_\delta(a) = f_\delta(b)$. Using the notation of Lemma 2.6, we then have that $(a,b) \in \bigcap_0^{n-1} R_i^f$. Now it is easy to prove that for every $\alpha \in \mathrm{Pol}_1 A$, if $\alpha \neq \mathrm{id}_A$ then $\alpha(a) = \alpha(b)$. ($\mathrm{Pol}_1 A$ is the subalgebra of ${}^AA$ generated by the constant functions and the identity function. Lemma 2.6 must be used also in this proof.) By 1.3(3), there is $\alpha \in \mathrm{Pol}_1 A$ such that $\alpha(a) \neq \alpha(b)$ and $\alpha(A)$ is a minimal set. Thus $\alpha = \mathrm{id}_A$, $A \in M(A)$. Then by 1.3(6) every $\alpha \in \mathrm{Pol}_1 A$ is constant or one-to-one. Thus $\mathrm{Pol}_1 A = \{\mathrm{id}_A\} \cup \{\text{constant functions}\}$. Now finally, $R_i^f = 1_A$ for all i, because R_i^f is the kernel of a polynomial function, and $(a,b) \in R_i^f$. Thus f is constant. □

THEOREM 4.8. *Suppose that* $A = \langle A,f\rangle$ *satisfies TMS and TC*. If* f *is not constant, then* A *is weakly isomorphic to an algebra* $\langle U,\sigma\rangle^{[k]}$ *where* $\sigma \in \mathrm{Sym}\, U$.

Proof. We assume, by 4.7, that f is δ-injective. Now we claim that the clone, Clo A, of term operations of A has no essentially n-ary members, if n is large. Indeed, it follows by Lemma 2.6 that if g is an essentially n-ary, n-ary operation in Clo A, then $|A| \geq 2^n$. This is because g induces an injective map of $\Pi(A/R_i^g,\ i < n)$ into A, and $R_i^g < 1_A$ iff g depends on its i-th variable.

Let k be the largest n such that Clo A has an essentially n-ary, δ-injective operation. Let g be a k-ary member of Clo A such that g is δ-injective and essentially k-ary. We assume that $k > 1$, since otherwise f is essentially unary and we are done (as f_δ is a permutation). Choose $n > 1$ such that $g_\delta^n = \mathrm{id}_A$, and put $d(x_0,\dots,x_{k-1}) = g_\delta^{n-1} g(x_0,\dots,x_{k-1})$. This d is essentially k-ary and $d_\delta = \mathrm{id}_A$.

We claim that d satisfies the identities

(1) $d(x,\dots,x) = x$

(2) $d\big(d(x_0^0,\dots,x_{k-1}^0),\dots,d(x_0^{k-1},\dots,x_{k-1}^{k-1})\big) = d(x_0^0,x_1^1,\dots,x_{k-1}^{k-1})$

Indeed, (1) is the equation $d_\delta = id_A$. To prove (2), note first that the k^2-ary operation $\bar{d}$ on the left-side of (2) is δ-injective, in fact, $\bar{d}_\delta = id_A$. Thus, by our assumption, $\bar{d}$ depends on at most k arguments. Suppose that for some i, say $i=0$, $\bar{d}$ is independent of $x_0^i,\dots,x_{k-1}^i$. Then

$$d(x,x_1,\dots,x_{k-1}) = \bar{d}(x,\dots,x,x_1,\dots,x_1,\dots,x_{k-1},\dots,x_{k-1})$$

is independent of x, a contradiction. Thus $\bar{d}$ must depend on exactly one x_j^i, for each $i<k$. Let $x_{j_0}^0,\dots,x_{j_{k-1}}^{k-1}$ be the variables on which $\bar{d}$ depends. Notice that

$$\begin{aligned} d(x_0,\dots,x_{k-1}) &= \bar{d}(x_0,\dots,x_{k-1},\dots,x_0,\dots,x_{k-1}) \\ &= \bar{d}(x_{j_0},\dots,x_{j_0},x_{j_1},\dots,x_{j_1},\dots,x_{j_{k-1}},\dots,x_{j_{k-1}}) \\ &= d(x_{j_0},\dots,x_{j_{k-1}}) \ . \end{aligned}$$

So $i \to j_i$ must be a permutation π of $\{0,\dots,k-1\}$. (Since d depends on all variables.) Now the above computation implies that

$$\bar{d}(x_0^0,\dots,x_{k-1}^{k-1}) = \bar{d}\left(x_{\pi(0)}^0,\dots,x_{\pi(k-1)}^0,\dots,x_{\pi(0)}^{k-1},\dots,x_{\pi(k-1)}^{k-1}\right) \ .$$

If $\pi\pi(i) \neq \pi(i)$ for some i, then the displayed equation implies that $\bar{d}$ does not depend on $x_{j_i}^i$. Thus we can conclude that $\pi(i) = i$ for all i. Then it follows that

$$\begin{aligned} \bar{d}(x_0^0,\dots,x_{k-1}^{k-1}) &= \bar{d}(x_0^0,\dots,x_0^0,x_1^1,\dots,x_1^1,\dots,x_{k-1}^{k-1},\dots,x_{k-1}^{k-1}) \\ &= d(x_0^0,x_1^1,\dots,x_{k-1}^{k-1}) \ , \end{aligned}$$

as was claimed.

There is a classical representation theorem for operations which satisfy the identities (1) and (2). It states that there exists an algebra $\langle A',d'\rangle$ and an isomorphism $\phi\colon \langle A,d\rangle \cong \langle A',d'\rangle$, where $A' = A_0 \times \dots \times A_{k-1}$ for some sets A_i, and d' is the diagonal operation (which was defined in formula (4.2), but only in the case $A_0 = \dots = A_{k-1}$). There is an operation f' with $\phi\colon \langle A,f\rangle \cong \langle A',f'\rangle$. We now replace $\langle A,f\rangle$ by the isomorphic algebra, i.e. we henceforth assume that

(3) $A = A_0 \times \dots \times A_{k-1}$,

$d(\bar{x}^0,\dots,\bar{x}^{k-1}) = (x_0^0,x_1^1,\dots,x_{k-1}^{k-1})$ for any $\bar{x}^0,\dots,\bar{x}^{k-1} \in A$.

Now let us finally examine the basic operation f. Say f is n-ary, and let us define an operation in $\mathrm{Clo}_{nk}A$ by

$$q(x_0^0,\ldots,x_{n-1}^0,\ldots,x_0^{k-1},\ldots,x_{n-1}^{k-1}) = d(f(x_0^0,\ldots,x_{n-1}^0),\ldots,f(x_0^{k-1},\ldots,x_{n-1}^{k-1})) .$$

This q is δ-injective and thus depends on at most k variables, but for each $i<k$ it must depend on at least one of $x_0^i,\ldots,x_{n-1}^i$. For if, say, q were independent of $x_0^0,\ldots,x_{n-1}^0$, then we would have that $d(f_\delta(x_0),\ldots,f_\delta(x_{k-1}))$ is independent of x_0, giving that d is independent of its first variable, since f_δ is a permutation. It follows that for some $j_0,\ldots,j_{k-1}<n$, q depends precisely on $x_{j_0}^0,\ldots,x_{j_{k-1}}^{k-1}$. From this we derive easily the equation $f(x_0,\ldots,x_{n-1}) = d(f_\delta(x_{j_0}),\ldots,f_\delta(x_{j_{k-1}}))$, implying that

(4) $\quad$ Clo A is generated by d and f_δ .

We define one more auxiliary operation.

$$q'(x_0^0,\ldots,x_{k-1}^{k-1}) = d(f_\delta d(x_0^0,\ldots,x_{k-1}^0),\ldots,f_\delta d(x_0^{k-1},\ldots,x_{k-1}^{k-1})) .$$

Consideration of this operation leads, as in the demonstration of (2) above, to the conclusion that for a certain permutation π of $\{0,1,\ldots,k-1\}$, we have the identity

(5) $\quad f_\delta(d(x_0,\ldots,x_{k-1})) = d(f_\delta(x_{\pi 0}),\ldots,f_\delta(x_{\pi(k-1)}))$.

In view of (3), this means that there exist functions $\sigma_0\colon A_{\pi(0)} \to A_0,\ldots,\sigma_{k-1}\colon A_{\pi(k-1)} \to A_{k-1}$ such that

(6) $\quad$ for $\bar{x} = (x_0,\ldots,x_{k-1}) \in A$, $\quad f_\delta(\bar{x}) = (\sigma_0(x_{\pi 0}),\ldots,\sigma_{k-1}(x_{\pi(k-1)}))$.

The σ_i are bijective maps, since f_δ is a permutation of A.

Next we claim that π is a transitive permutation, that is, a cyclic permutation with one orbit. Suppose that this is false. Then we can write $\{0,\ldots,k-1\} = I\cup J$, $I\cap J=\emptyset$, $I\neq\emptyset\neq J$, and $\pi(I)=I$, $\pi(J)=J$. Let $\theta = \{(\bar{x},\bar{y}) \in {}^2A\colon x_i=y_i \text{ for all } i\in I\}$. From (3), (4) and (6), it is easy to see that θ is a congruence of A. Choose any $\bar{a}\in A$ and define $\alpha(\bar{x}) = d(\bar{\varepsilon}_0,\ldots,\bar{\varepsilon}_{k-1})$ with $\bar{\varepsilon}_i=\bar{a}$ for $i\in I$ and $\bar{\varepsilon}_j=\bar{x}$ for $j\in J$. Obviously, $\alpha\in \mathrm{Pol}_1 A$, and α is not constant. Thus $\alpha(A)$ contains a minimal set $B\in M(A)$. But then ${}^2B\subseteq\theta$, implying that $\mathrm{Cg}_A({}^2B) < 1_A$, which contradicts the comment following Definition 1.2.

So π is transitive. We can therefore write $\{0,1,\ldots,k-1\} = \{\ell_0,\ldots,\ell_{k-1}\}$, with $\ell_0=0$. and $\pi(\ell_{j+1}) = \ell_j$ for $j=0,\ldots,k-2$, and $\pi(0)=\ell_{k-1}$. We can use these facts to set up a bijection between ${}^kA_0$ and A. Recall that σ_ℓ (in (6)) is a bijection of $A_{\pi(\ell)}$ onto A_ℓ. Thus for $j=1,\ldots,k-1$, $\beta_j = \sigma_{\ell_j}\sigma_{\ell_{j-1}}\cdot\ldots\cdot\sigma_{\ell_1}$ is a bijection of A_0 onto A_{ℓ_j}. A bijection of ${}^kA_0$ onto A is defined by setting, for $\bar{a}\in {}^kA_0$, $\phi(\bar{a}) = (c_0,\ldots,c_{k-1})$ with $c_0=a_0$ and for $1\leqslant j<k$, $c_{\ell_j} = \beta_j(a_j)$. We have a unique algebra $\langle {}^kA_0,f',d',f'_\delta\rangle$ isomorphic to $\langle A,f,d,f_\delta\rangle$ under ϕ. Moreover, $\mathrm{Clo}\langle {}^kA_0,f'\rangle = \mathrm{Clo}\langle {}^kA_0,d',f'_\delta\rangle$, since this holds for the isomorphic algebra.

The structure of the operations d' and f'_δ can be determined. We write down their definitions in the next formulas, and leave the verification to the reader.

(7) $\quad d'(\bar{a}^0,\dots,\bar{a}^{k-1}) = d_k(\bar{a}^0,\bar{a}^{\ell_1},\dots,\bar{a}^{\ell_{k-1}})$, and

$$f'_\delta((a_0,\dots,a_{k-1})) = (\sigma(a_{k-1}),a_0,a_1,\dots,a_{k-2})$$

where d_k is the diagonal operation on ${}^kA_0$, defined in formula (4.2), and $\sigma \in \mathrm{Sym}\, A_0$ is $\sigma_0\beta_{k-1}$.

The operations d' and f' obviously belong to the clone of $A' = \langle A_0,\sigma\rangle^{[k]}$. So $\langle {}^kA_0,f'\rangle$ is a reduct of A'. On the other hand, d_k is obtained from d' by permuting the variables, and the binary operation in the proof of 4.5(2) is expressible as $b(x,y) = f'_\delta d_k(x,\dots,x,y)$. Thus A' is equivalent to $\langle {}^kA_0,f'\rangle$, and weakly isomorphic to $\langle A,f\rangle$. This concludes the proof. □

In the proof of the theorem, excluding the helping Lemma 4.7, TC* was invoked only in the first paragraph, to get a bound on the essential arity of term operations. TMS was used only to conclude that π is transitive; but the argument showed that the orbits of π induce factor congruence relations on A in any case. We should point out that this argument is modeled on a proof of J.Płonka's characterization of idempotent algebras having no term operations of large essential arity (his "k-dimensional diagonal algebras"). The argument, with minor revisions, will prove the following theorem. We omit the proof because the result is peripheral to our main concerns.

Finiteness is an implicit assumption of this theorem.

THEOREM 4.9. *The following are equivalent, for any algebra* A.

(1) The clone of term operations, Clo A, *is generated by* δ*-injective operations, and there is a bound on the essential arities of operations in this clone.*

(2) A *is weakly isomorphic to a non-indexed product of algebras of the form* $\langle U,F\rangle^{[k]}$, $F \subseteq \mathrm{Sym}\, U$.

Either of these statements implies that A *satisfies TC*. Moreover, they imply that* A *satisfies TMS iff it is weakly isomorphic to an algebra* $\langle U,F\rangle^{[k]}$, $F \subseteq \mathrm{Sym}\, U$.

We wonder if it may be possible to describe all clones satisfying TC*; but we shall not pursue this goal here. Before moving on, we reword Theorem 4.8 slightly.

THEOREM 4.10. *Suppose that* $A = \langle A,f\rangle$ *satisfies TMS and TC*, and has just one operation. There exists an algebra* $\langle U,\sigma\rangle$, $\sigma \in \mathrm{Sym}\, U$, *such that:*

i) $\mathrm{Con}\, A \cong \mathrm{Con}\langle U,\sigma\rangle$;

ii) if $\mathrm{Con}\, A$ *does not consist of all equivalence relations on the set* A *then* A *is weakly isomorphic to some* $[k]$*-th power of* $\langle U,\sigma\rangle$.

Proof. By Theorem 4.8. If f is constant, we can take $U = A$, $\sigma = \mathrm{id}_A$.

Proposition 4.3(3) supplies the lattice isomorphism if f is not constant. □

5. CONGRUENCE LATTICES OF ALGEBRAS WITH ONE OPERATION

We return to the question with which the paper began, having the machinery in hand now to resolve it. We define three classes of lattices. C is the class of finite simple lattices whose co-atoms intersect to 0. Incidentally, for precisely this class of lattices, R.Wille [15] proved that the clone of polynomial operations of each lattice is identical with the set of operations preserving the lattice ordering. The second class, M, a subclass of C, is the class of finite lattices isomorphic to $\mathit{Sub}\ V$ for some non-trivial vector space V.

To define the third class, we first define some lattices. Given any pair (m,n) of positive integers, we write $L_{m,n}$ for the lattice of congruences of the algebra $A_{m,n} = \langle m\times n,\sigma\rangle$, where $\sigma((i,j)) = (i,j+1)$ if $i<m$, $j < n-1$, and $\sigma((i,n-1)) = (i,0)$. Thus $L_{m,n}$ is the congruence lattice of a permutation consisting of m cycles of equal length n. In particular, $L_{m,1}$ is the full lattice of equivalence relations on an m-element set.

<u>Exercise 5.1</u>. Suppose that $L = L_{m,n}$ with $m\cdot n > 1$. Then $L \in M$ iff $L \in C$ and is modular, and this is *iff* $m=2$ or 3 and $n=1$, or $m=1$ and n is prime. L satisfies $\wedge(\text{co-atoms}) = 0$ iff n is square-free. L is simple iff $m>1$, or $m=1$ and n is prime.

The third class, N, is the class of lattices isomorphic to $L_{m,n}$ for some (m,n) satisfying: $m>1$; $m>3$ if $n=1$; n is square-free. Notice that, by the exercise, N is just the class of lattices in $C-M$ isomorphic to $L_{m,n}$ for some $m\geq 1$, $n\geq 1$.

LEMMA 5.2. *Suppose that* $L = \mathit{Con}\langle U,\sigma\rangle$, $\sigma \in \mathrm{Sym}\ U$, U *finite. Then* $L \in C-M$ *iff* $L \in N$. *Moreover,* $L \in N$ *and* $L \cong L_{m,n}$ *imply* $A_{m,n} \cong \langle U,\sigma\rangle$.

<u>Proof</u>. We assume that $L \in C$. We shall prove that $\langle U,\sigma\rangle \cong A_{k,\ell}$ for some pair (k,ℓ). Then by the exercise, the only further thing we must do is prove that if the pair (k,ℓ) satisfies the conditions for $L_{k,\ell} \in N$, then k and ℓ are determined by the abstract shape of L. Suppose, to get a contradiction, that the orbits of σ are not equal-sized. Say U_1 and U_2 are orbits and $\ell = |U_1| < |U_2|$. We claim that any pair $(b,\sigma^{\ell}b)$, $b \in U_2$, belongs to every co-atom of L. Since $b \neq \sigma^{\ell}b$ when $b \in U_2$, this will contradict that $L\in C$.

To prove the claim, let θ be any co-atom of L. Define $\bar\theta = \{(x,y): \exists\, t>0\ (x,\sigma^{t}y) \in \theta\}$. It is easily checked that $\bar\theta \in L$ and $\bar\theta \geq \theta$. Thus two cases arise. If $\bar\theta=\theta$ then we are done, since each $\bar\theta$ equivalence class is a union of orbits. Assume that $\bar\theta = 1_U$. Choose any $a \in U_1$, $b \in U_2$, t such that $(a,\sigma^{t}b) \in \theta$. Since $\sigma^{\ell}a = a$, we get $(\sigma^{t}b,\sigma^{t+\ell}b) \in \theta$. Then since id_U is a power of σ^{t}, it follows that $(b,\sigma^{\ell}b) \in \theta$, as desired.

Since the orbits are of equal size, we have that $\langle U,\sigma\rangle \cong A_{k,\ell}$ for some $k,\ell \geqslant 1$. Now we assume also that $L = Con\langle U,\sigma\rangle$ belongs to N, so that $k>1$, $k>3$ if $\ell=1$, and ℓ is square-free, by Exercise 5.1. Our problem is to show that k and ℓ are precisely determined by the shape of L. Let $U_0,\dots,U_{k-1}$ be the orbits of σ. We begin by observing that there are two types of atoms in L. If θ is an atom of $Con\langle U_i,\sigma|_{U_i}\rangle$, then $\theta \cup 0_U$ is an atom of L. We call U_i the support of this atom. All atoms of this sort we call "type 1," and we let At(1) be the set of them. If $a \in U_i$, $b \in U_j$, $i \neq j$, then $\{(\sigma^t a,\sigma^t b)\colon 0 \leqslant t < \ell\} \cup 0_U$ is an atom of L. We say that it is of "type 2," that it has support $U_i \cup U_j$, and we write At(2) for the set of type 2 atoms. Obviously, every atom is of type 1 or type 2. The element $\Delta = {}^2U_0 \cup \dots \cup {}^2U_{k-1}$ of L is very special. The interval $\Delta/0_U$ is a distributive lattice. (This follows easily from the fact that $Con\langle U_i,\sigma|_{U_i}\rangle$ is isomorphic to the distributive lattice of divisors of ℓ.)

Given distinct atoms θ and θ', there are several possibilities for their join. If they are both of type 1, then $\theta \vee \theta'/0 \cong M_2$, since $\theta \vee \theta' \leqslant \Delta$. If they are both of type 2, with unequal but intersecting supports, then $\theta \vee \theta'/0 \cong M_3$. If they are type 2 with disjoint supports, then $\theta \vee \theta'/0 \cong M_2$. For all other pairs of distinct atoms $\theta \vee \theta'$ has height $\geqslant 3$. Thus $\theta \vee \theta'/0 \cong M_3$ if and only if $\theta,\theta' \in$ At(2) and they have overlapping but unequal supports.

The argument breaks into two cases.

Case 1, $k \geqslant 3$. (This holds iff $\theta \vee \theta'/0$ is an M_3, for some atoms θ and θ' of of L.) Let ρ be the binary relation on atoms defined by $\theta\rho\theta'$ iff $\theta \vee \theta'/0 \cong M_3$. Then $\mathrm{At}(2) = \{\theta\colon \theta\rho\theta' \text{ for some } \theta'\}$. Let η be the relation on atoms defined by $\theta\eta\theta'$ iff $\theta \vee \theta'/0 \cong M_2$. Now for any $\theta_0 \in$ At(2), the relation

$$\theta \equiv \theta' \leftrightarrow \theta\rho\theta_0\rho\theta' \wedge \neg\theta\rho\theta' \wedge \neg\theta\eta\theta'$$

is an equivalence relation. Its domain is the set of type 2 atoms which share 1/2 support with θ_0. Two of these atoms are in the same equivalence class iff their supports are equal. It is easy to see that the equivalence classes have size ℓ, and their number is $2(k-2)$. Thus k and ℓ are determined.

Case 2, $k=2$. Here, an atom is of type 2 iff its join with every other atom has height at least 3. Thus At(2) is abstractly defined. $|\mathrm{At}(2)| = \ell$.

The proof of the lemma is finished. □

It may be interesting to observe that M, like N, is a two parameter family of lattices; a finite vector space is determined by its dimension and the size of its field.

Here is the principal result of this section.

THEOREM 5.3. *For any lattice* L *in* C, *the following are equivalent.*

(1) L *is isomorphic to the congruence lattice of a finite algebra with one basic operation.*

(2) L *belongs to* M *or to* N.

Proof. Suppose that $L \in C$. To see that (1) implies (2), let $L \cong Con\langle A,f\rangle$, A finite, and let $L \notin M$. By Corollary 1.10 and Theorem 2.11, the algebra $\langle A,f\rangle$ has TMS and TC*. Then by Theorem 4.10, there exists $\langle U,\sigma\rangle$, $\sigma \in \mathrm{Sym}\, U$, U finite, with $L \cong Con\langle U,\sigma\rangle$. And by Lemma 5.2, $L \in N$.

Now $L \in N$ trivially implies that (1) holds. So suppose that $L \in M$ and let $L \cong Sub\ V$ ($\cong Con$ V) where $V = \langle V,+,\bar{f}\ (f \in F)\rangle$ is a finite vector space over a field F. Say $F = \{0,1,f_2,\ldots,f_{q-1}\}$. Define $h(x_0,\ldots,x_{q-1}) = x_0 + x_1 + \bar{f}_2(x_2) + \ldots + \bar{f}_{q-1}(x_{q-1})$. It is trivial to see that $Con\ V = Con\langle V,h\rangle$. With this, the proof is concluded. □

Of course, the class $C-M-N$ of lattices excluded by the theorem is contained in a larger, but less understood, class of excluded lattices, composed of those that force TMS and TC* and do not belong to N.

For relatively small lattices, it may be easy to check that the lattice belongs to $C-M$, and difficult to see that it does not belong to N. The next exercise provides a simple criterion which at least ensures that $L \notin N$. The result is related to some facts proved in [9].

Exercise 5.4. Every lattice in N has an element x such that $x/0 \cong M_2$.

THEOREM 5.5. *Let* $L_{m,n} \in N$ *and let* $\langle A,f\rangle$ *be a finite algebra with one operation.*

(1) *If* $n=1$, *then* $Con\langle A,f\rangle \cong L_{m,n}$ *iff* f *is constant and* $|A| = m$, *or* $|A| = m^k$ *for some* $k \geq 1$ *and* $\langle A,f\rangle$ *is weakly isomorphic to* $\langle m,\mathrm{id}\rangle^{[k]}$.

(2) *If* $n>1$, *then* $Con\langle A,f\rangle \cong L_{m,n}$ *iff* $|A| = (mn)^k$ *and* $\langle A,f\rangle$ *is weakly isomorphic to* $A_{m,n}^{[k]}$ *for some* $k \geq 1$.

Proof. Suppose that $Con\langle A,f\rangle \cong L_{m,n}$. Following the first paragraph in the proof of Theorem 5.3, using Theorem 4.8 instead of 4.10, we obtain that either f is constant, or $\langle A,f\rangle$ is weakly isomorphic to $\langle U,\sigma\rangle^{[k]}$. If f is constant, then $L_{m,n} \cong L_{a,1}$, $a = |A|$, so by Lemma 5.2, $m = a$ and $n = 1$. Assume that f is not constant. By Lemma 5.2, $\langle U,\sigma\rangle \cong A_{m,n}$, and that concludes the proof. □

We wonder if there is an analogue of Theorem 5.5 for the class M.

REFERENCES

1. R.Freese, W.A.Lampe and W.Taylor, Congruence lattices of algebras of fixed similarity type, I. Pacific J. Math. 82 (1979), 59-68.

2. B.Jónsson, *Topics in Universal Algebra.* Springer Lecture Notes, No. 250 (1970).

3. P.Köhler, M_7 as an interval in a subgroup lattice. Algebra Universalis (to appear).

4. W.A.Lampe, Congruence lattices of algebras of fixed similarity type, II. Pacific J. Math. (to appear).

5. R.McKenzie, A new product of algebras and a type reduction theorem. Algebra Universalis (to appear).

6. R.McKenzie, Categorical quasi-varieties revisited. (Preprint 1981).

7. P.P.Pálfy, On certain congruence lattices of finite unary algebras. Commentationes Math. Univ. Carolinae 19, 1 (1978), 89-85.

8. P.P.Pálfy, Unary polynomials in algebras, I. (Preprint 1982).

9. P.P.Pálfy and P.Pudlák, Congruence lattices of finite algebras and intervals in subgroup lattices of finite groups. Algebra Universalis 11 (1980), 22-27.

10. J.Płonka, Diagonal algebras. Fund. Math. 58 (1966), 309-321.

11. P.Pudlák and J.Tuma, Every finite lattice can be embedded into a finite partition lattice. Algebra Universalis 10 (1980), 74-95.

12. N.Sauer, M.G.Stone and R.H.Weedmark, Every finite algebra with congruence lattice M_7 has principal congruences, (this volume).

13. W.Taylor, The fine spectrum of a variety. Algebra Universalis 5 (1975), 262-303.

14. W.Taylor, Some applications of the term condition. Algebra Universalis 14 (1982), 11-25.

15. R.Wille, Eine Charakterisierung endlicher, ordnungspolynomvollständiger Verbände. Arch. Math. (Basel) 28 (1977), 557-560.

University of California
Berkeley, California

INHERENTLY NONFINITELY BASED FINITE ALGEBRAS

George F. McNulty *
Caroline R. Shallon **

Dedicated to Bjarni Jonsson
In honor of his 60th Birthday

A variety V is *inherently nonfinitely based* provided V is locally finite and W is not finitely based whenever W is a locally finite variety and V $\subseteq$ W. The central task of the present work is to develop the theory of inherently nonfinitely based varieties; especially to provide conditions sufficient to insure that a variety generated by a finite groupoid is inherently nonfinitely based. These conditions, for the most part, have a syntactical character which makes their formulation a bit complex. However, they are easily verifiable conditions by means of which we have discovered that a good number of small groupoids actually generate varieties which are inherently nonfinitely based. We have included a list of these as an appendix.

An algebra $\mathfrak{A}$ will be called *inherently nonfinitely based* if HSP $\mathfrak{A}$ is inherently nonfinitely based. Evidently, if $\mathfrak{A}$ is inherently nonfinitely based and $\mathfrak{L}$ is any finite algebra such that $\mathfrak{A} \in$ HSP $\mathfrak{L}$, then $\mathfrak{L}$ is also inherently nonfinitely based. Hence, the existence of one inherently nonfinitely based finite algebra insures the existence of infinitely many more, each with a distinct equational theory. In this way, nonfinitely based finite algebras are seen to be much more common and much less sporadic than appeared to be the case only a few years ago.

Not all finite algebras which fail to be finitely based turn out to be inherently nonfinitely based. In particular, the nonassociative rings discovered by Polin [16], as well as their descendants, the rings of Oates-MacDonald and Vaughan-Lee [10], the loops of Vaughan-Lee [18], and even the pointed group of Bryant [2] are all nonfinitely based but, by construction, they all fail to be inherently nonfinitely based. As we will establish below, the first nonfinitely based finite algebra to be

*) The first author was supported, in part, by NSF grant MCS 80-01778

**) Part of this work subsumes Chapter 7 of the second author's Ph.D. thesis written under the direction of Kirby Baker at UCLA.

discovered, that of Lyndon [4], also fails to be inherently nonfinitely based. On the other hand, the groupoids discovered by Visin [19], Murskii [8], and Shallon [17] are inherently nonfinitely based. The status of Perkins' [13] six element semigroup and of Park's [13] four element commutative groupoid is at present unknown.

The concept of an inherently nonfinitely based variety was introduced independently around 1979 by V. L. Murskii [9] and P. Perkins [14]. In Murskii's work the notion is implicit; he demonstrates that the three element groupoid first published in Murskii [8] is inherently nonfinitely based. Perkins explicitly identifies the notion and proves several general results concerning it. Both men were investigating the asymptotic growth of nonfinitely based finite groupoids and Murskii achieved a sharp result. (The asymptotic density of nonfinitely based finite groupoids behaves like n^{-6}). Curiously, the ideas of Murskii and Perkins about inherently nonfinitely based varieties, for all their common motivation and timing, seem to have little overlap. Our work is primarily an elaboration of the ideas put forward by Murskii and Perkins.

Sections 1 and 2 contain our main results. A proof that Lyndon's groupoid is not inherently nonfinitely based can be found in section 3. Some open problems are gathered in section 4. The last section is an appendix of nonfinitely based finite groupoids.

We are happy to acknowledge the encouragement and fruitful discussions we had on these topics with many people. Among them are Kirby Baker, the thesis advisor of the second author, Joel Berman, who brought Murskii [9] to our attention, Tom Harrison, who read an earlier version of this paper and caught many errors, the Hawaiian Universal Algebra Seminar: Cliff Bergman, Ralph Freese, Bill Lampe, J. B. Nation, Doug Pickering, and Dick Pierce, as well as Ralph McKenzie, Peter Perkins, Don Pigozzi, Ivo Rosenberg, and Walter Taylor. The first author is grateful to the University of Hawaii for its hospitality while this paper was being written.

§1. GRAPH ALGEBRAS AND RESEMBLANCE OF TERMS.

An algebra equipped with just one fundamental operation is called a *groupoid* if that operation is binary. For the remainder of this paper, except as otherwise noted, all algebras will be groupoids. We adopt the customary notation and write terms with parentheses using juxtaposition to denote the operation. Our restriction to groupoids is really inessential but it makes the underlying ideas more appealing.

We will use the word "graph" to mean a graph without multiple edges, though loops at the vertices are permitted. With each graph $G = (V,E)$ we associate a groupoid called the *graph algebra of* G and denoted by $\mathfrak{g}(G)$. The universe of $\mathfrak{g}(G)$ is $V \cup \{\infty\}$ where $\infty \notin V$. The operation $*$ of $\mathfrak{g}(G)$ is defined so that $\infty * a = a * \infty = \infty$ for all $a \in V \cup \{\infty\}$ and

$$a * b = \begin{cases} a & \text{if } a \text{ and } b \text{ are adjacent in } G \\ \infty & \text{otherwise.} \end{cases}$$

The graph algebra $\mathfrak{G}(G)$ is *loopless* if G has no loops and *looped* if every vertex of G has a loop.

Under two very similar hypotheses a locally finite variety V will turn out to be inherently nonfinitely based and to have a number of other interesting properties. These hypotheses are:

(#) *Every loopless graph algebra belongs to* V.

($) *Every looped graph algebra belongs to* V.

Before taking up the main theorem of this section, it is convenient to look more deeply at graph algebras and at these two hypotheses.

Evidently G can be recovered from $\mathfrak{G}(G)$. Two graph algebras are isomorphic if and only if their graphs are isomorphic. In fact, one can read many properties of graph algebras in their graphs.

THEOREM 1. *Suppose* $\mathfrak{A}$ *is a graph algebra arising from the graph* G.

i) $\mathfrak{A}$ *is simple if and only if* G *is connected and any two distinct vertices of* G *have distinct neighborhoods.*

ii) $\mathfrak{A}$ *is subdirectly irreducible if and only if* G *is connected and no more than one pair of distinct vertices have identical neighborhoods.*

Proof: Suppose G is disconnected. Let C be one of the components and let $D = V \sim C$. Let α be the equivalence relation on $V \cup \{\infty\}$ with blocks $C \cup \{\infty\}$ and $\{d\}$ for all $d \in D$. Let β be the equivalence relation with blocks $D \cup \{\infty\}$ and $\{c\}$ for all $c \in C$. It is straightforward to check that α and β are both congruence relations on $\mathfrak{A}$. But $\alpha \cap \beta$ is the identity relation. Hence $\mathfrak{A}$ is not subdirectly irreducible, much less simple.

So we restrict our attention to the case when G is connected. Note that $\theta(a,\infty)$, the congruence relation generated by $\{(a,\infty)\}$, is the complete relation if $a \neq \infty$. Indeed, if $b \in A \sim \{\infty\}$ and $a, c_1, c_2, \ldots c_{n-1}, b$ is a path connecting a and b in G, then

$$b = b(c_{n-1}(c_{n-2}\cdots(c_2(c_1 a))\ldots)$$

so $(b,\infty) \in \theta(a,\infty)$.

Now we verify the Theorem. Let a and b be vertices in G. Let $N_a = \{c\colon a \text{ is adjacent to } c\}$ and $N_b = \{c\colon b \text{ is adjacent to } c\}$. If $N_a = N_b$, then $\theta(a,b)$ is the congruence relation with blocks $\{a,b\}$ and $\{d\}$ for all $\{d\}$ with $a \neq d \neq b$. If $N_a \neq N_b$ then $\theta(a,b)$ is the complete relation, since without loss of generality there is $c \in N_a \sim N_b$ whence

$$c = ca \equiv cb = \infty \mod \theta(a,b).$$

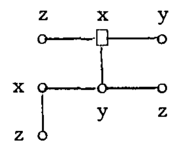
The theorem follows immediately. $\square$

It turns out to be very easy to construct simple graph algebras of any size desired.

Computing the value of a term function in a graph algebra is not hard. The following analysis of terms reveals how. With each term θ we will associate a rooted labelled tree $T(\theta)$ the vertices of which are labelled with the variables occurring in θ. If θ is a variable, then $T(\theta)$ consists of a single vertex, the root, which is labelled with the variable θ. If θ is the term $\phi\psi$, then $T(\theta)$ is the tree obtained from disjoint copies of $T(\phi)$ and $T(\psi)$ by adding an edge between the roots of $T(\phi)$ and $T(\psi)$ and retaining the root of $T(\phi)$ as the root of $T(\theta)$. Thus $T(\theta)$ will be a connected acyclic labelled graph with a distinguished vertex. For example, if θ is the term

$$((xy)z)((yz)(xz))$$

then $T(\theta)$ is



where the square vertex is the root. Different terms may give rise to the same tree. The term $((x((y(xz))z))z)y$ has the tree drawn above. The following lemma, easily established by induction on the complexity of the term θ, is very useful.

LEMMA. *Let* $\mathfrak{A}$ *be a graph algebra and let* θ *be a term. Under any assignment of members of* $\mathfrak{A}$ *to the variables in* θ *we have:*

i) θ *is given the value* ∞ *if* ∞ *is assigned to any variable occuring in* θ

ii) θ *is given the value* ∞ *if values not adjacent in the graph of* $\mathfrak{A}$ *are assigned to variables which label adjacent nodes in* $T(\theta)$.

iii) θ *is given the value assigned to the root of* $T(\theta)$ *in all other cases.*

The terms ϕ and ψ *resemble* each other provided the roots of $T(\phi)$ and $T(\psi)$ have the same labels and for any variables x and y, $T(\phi)$ has adjacent vertices labelled x and y if and only if $T(\psi)$ has adjacent vertices labelled x and y. ϕ *weakly resembles* ψ if the roots of $T(\phi)$ and $T(\psi)$ have the same labels and for any two distinct variables x and y, $T(\phi)$ has adjacent vertices labelled x and y if and only if $T(\psi)$ has adjacent vertices labelled x and y. The variable x is *doubled* in θ if $T(\theta)$ has two adjacent vertices labelled x. These notions provide syntactical equivalents for (#) and ($).

THEOREM 2. *The following are equivalent:*

i) V *satisfies* (#).

ii) *Every loopless graph algebra arising from a finite connected graph belongs to* V.

iii) *If* $V \models \phi \approx \psi$, *then either* ϕ *resembles* ψ *or else both* ϕ *and* ψ *have doubled variables.*

Proof. (i) ⇒ (ii) is clear.

Let ϕ be any term. Let $\mathfrak{L}_\phi$ be the groupoid whose universe consists of ∞ and the variables which occur in ϕ and whose fundamental operation * satisfies $x * \infty = \infty * x = \infty$ for all x occuring in ϕ and

$$x * y = \begin{cases} x & \text{if } T(\phi) \text{ has adjacent vertices labelled } x \text{ and } y \\ \infty & \text{otherwise.} \end{cases}$$

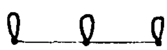
Evidently $_\phi$ is a finite connected graph algebra which is loopless if ϕ has no doubled variables. Moreover, if ϕ resembles ψ, then $_\phi = {}_\psi$.

(ii) ⇒ (iii). Suppose $V \models \phi \approx \psi$. First assume that ϕ has no doubled variables. By (ii), $\mathfrak{L}_\phi \in V$. In $\mathfrak{L}_\phi$ assign x (construed as an element of $\mathfrak{L}_\phi$) to x (construed as a variable in ϕ). Under this assignment ϕ is given the value of its root, according to the Lemma. But ψ must be given the same value since $\mathfrak{L}_\phi \models \phi \approx \psi$. Again by the Lemma, we conclude that ϕ resembles ψ. A similar argument yields that ϕ resembles ψ if ψ has no doubled variables. So the only case remaining is for both ϕ and ψ to have doubled variables. Thus (iii) is established.

(iii) ⇒ (i). This follows immediately from the Lemma. □

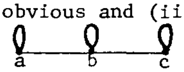
THEOREM 2'. *The following are equivalent:*

i) V *satisfies* ($).

ii) *The graph algebra of*  *belongs to* V.

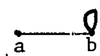
iii) *If* $V \models \phi \approx \psi$, *then* ϕ *weakly resembles* ψ.

Proof. As in the previous proof the only implication that requires argument is (ii) ⇒ (iii), since (i) ⇒ (ii) is obvious and (iii) ⇒ (i) follows from the Lemma.

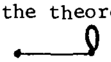
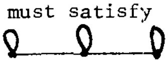
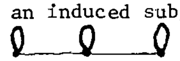
Let $\mathfrak{A}$ be the graph algebra of 

. Suppose $V \models \phi \approx \psi$ and that x and y are distinct variables labelling adjacent vertices in $T(\phi)$. Assign a to x and c to y and b to every other variable. Under this assignment ϕ is given the value ∞, according to the Lemma. Since $\mathfrak{A} \models \phi \approx \psi$, we deduce that ψ is given the value ∞ by the same assignment. According to the Lemma, two values not adjacent in the graph of must have been assigned to variables labelling adjacent vertices in $T(\psi)$. a and c are the only nonadjacent values in the graph and they were assigned to x and y respectively. Hence x and y label adjacent vertices in $T(\psi)$. Thus ϕ weakly resembles ψ. □

EXAMPLE 3. (Murskii's Groupoid) *The variety generated by the graph algebra of*  *satisfies* (#).

Proof. Let $\mathfrak{A}$ be the graph algebra of  . Suppose $\mathfrak{A} \models \phi \approx \psi$. Evidently the same variables occur in ϕ and ψ. If x is doubled in ϕ then by assigning a to x and b to all other variables, ϕ would be given the value ∞. Hence x must also be doubled in ψ, according to the Lemma. So assume that ϕ and ψ have no doubled variables and that vertices labelled x and y are adjacent in ϕ. Assign a to both x and y and b to all other variables. Under this assignment ϕ is given the value ∞. So ψ is given the value ∞ as well. Thus two variables assigned a are labels for adjacent vertices of $T(\psi)$. As ψ has no doubled variables we conclude that $T(\psi)$ has adjacent vertices labelled x and y. Thus ϕ resembles ψ as desired. □

THEOREM 4. *Let* G *be a finite connected graph. The variety generated by* $\mathfrak{G}(G)$ *satisfies one of* (#) *and* ($) *if and only if* G *has at least two vertices,* G *has at least one vertex with a loop, and* G *is not a complete graph with loops at all vertices.*

Proof. First suppose that G is a finite connected graph with all the properties listed in the theorem. If G has a vertex without a loop, then, by connectedness, G has  as an induced subgraph. But then Murskii's Groupoid belongs to the variety generated by $\mathfrak{G}(G)$ and, according to Example 3, this variety must satisfy (#). On the other hand, if every vertex of G has a loop, then  is an induced subgraph of G, in view of connectedness. Thus, the graph algebra of  belongs to the variety generated by $\mathfrak{G}(G)$ and so by Theorem 2' this variety satisfies ($).

To establish the converse we need to show that the variety generated by $\mathfrak{G}(G)$ satisfies neither (#) nor ($) when G is a finite connected graph not having at least one of the listed properties.

Case 0. G *has exactly one vertex.* There are two graph algebras to consider:

	∞	a
∞	∞	∞
a	∞	∞

$\mathfrak{A}_0$

and

	∞	a
∞	∞	∞
a	∞	a

$\mathfrak{A}_1$

Both $\mathfrak{A}_0$ and $\mathfrak{A}_1$ are commutative, but the commutative law violates (#) and ($) in view of (iii) in Theorems 2 and 2'.

Case 1. G *has more than one vertex, but no loops.*

Suppose G has n vertices. Let θ be any term with n+1 distinct variables such that $T(\theta)$ has adjacent vertices labelled by every pair of distinct variables, but θ has no doubled variables. (Such terms are easy to devise by starting with a tree correctly labelled.) Then $\mathfrak{G}(G) \models \theta \approx xx$ by the pigeonhold principle, where x is a variable not occurring in θ. So neither (#) nor ($) can hold.

Case 2. G *is a complete graph with loops at each vertex, and* G *has at least two vertices.*

In view of the Lemma, any assignment from $\mathfrak{G}(G)$ that does not assign ∞ to a variable occurring in ϕ will give ϕ the value assigned its root. Hence $\mathfrak{G}(G) \models \phi \approx \psi$ if and only if the same variables occur in ϕ and ψ and the roots of $T(\phi)$ and $T(\psi)$ have the same labels. According to (iii) of Theorems 2 and 2' neither (#) nor ($) can hold. □

COROLLARY 5. *There is no finite set* F *of finite loopless graphs such that* V *satisfies* (#) *if and only if* $\mathfrak{G}(G) \in V$ *for all* $G \in F$.

We are now in a position to prove the main results of this section.

THEOREM 6. *Let* V *be a variety satisfying either* (#) *or* ($). *Then*

0. *If* V *is locally finite, then* V *is inherently nonfinitely based.*

1. V *has simple algebras of every cardinality larger than* 4.

2. V *is residually large.*

3. V *does not have definable principal congruence relations.*

Proof. Strictly speaking, each part of this theorem requires two proofs - one under each of the hypotheses. We will only supply the proof under hypothesis (#). Roughly speaking, the proof under ($) can be obtained by converting the loopless graphs involved in the (#)-proofs into looped graphs.

0. Suppose $V \subseteq W$ and both V and W are locally finite. Since V satisfies (#) we know that W also satisfies (#). Thus, if we can show that V is not finitely based, then, *mutatis mutandis*, W is not finitely based either and so V will be inherently nonfinitely based.

Let $V^{[n]}$ denote the variety of all algebras satisfying all equations true in V all of whose variables are among $x_0, x_1, \ldots, x_{n-1}$. According to Birkhoff [1] a locally finite variety V of finite type is not finitely based iff $V \neq V^{[n]}$ for every natural number n. (See Burris and Sankapannavar [3] page 228 for the elements of a proof.) For each natural number n we construct an algebra $\mathfrak{L}_n$ such that

$\mathfrak{L}_n \in V^{[n]}$ but $\mathfrak{L}_n \notin V$.

The universe B_n of $\mathfrak{L}_n$ is the set

$$(\{0,1,\ldots,n\} \times \omega) \cup \{\infty\}$$

where ω is the set of natural numbers and ∞ is a set not belonging to $\{0,1,\ldots,n\} \times \omega$. The fundamental operation $\circ$ of $\mathfrak{L}_n$ is defined so that $\alpha \circ \infty = \infty \circ \alpha = \infty$ for all $\alpha \in B_n$ and

$$(a,j) \circ (b,k) = \begin{cases} (a,m) & \text{if } a+1 \equiv b \mod(n+1) \text{ where } m = \max(j,k+1) \\ (a,m) & \text{if } a \equiv b+1 \mod(n+1) \text{ where } m = \max(j,k-1) \\ \infty & \text{otherwise.} \end{cases}$$

The algebras $\mathfrak{L}_n$ were first devised by Murskii [9], whose argument that the Murskii Groupoid is inherently nonfinitely based we have adapted here. $\mathfrak{L}_n$ is not a graph algebra. On the other hand, the "projection" of $\mathfrak{L}_n$ onto its first coordinate is the graph algebra of a cycle $n+1$ vertices. This means that some parts of the Lemma concerning the evaluation of terms in graph algebras still holds. In particular, let θ be any term and assign members of B_n to the variables in θ. Observe the following:

i) θ is given the value ∞ if ∞ is assigned to a variable occurring in θ.

ii) θ is given the value ∞ if two pairs with nonadjacent (on the $n+1$ cycle) first coordinates are assigned to variables labelling adjacent vertices of $T(\theta)$.

iii) θ is given a value different from ∞ in all other cases; moreover, the first coordinate of this value is the first coordinate of the value assigned to the root of $T(\theta)$.

Thus the only gap in our ability to evaluate terms in $\mathfrak{L}_n$ lies with the second coordinates in Case (iii) above. Since we wish to show that $\mathfrak{L}_n \in V^{[n]}$ we will concern ourselves with terms all of whose variables are among $x_0,x_1,\ldots,x_{n-1}$. Let θ be such a term. Let Δ_θ denote the set $\{i : x_i \text{ occurs in } \theta\}$.

Claim. Under any assignment of members of B_n to the variables in θ either θ is given the value ∞ or else the value assigned to θ depends only on Δ_θ and the root of $T(\theta)$.

Proof. Suppose θ is not given the value ∞. Then ∞ is assigned to no variable occurring in θ, So let (a_0,k_0), $(a_1,k_1),\ldots$ be the values assigned respectively to $x_0,x_1,\ldots$. Let (a_θ,k_θ) be the value assigned to the variable which labels the root of $T(\theta)$. Now θ has at most n distinct variables and so at least one of $0,1,\ldots,n$ is not among $a_0,a_1,a_2,\ldots$. In view of the automorphisms of $\mathfrak{L}_n$, we can assume that $0 \notin \{a_0,a_1,a_2,\ldots\}$. We will prove by induction on the complexity of θ that θ is assigned

$$(a_\theta, \max_{i\in\Delta_\theta} (k_i + a_i - a_\theta)).$$

This is obvious if θ is a variable, so suppose θ is $\phi\psi$. Thus neither ϕ nor ψ is assigned ∞. Therefore by the inductive hypothesis, ϕ is assigned

$$(a_\phi, \max_{i\in\Delta_\phi} (k_i + a_i - a_\phi))$$

while ψ is assigned

$$(a_\psi, \max_{i\in\Delta_\psi} (k_i + a_i - a_\psi)).$$

But $a_\phi = a_\theta$ since the root of $T(\theta)$ is the same as the root of $T(\phi)$. Moreover, a_ϕ and a_ψ are successive natural numbers. So there are two cases:

<u>Case 0</u>. $a_\phi + 1 = a_\psi$.

In this case θ is given the value

$$(a_\theta, \max(\max_{i\in\Delta_\phi} (k_i + a_i - a_\theta), 1+ \max_{j\in\Delta_\psi} (k_j + a_j - a_\psi))$$

which is equal to

$$(a_\theta, \max(\max_{i\in\Delta_\phi} (k_i + a_i - a_\theta), \max_{j\in\Delta_\psi} (k_j + a_j - (a_\psi - 1)))$$

but this is

$$(a_\theta, \max(\max_{i\in\Delta_\phi} (k_i + a_i - a_\theta), \max_{j\in\Delta_\psi} (k_j + a_j - a_\theta))$$

or

$$(a_\theta, \max_{i\in\Delta_\theta} (k_i + a_i - a_\theta)) \qquad \text{as desired.}$$

<u>Case 1</u>. $a_\phi = a_\psi + 1$.

This case is handled in a manner analogous to Case 0. So the claim is established.

If ϕ and ψ both have doubled variables, then $\mathfrak{L}_n \models \phi \approx \psi$ since any assignment will give both ϕ and ψ the value ∞; while if ϕ resembles ψ and both ϕ and ψ are terms in the variables $x_0,\ldots,x_{n-1}$, then $\mathfrak{L}_n \models \phi \approx \psi$, since resemblance insures that any assignment gives both or neither the value ∞ and in the non-∞ case the assignment gives ϕ and ψ the same value, in view of resemblance and the claim. But this means that $\mathfrak{L}_n \in V^{[n]}$.

To see that $\mathfrak{L}_n \notin V$ we produce an equation true in V but not true in $\mathfrak{L}_n$. For each natural number p let θ_p be the term

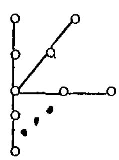
$$x_0(x_1(x_2\ldots(x_n(x_0(x_1(\ldots(x_m x_{m+1})\ldots)$$

where there are exactly $p+1$ occurrences of variables in ϕ_p but $x_0, x_1, \ldots, x_n$ are the only variables to occur in ϕ_p. (One could view ϕ_p as a string of variables which is of length $p+1$ and is indexed cyclically modulo $n+1$.) Since V is locally finite, there must be natural numbers p and q with $p \neq q$ such that $V \models \phi_p \approx \phi_q$. But by assigning $(i,0)$ to x_i in $\mathfrak{L}_n$, it turns out that ϕ_p is given the value $(0,p)$ while ϕ_q is given the value $(0,q)$. Hence $\mathfrak{L}_n \not\models \phi_p \approx \phi_q$ and so $\mathfrak{L}_n \notin V$. This concludes the proof of part 0 of the theorem. (To obtain the conclusion under ($) modify $\mathfrak{L}_n$ so that $(a,j) \circ (a,k) = (a, \max(j,k))$.)

1. For each k with $k \geq 4$, let $\mathfrak{G}_k$ be the graph algebra of

   i) The path with k vertices, if k is finite.

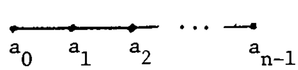
   ii) If k is infinite, the tree with k branches depicted below:



In either case $\mathfrak{G}_k \in V$ and is simple by Theorem 1.

2. This follows immediately from (1) above.

3. Let $\mathfrak{P}_n$ be the graph algebra of the path

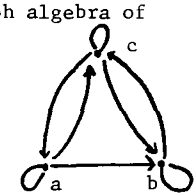


on n vertices. Let τ be any term in which the variable u occurs. Note that if there is an assignment which gives the value a_{n-1} to u and the value a_0 to τ, then τ has occurrences of at least n distinct variables. But (a_0,∞) belongs to the principal congruence on $\mathfrak{P}_n$ generated by (a_{n-1},∞). This means that any principal congruence formula (see Burris and Sankapannavar [3], page 222) for any variety to which $\mathfrak{P}_n$ belongs must have at least n occurrences of distinct variables. Since $\mathfrak{P}_n \in V$ we conclude that no finite set of principal congruence formulas serve to define congruences in V. Therefore V fails to have definable principal congruences. □

In recent years Michael Vaughan-Lee and Sheila Oates-Macdonald (aka Oates-Williams) in [10] and [11] have obtained some results concerning the subvarieties of the variety generated by Murskii's Groupoid. As all the algebras they employ to prove their results are openly loopless graph algebras, the same results by the same proof hold for all varieties satisfying (#). We gather these results in the next Theorem.

THEOREM 7. (See also Oates-Macdonald and Vaughan-Lee [10] and Oates-Williams[11]) *If* V *is a variety satisfying* (#), *then* V *has an infinite ascending chain of finite critical algebras, an infinite ascending chain of subvarieties, and an infinite descending chain of subvarieties.*

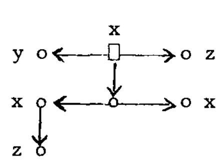
The possibility of obtaining the conclusions about ascending chains under hypothesis ($) is open. One impediment is that looped graph algebras only generate three distinct varieties: that generated by the graph algebra of , that generated by the graph algebra of , and that generated by the graph algebra of . One possible route around this difficulty is to develop the theory of "digraph" algebras. Shallon [17] sets down the beginnings of such a program. In this way ($) can be seen to entail an infinite descending chain. To conclude this section we sketch the proof that the digraph algebra of



satisfies ($). The digraph algebra is constructed like the graph algebra by adding a new "multiplicative zero" ∞ and translating $a \to b$ as $a * b = a$. Our particular digraph algebra will be denoted by $\mathfrak{M}$. It is

	∞	a	b	c
∞	∞	∞	∞	∞
a	∞	a	a	a
b	∞	∞	b	b
c	∞	c	c	c

If θ is a term, then $\vec{T}(\theta)$ is the directed tree obtained from $T(\theta)$ by directing all the edges outward from the root. So if θ is $((xy)z)((yx)(xz))$, then $\vec{T}(\theta)$ is



Now the lemma concerning evaluation of terms in digraph algebras will be just like the lemma for graph algebras. Simple and subdirectly irreducible digraph algebras can be characterized by properties of their graphs (See Shallon [17]).

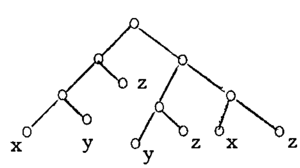
To see that our particular digraph algebra $\mathfrak{A}$ satisfies (\$) suppose $\mathfrak{A} \models \phi \approx \psi$. Suppose x and y are distinct variables and $x \to y$ occurs in $\vec{T}(\phi)$. Assign b to x, a to y, and c to every other variable. Under this assignment ϕ is given the value ∞ so ψ is given the value ∞ as well. In view of the lemma about evaluation $u \to v$ occurs in $\vec{T}(\psi)$ where b is assigned to u and a is assigned to v. So u is x and v is y. Therefore ϕ weakly resembles ψ (even in some directed sense). Thus $\mathfrak{A}$ satisfies (\$).

Digraph algebras represent a rich source of examples of finite algebras which are inherently nonfinitely based.

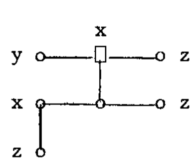
§2. NONASSOCIATIVE NONABSORPTIVE GROUPOIDS.

Just as the results of the last section were primarily inspired by the work of V. L. Murskii, the present section draws its motivation from the work of P. Perkins. Again, we develop syntactical conditions on locally finite varieties which entail that the variety is inherently nonfinitely based.

Every term θ can be construed, in the well-known way, as an ordered tree the leaves of which are labelled with the variables occurring in θ. In this view the term $((xy)z)(yz)(xz))$ is rendered as

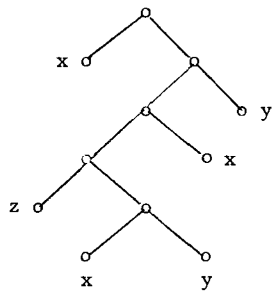


Notice that this way of associating a tree with a term is much different from $T(\theta)$ which is



Moreover, the rendering of θ as an ordered tree is faithful in the sense that θ can be recovered from the ordered tree.

A term θ is *slender* provided the interior nodes of the ordered tree rendering of θ are linearly ordered. Equivalently, θ is slender if and only if whenever $\phi\psi$ is a subterm of θ then at least one of ϕ and ψ is a variable. Thus $x(((z(xy))x)y)$ is slender and is rendered by



Yet another characterization is to insist that every left parenthesis occurs to the left of every right parenthesis.

Suppose θ is slender. θ has a unique subterm of the form xy where x and y are variables. In the tree rendition, this is the tree consisting of the lowest interior node and the two "leaves" suspended from it. Every occurrence of a variable in θ but outside this unique lowest term can be assigned a unique rank. Indeed, number the interior nodes of the tree so that the lowest is numbered 0, the next highest 1, and so on. Now number the leaves of the tree with the numbers of the interior nodes from which they are suspended. Thus 0 is assigned to the two lowest leaves but thereafter every number is assigned a unique leaf. The *code* of θ is a configuration $\left.\begin{matrix}u\\v\end{matrix}\right\} w_1w_2\cdots w_n$ where u and v are the leaves assigned 0 and w_i is the leaf assigned i and there are n+2 occurrences of variables in θ. In this code $\left.\begin{matrix}u\\v\end{matrix}\right\}$ indicates an unordered part of the code. Both u and v are adjacent to w_1. Hence the code of x(((z(xy))x)y) is

$$\left.\begin{matrix}x\\y\end{matrix}\right\} z\,x\,y\,x\,.$$

The *reduced code* of θ is obtained from the code of θ by replacing all consecutive occurrences of single variables by just one occurrence of the same variable. For example, if θ has code $\left.\begin{matrix}x\\y\end{matrix}\right\}$ yyzxxxyzxx, then the reduced code of θ is $\left.\begin{matrix}x\\y\end{matrix}\right\}$ zxyzx. A slender term θ is said to be *singular* provided no variable occurs more than once in the reduced code of θ.

Let θ be any slender term. $\partial\theta$ denotes the set of all slender singular terms ϕ such that some substitution instance of ϕ is a subterm of θ. If Δ is any set of slender terms, then let $\partial\Delta = \bigcup_{\theta\in\Delta} \partial\theta$.

The next theorem represents only a modest extension of a theorem in Perkins [14].

THEOREM 8. *Let* V *be a locally finite variety of groupoids. If there is a set* Δ *of slender singular terms with arbitrarily long reduced codes such that*

i) $\partial\Delta \subseteq \Delta$, *and*

ii) *if* $V \models \phi \approx \psi$ *and* $\phi \in \Delta$, *then* $\psi \in \Delta$ *and* ϕ *and* ψ *have the same* *reduced code,*

then V *is inherently nonfinitely based.*

Proof. Suppose V fulfills the hypotheses and that $W \supseteq V$ with W locally finite. Then W fulfills the hypotheses, as well. Thus, if the hypotheses entail that V is not finitely based, they will actually entail that it is inherently non-finitely based. We will prove that V is not finitely based. To do this, we establish that $V \neq V^{[m]}$ for every natural number m, by producing an equation true in V but not true in $V^{[m]}$.

Fix the natural number m.

Since V is locally finite, there is a natural number p such that among any collection of p distinct terms in $x_0, x_1, \ldots, x_m$ there must be at least two which form an equation true in V. Pick $\theta \in \Delta$ such that the reduced code of θ has length greater than p. Without loss of generality, we assume that the reduced code of θ is

$$\left.\begin{matrix} x_1 \\ x_0 \end{matrix}\right\} x_2\ x_3\ \cdots\ x_{n-1}$$

Let θ^* result from θ by substituting x_i for x_j where $i \equiv j \bmod (m+1)$ for $j < n$ and $i < m+1$. So θ^* amounts to an indexing modulo $m+1$ of the variables of θ. Since θ^* is a substitution instance of θ, we know that $\partial\theta \subseteq \partial\theta^*$. On the other hand, it follows from singularity that $\partial\theta^* \subseteq \partial\theta$. Now θ^* has at least p+1 subterms, each with a distinct reduced code. Moreover, these reduced codes have the property that between any two occurrences of the same variable all the other m variables must appear (even in order modulo $m+1$).

Let ϕ and ψ be two subterms of θ^* with different reduced codes such that $V \models \phi \approx \psi$. We will prove that $V^{[m]} \not\models \phi \approx \psi$. To see this, let Γ be the set of all terms η such that

i) η is slender,

ii) η has the same reduced code as ϕ, and,

iii) $\partial\eta \subseteq \Delta$

Note that $\phi \in \Gamma$ since $\partial\phi \subseteq \partial\theta^* = \partial\theta \subseteq \Delta$. However, $\psi \notin \Gamma$ since ϕ and ψ have different reduced codes. The following claim yields $V^{[m]} \not\models \phi \approx \psi$, thus concluding the proof.

Claim. If $\eta \in \Gamma$ and $V^{[m]} \models \eta \approx \mu$, then $\mu \in \Gamma$.

Proof. $V^{[m]} \models \eta \approx \mu$ means that $\eta \approx \mu$ can be derived from equations true in V which involve no variables other than $x_0, x_1, \ldots, x_{m-1}$. We prove the claim by induction on the length of such derivations. The crucial step is to suppose that $\sigma \approx \tau$ is true in V, involves only variables among $x_0, x_1, \ldots, x_{m-1}$, and that $\sigma' \approx \tau$

is a substitution instance of $\sigma \approx \tau$ such that σ' is a subterm of η and μ is obtained by replacing σ' by τ'.

Since $\eta \in \Gamma$ and σ' is a subterm of η, it follows that between any two occurrences of the same variable in the reduced code of σ' all m other variables occur. But σ' is a substitution instance of σ, which involves no more than m distinct variables. Therefore there is a slender singular term $\hat{\sigma}$ such that σ' is a substitution instance of $\hat{\sigma}$ and $\hat{\sigma}$ is a substitution instance of σ. Let $\hat{\tau}$ be the corresponding substitution instance of τ. Evidently $\hat{\sigma} \in \partial\eta \subseteq \Delta$ and $V \models \hat{\sigma} \approx \hat{\tau}$. So $\hat{\tau} \in \Delta$ and $\hat{\sigma}$ and $\hat{\tau}$ have the same reduced codes, according to hypothesis (ii) of the theorem. Hence σ' and τ' have the same reduced code. Consequently μ is slender and has the same reduced code as η. It remains to show that $\partial\mu \subseteq \Delta$.

Let γ be any slender term. $\bar{\gamma}$ is the term obtained from γ by the following recursion:

$\bar{\gamma}$ is x_0 if γ is a variable.

$\bar{\gamma}$ is $\bar{\rho}x_k$ if γ is ρy and either y is the last variable in the reduced code of ρ and x_k is the last variable in the reduced code of $\bar{\rho}$ or else y is not the last variable in the reduced code of ρ and k is the least natural number such that x_k does not occur in $\bar{\rho}$.

The case when γ is $u\rho$ and ρ is not a variable is handled similarly.

Thus $\bar{\gamma}$ is a singular slender term which results from renaming the variables in γ. (It is easy to see that $\bar{\theta}^*$ is just θ.) Note that $\partial\bar{\gamma} = \partial\gamma$.

Recall that $\hat{\sigma} \approx \hat{\tau}$ produced $\eta \approx \mu$ by replacement of τ' for σ' in η. Since $\hat{\sigma}$ and $\hat{\tau}$ are singular, observe that $\hat{\sigma} \approx \hat{\tau} \models \bar{\eta} \approx \bar{\mu}$. Since $\bar{\eta} \in \partial\eta \subseteq \Delta$ and $V \models \bar{\eta} \approx \bar{\mu}$, we deduce that $\bar{\mu} \in \Delta$. But $\partial\mu = \partial\bar{\mu}$, so $\partial\mu \subseteq \Delta$ as desired. □

Call a term **-singular* provided no variable occurs in it more than once. The proof written down above is not different in any important respect from the proof supplied by Peter Perkins for the following theorem.

THEOREM 8' (P. Perkins [14]) *Let* V *be a locally finite variety of groupoids. If there is a set* Δ *of slender *-singular terms of unbounded length such that*

i) $\partial\Delta \subseteq \Delta$, *and*

ii) *if* $V \models \phi \approx \psi$ *and* $\phi \in \Delta$, *then* $\psi \in \Delta$ *and* $xy \approx yx \models \phi \approx \psi$, *then* V *is inherently nonfinitely based.*

Theorem 8' is an immediate consequence of Theorem 8. The more complicated Theorem 8 has the following consequence.

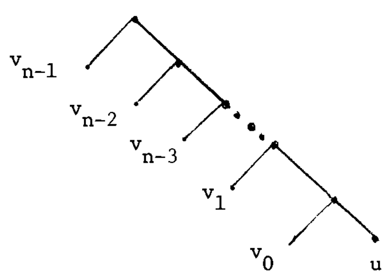
EXAMPLE 9 VISIN'S GROUPOID

Let $\mathfrak{A}$ be the groupoid with the following table:

	o	a	b	c
o	o	o	o	o
a	o	o	o	c
b	o	a	o	a
c	o	o	o	o

$\mathfrak{A}$ is inherently nonfinitely based.

Let Δ be the set of all singular terms of the form



where $u \notin \{v_0, v_1, \ldots, v_{n-1}\}$. Evidently $\partial\Delta \subseteq \Delta$. To verify hypothesis (ii) of Theorem 8, assume $\phi \in \Delta$ and $\mathfrak{A} \models \phi \approx \psi$. We must show that $\psi \in \Delta$ and that ψ and ϕ have the same reduced codes.

Claim 0. The same variables occur in ϕ and ψ.

Proof. By assigning a to u and b to all other variables in ϕ, ϕ will be given the value a. Hence ψ is given the value a by this assignment. Thus there are assignments that give both ϕ and ψ the value a. If some variable occurred in one of ϕ or ψ but not the other, it would be possible to alter one of these assignments to give one term the value a and the other the value 0. □

Claim 1. If $\sigma\tau$ is a subterm of ψ, then σ is a variable.

Proof. Since there is an assignment that gives ϕ the value a and assigns the variables values from $\{a,b\}$, this assignment must give every nonvariable subterm of ϕ and of ψ the value a. Thus $\sigma\tau$ has the value a. From the table for $\mathfrak{A}$ we see that σ has the value b while τ has the value a. Hence σ must be a variable. □

Claim 2. ϕ and ψ have the same rightmost variable.

Proof. Again assign a to the rightmost variable of ϕ and b to all other variables. Let uv be the unique subterm of ψ where u and v are variables.

Under the assignment uv must be assigned the value a (since 0, the only other possible assignment would reduce the value of ψ to 0). uv can be assigned a only if u is assigned b and v is assigned a. But v is the rightmost variable of ψ and it must be the rightmost variable of ϕ since that was the only variable assigned a. □

Claim 3. The rightmost variable of ψ occurs exactly once in ψ.

Proof. Suppose x occurs in ψ at other than the rightmost position. Thus $x\tau$ is a subterm of ψ. Under the same assignment used above $x\tau$ is assigned a, hence x must have been assigned b. But the rightmost variable was assigned a, so x is not the same as the rightmost variable. □

Claim 4. The reduced codes of ϕ and ψ are the same.

Proof. Let v be the common rightmost variable. Let ${}^{u_0}_{\,v}\}\ u_1, u_2 \ldots u_n$ be the reduced code of ϕ and let ${}^{w_0}_{\,v}\}\ w_1, w_2 \ldots w_m$ be the reduced code of ψ. Since ϕ is singular and the variables of ϕ and ψ are the same, we know that $n \le m$. First suppose $u_0 u_1 \ldots u_n$ is a proper initial segment of $w_0 w_1 \ldots w_m$. Thus $w_{n+1} = u_i$ for some $i < n$. Assign c to v, a to u_j for $j \le i$ and b to u_j for $j > i$. Under this assignment ϕ is given the value a, while ψ is given the value 0. So $u_0 u_1 \ldots u_n$ is not a proper initial segment of $w_0 w_1 \ldots w_m$. If ${}^{u_0}_{\,v}\}\ u_1 \ldots u_n$ is not the same as ${}^{w_0}_{\,v}\}\ w_1 \ldots w_m$, then there must be a smallest i such that $u_i \ne w_i$. Say $w_i = u_k$. By reasoning as under the first supposition we conclude that $i < k$. Assign c to v, a to u_j for $j < k$, and b to u_j for $j \ge k$. Under this assignment ϕ is given the value a while ψ is given the value 0. □

In view of claims 1–4, $\psi \in \Delta$. Together with claim 4 itself this means that the variety generated by $\mathfrak{A}$ fulfills hypothesis (ii) of Theorem 8. Hence $\mathfrak{A}$ is inherently nonfinitely based. □

The algebra $\mathfrak{A}$ was constructed by Visin [19] in 1963. Visin proved that is not finitely based. This was the second nonfinitely based finite algebra to be discovered.

An element a of a groupoid $\mathfrak{A}$ is a *zero of* $\mathfrak{A}$ provided $ab = ba = a$ for all b in $\mathfrak{A}$. An element u of $\mathfrak{A}$ is a *unit* of $\mathfrak{A}$ provided $ub = bu = b$ for all b in $\mathfrak{A}$. $\mathfrak{A}$ is said to be *absorptive* provided $\mathfrak{A} \models x \approx \theta$ where θ is some term different from the variable x.

On the basis of Theorem 8', Perkins proved the following theorem.

THEOREM 10. (P. Perkins [14]) *Every finite groupoid with a zero and a unit which is noncommutative, nonabsorptive, and nonassociative is inherently nonfinitely based.*

THEOREM 11. *Every nonassociative nonabsorptive finite groupoid with a zero and* *a unit is inherently nonfinitely based.*

Proof. Suppose $\mathfrak{A}$ is a finite groupoid with a zero, denoted by 0, and a unit, denoted by 1, which is nonassociative and nonabsorptive. In view of Theorem 10 we can also assume that $\mathfrak{A}$ is commutative. To prove that $\mathfrak{A}$ is inherently nonfinitely based, we invoke Theorem 9' taking Δ to be the set of all slender *-singular terms.

Evidently $\partial\Delta \subseteq \Delta$, so we only need to verify the second hypothesis of Theorem 8'. Thus suppose $\eta \in \Delta$ and $\mathfrak{A} \models \eta \approx \mu$. We prove that $xy \approx yx \vdash \eta \approx \mu$, verifying $\mu \in \Delta$ along the way.

Claim 0. η and μ have the same variables.

Proof. Suppose x occurs in one of η and μ. Assign 0 to x and 1 to all other variables. Then η and μ must both be given the value 0 and hence x occurs in both η and μ. □

Claim 1. μ is *-singular.

Proof. η is *-singular. Let x occur in η. By assigning 1 to all variables other than x and invoking the fact that $1 \cdot b = b \cdot 1 = b$ for all b in $\mathfrak{A}$, we see that η reduces to x and μ reduces to some term μ' which has the same number of occurrences of x as μ does and $\mathfrak{A} \models x \approx \mu'$. Since $\mathfrak{A}$ is nonabsorptive μ' must just be x. Hence μ is *-singular. □

Claim 2. μ is slender.

Proof. Suppose not. Then μ has a subterm $\phi\psi$ such that at least two variables occur in ϕ and at least two variables occur in ψ. Say these variables are x, y, z, and w. By using the unit to delete all other variables and recalling that $\mathfrak{A}$ is communicative, it follows that

$$\mathfrak{A} \models \eta' \approx (xy)(zw)$$

where η' is one of the following twelve terms:

$x(y(zw))$	$y(x(zw))$	$z(x(yw))$	$w(x(yz))$
$x(z(yw))$	$y(z(xw))$	$z(y(xw))$	$w(y(xz))$
$x(w(yz))$	$y(w(xz))$	$z(w(xy))$	$w(z(xy))$

If η' is in the first two columns delete w (using the unit) to obtain

$$\mathfrak{A} \models (xy)z \approx x(yz)$$

or

$$\mathfrak{A} \models (xy)z \approx y(xz)$$

If η' is in the last two columns delete y (using the unit) to obtain

$$\mathfrak{A} \models x(zw) \approx z(xw)$$

or

$$\mathfrak{A} \models x(zw) \approx w(xz)$$

Thus, noticing the commutativity of $\mathfrak{A}$, we come to associativity. □

Claim 3. η and μ have the same code.

Proof. Let xy be the unique subterm of η such that x and y are variables. Let z be any other variable in η. Now use the unit to delete all other variables. To avoid associativity either xy or yx must be a subterm of μ. Thus the code of η is $\left.\begin{smallmatrix}x\\y\end{smallmatrix}\right\} u_0 \ldots u_{n-1}$ while the code of μ is $\left.\begin{smallmatrix}x\\y\end{smallmatrix}\right\} v_0 \ldots v_{n-1}$. Suppose $u_i \neq v_i$ with i as small as possible, but v_i is u_k. By deleting all variables except x, y_i, and u_k, we obtain

$$\mathfrak{A} \models (xu_i)u_k \approx (xu_k)u_i$$

which yields associativity. □

Now it is easy to see that two slender *-singular terms with the same code form an equation derivable from the commutative law. Thus $\mathfrak{A}$ is inherently nonfinitely based according to Theorem 8'. □

It is very easy to construct finite groupoids which fulfill the hypotheses of Theorem 11. The appendix contains a number of such examples. It is interesting to note that the hypotheses of Theorem 11 can be construed as a single first-order sentence in the language of groupoids. In this view, the condition is simpler than the condition of "varietal congruence distributivity" present in Baker's Finite Basis Theorem that entails a kind of "inherent" finite basis property.

§3. LYNDON'S GROUPOID IS NOT INHERENTLY NONFINITELY BASED.

Lyndon's groupoid L has the following table:

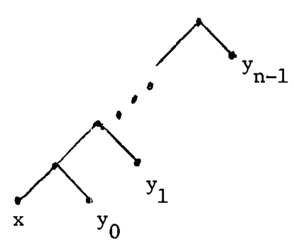
	o	a	b	c	d	e	f
o	o	o	o	o	o	o	o
a	o	o	o	o	o	o	o
b	o	o	o	o	o	o	o
c	o	o	o	o	o	o	o
d	o	d	e	f	o	o	o
e	o	e	e	e	o	o	o
f	o	f	f	f	o	o	o

This, in all essentials, is the first nonfinitely based finite algebra to be discovered. In 1954 Lyndon [4] proved that it is not finitely based. To see, on the other hand, that it fails to be inherently nonfinitely based we will construct an 8 element groupoid $\mathfrak{A}$ which is finitely based and has L as a subalgebra. $\mathfrak{A}$ has the following table:

	o	a	b	c	d	e	f	g
o	o	o	o	o	o	o	o	o
a	o	o	o	o	o	o	o	o
b	o	o	o	o	o	o	o	o
c	o	o	o	o	o	o	o	o
d	o	d	e	f	o	o	o	d
e	o	e	e	e	o	o	o	e
f	o	f	f	f	o	o	o	f
g	o	d	e	f	o	o	o	o

Let $\Sigma = \{x(yz) \approx ww,\ (xx)y \approx zz,\ xy \approx (xy)y,\ (xy)z \approx ((xy)z)y\}$. We will prove that Σ is a base for $\mathfrak{A}$. It is straightforward to verify that $\mathfrak{A} \models \Sigma$. We will provide a proof that if $\mathfrak{A} \models \phi \approx \psi$, then $\Sigma \models \phi \approx \psi$.

Call ϕ a *zero term* provided ϕ has a subterm of theform xx or one of the form $\eta\pi$ where π is not a variable. Every nonzero term θ has a tree rendering of the form



where x and y_0 are different. The *weak code* of θ is obtained from $y_0y_1\cdots y_{n-1}$ by retaining only the leftmost occurrence of each variable.

Claim 0. $\mathfrak{A} \models \phi \approx \psi$ if and only if both ϕ and ψ are zero terms or ϕ and ψ are both nonzero terms with the same leftmost variable and the same weak code.

Proof. Suppose ϕ and ψ are both zero terms. It is easy to see that any assignment from $\mathfrak{A}$ gives both terms the value 0 and so $\mathfrak{A} \models \phi \approx \psi$. Now suppose ϕ and ψ are both nonzero terms with the same leftmost variable and the same weak code. The last two equations in Σ are enough to insure that $\Sigma \vdash \phi \approx \psi$. But $\mathfrak{A} \models \Sigma$, so $\mathfrak{A} \models \phi \approx \psi$.

For the converse, we consider several cases.

Case a. ϕ is a zero term and ψ is a nonzero term.

In this case assign g to the left most variable of ψ and a to all other variables. Under this assignment ϕ is given the value 0 while ψ is given the value d. Hence $\mathfrak{A} \not\models \phi \approx \psi$.

Case b. ϕ and ψ are nonzero terms with different leftmost variables.

In this case assign g to the leftmost variable of ψ and a to all other variables. Under this assignment ϕ is given the value 0 while ψ is given the value d. Hence $\mathfrak{A} \not\models \phi \approx \psi$.

Case c. ϕ and ψ are nonzero terms with the same leftmost variables yet different weak codes.

In this case, suppose the weak code of ϕ is $u_0u_1 \ldots u_{n-1}$ while the weak code of ψ is $v_0v_1 \ldots v_{n-1}$. (Since $\mathfrak{A}$ has a zero, it does no harm to suppose the codes have the same length.) Let i be the least number such that $u_i \neq v_i$. Assign g to the leftmost variable, a to u_j for all $j < i$, b to u_i, and c to all other variables. Under this assignment, ϕ is given the value c while ψ is given the value f. Hence $\mathfrak{A} \not\models \phi \approx \psi$ and the claim is established. □

It remains only to observe that Σ entails all equations of the form described in the claim. The first two equations in Σ handle the zero terms while the second two handle the nonzero terms.

So $\mathfrak{A}$ is finitely based and therefore its subalgebra L is not inherently nonfinitely based. □

§4. OPEN PROBLEMS.

In this section we gather several open problems, some of which have been outstanding for decades and others which are posed here for the first time.

TARSKI'S FINITE BASIS PROBLEM

Fix a finite similarity type which provides at least one operation of rank more than one. Is the set of all finitely based finite algebras (whose universes are sets of natural numbers) of this type recursive?

McKenzie [7] has recently reduced Tarski's Problem to the case of groupoids. Otherwise nothing is known. It is not even known whether the set involved is recursively enumerable or co-r.e.

TARSKI'S HIGH SCHOOL ALGEBRA PROBLEM

Is $(\omega,+,\cdot,\uparrow,0,1)$ *finitely based?*

Here ω denotes the set of natural numbers and $\uparrow$ denotes exponentiation (i.e. $x \uparrow y$ is x^y). Charles Martin [5] has shown the surprising result that $(\omega,+,\cdot,\uparrow,0)$ is not finitely based. More generally, we might ask which reducts of $(\omega,+,\cdot,\uparrow,0,1,!,(\ ),2^x)$ are finitely based, where $\binom{x}{y}$ is the usual binomial coefficient. This algebra has a natural combinatorial appeal.

THE LINEAR SEMIGROUP PROBLEM

Let F *be a finite field and let* F_n *be the semigroup of* $n \times n$ *matrices over* F. *Is* F_n *finitely based?*

Perkins [13] found a six element subalgebra of $GF(2)_2$ which is not finitely based. It is not known whether Perkins' semigroup is inherently nonfinitely based.

THE CHAUTAUQUA PROBLEM

Let A *be a finite set with at least three elements. In the lattice of clones over* A, *is there always an infinite ascending chain* $C_0, C_1, \ldots$ *of finitely generated clones such that* (A, C_i) *is finitely based when* i *is even and not finitely based when* i *is odd?*

Another way to state this problem is to ask whether by adding more and more operations to the set A one can make the resulting algebras alternate between being finitely based and nonfinitely based.

THE CONGRUENCE MODULAR PROBLEM

Is there a finite algebra belonging to a congruence modular variety which is inherently nonfinitely based?

The known examples of nonfinitely based finite algebras in congruence modular varieties all turn out, it seems by necessity, not to be inherently nonfinitely based.

THE REDUCTION PROBLEM

Is there a recursive function F *such that* $F\mathfrak{A}$ *is a finite groupoid for every finite algebra* $\mathfrak{A}$ *and* $F\mathfrak{A}$ *is inherently nonfinitely based if and only if* $\mathfrak{A}$ *is inherently nonfinitely based?*

In particular, we ask whether McKenzie's construction in [7] gives a positive answer to this question. In a related case, we also wonder whether the construction put forward in Pigozzi [8] preserves the inherent nonfinite basis properties.

We conclude by asking whether the algebra constructed by Park [12] is inherently nonfinitely based. (see the note added in proof.)

§5. APPENDIX: SMALL NONFINITELY BASED GROUPOIDS

This appendix lists all of the nonfinitely based groupoids of no more than four elements currently known to the authors. We have omitted various groupoids on the basis of isomorphism and dual isomorphism. Blank boxes mean that any element can be used.

INHERENTLY NONFINITELY BASED GRAPH ALGEBRAS

	o	a	b
o	o	o	o
a	o	o	o
b	o	b	b

Murskii [8],[9]

	o	a	b	c
o	o	o	o	o
a	o	a	a	o
b	o	b	b	b
c	o	o	c	c

Shown nonfinitely based in Shallon [17]

	o	a	b	c
o	o	o	o	o
a	o	a	a	a
b	o	o	b	b
c	o	c	c	c

Shown nonfinitely based in Shallon [17]

INHERENTLY NONFINITELY BASED FOUR ELEMENT GROUPOIDS GENERATING MURSKII'S GROUPOID

	o	a	b	c
o	o	o	o	
a	o	o	a	
b	o	b	b	
c				

The blanks may be filled arbitrarily

	o	a	b	c
o	o	o	o	o
a	o	o	a	a
b	o			
c	o			

The blanks may be filled with any array of b's and c's

	o	a	b	c
o	o	o	o	o
a	o	o	c	o
b	o	b	b	b
c	o	o	c	o

	o	a	b	c
o				
a			a	
b		b	b	
c				

The blanks may be filled with any array of 0's and c's.

These groupoids exhaust the four element groupoids $\mathfrak{A}$ such that Murskii's groupoid belongs to HS $\mathfrak{A}$.

APPLICATIONS OF THEOREM 8

	o	a	b	c
o	o	o	o	o
a	o	o	o	c
b	o	a	o	a
c	o	o	o	o

Shown nonfinitely based in Visin [19]

	o	1	a	b
o	o	o	o	o
1	o	1	a	b
a	o	a	a	o
b	o	b	a	a

Perkins [14]

	o	1	a	a
o	o	o	o	
1	o	1	a	b
a	o	a	o	β
b		b	α	a

$\alpha, \beta \in \{1,a,b\}$

Perkins [14]

	o	1	a	b
o	o	o	o	α
1	o	1	a	b
a	o	a	o	1
b		b		

$\alpha \in \{0,1,b\}$

	o	1	a	b
o	o	o	o	
1	o	1	a	b
a	o	a	o	b
b		b		

$\alpha \in \{0,1,a\}$

	o	1	a	b
o	o	o	o	
1	o	1	a	b
a	o	a	o	o
b		b		

$\alpha \in \{0,1,b\}$

	o	1	a	b
o	o	o	o	
1	o	1	a	b
a	o	a	o	a
b		b		a

LYNDON'S GROUPOID

	o	a	b	c	d	e	f
o	o	o	o	o	o	o	o
a	o	o	o	o	o	o	o
b	o	o	o	o	o	o	o
c	o	o	o	o	o	o	o
d	o	d	e	f	o	o	o
e	o	e	e	e	o	o	o
f	o	f	f	f	o	o	o

Lyndon [4] showed that this groupoid is nonfinitely based. However, it fails to be inherently nonfinitely based.

NONFINITELY BASED GROUPOIDS NOT KNOWN TO BE INHERENTLY NONFINITELY BASED

	o	a	b	c
o	o	o	o	o
a	o	a	b	o
b	o	b	b	c
c	o	o	c	c

Shown by Park [12]
to be nonfinitely based

	o	1	a	b	c	d
o	o	o	o	o	o	o
1	o	1	a	b	c	d
a	o	a	a	b	o	o
b	o	b	o	o	a	b
c	o	c	c	d	o	o
d	o	d	o	o	c	d

This semigroup was shown to be nonfinitely based by Perkins [13]. This is the semigroup of the following six matrices under multiplication.

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

§6 REFERENCES

1. Garrett Birkhoff, *On the structure of abstract algebras,* Proc. Cambridge Phil. Soc. 31 (1935) 433-454.

2. Roger Bryant, *The laws of finite pointed groups,* Bull. London Math. Soc., to appear.

3. Stanley Burris and H. P. Sankappanavar, *A Course in Universal Algebra,* Springer-Verlag, New York, 1981, 276 pp. + xvi.

4. Roger Lyndon, *Identities in finite algebras,* Proc. Amer. Math. Soc. 5 (1954)8-9.

5. Charles Martin, *Equational theories of natural numbers and transfinite ordinals,* Ph.D. thesis, U. C. Berkeley, 1973, 213 pp. + xvi.

6. Ralph McKenzie, *Para primal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties,* Algebra Universal 8 (1978) 336-348.

7. Ralph McKenzie, *A new product of algebras and a type reduction theorem,* Algebra Universalis, to appear.

8. V. L. Murskii, *The existence in three valued logic of a closed class with finite basis not having a finite complete set of identities,* Dokl. Akad. Nauk. SSSR 163 (1965) 815-818; English transl. Soviet Math. Dokl. 6 (1965) 1020-1024.

9. V. L. Murskii, *On the number of* k*-element algebras with one binary operation without a finite basis of identities,* (Russian) Problemy Kibernet 35 (1979) 5-27.

10. Sheila Oates-MacDonald and Michael Vaughan-Lee, *Varieties that make one Cross,* J. Anstral. Math. Soc. (Series A) 26 (1978) 368-382.

11. Sheila Oates-Williams, *Murskii's algebra does not satisfy min,* Bull. Austral. Math. Soc. 22 (1980) 199-203.

12. Robert Park, *A four-element algebra whose identities are not finitely based*, Algebra Universalis 11 (1980) 255-260.

13. Peter Perkins, *Bases for equational theories of semigroups*, J. Algebra 11 (1969) 293-314.

14. Peter Perkins, *Basis questions for general algebras*, preprint.

15. Don Pigozzi, *Finite groupoids without finite bases for their identities*, Algebra Universalis 13 (1981).

16. S. V. Polin, *On the identities of finite algebras*, Sib. Math. J. 17 (1976) 1356-1366.

17. Caroline Shallon, *Nonfinitely based finite algebras derived from lattices*, Ph.D. Dissertation, U.C.L.A. 1979, 144 pp. + viii.

18. Michael Vaughan-Lee, *Laws in finite loops*, Algebra Universalis 9 (1979) 269-280.

19. V. V. Visin, *Identical transformations in four-place logic*, Dokl. Akad. Nauk. SSSR 150 (1963) 719-721.

Department of Mathematics and Statistics
University of South Carolina
Columbia, South Carolina 29208

Space Flight Mechanics Department
Hughes Aircraft Corporation
P. O. Box 92919
Los Angeles, California 90009

Note Added in Proof:

By extending the methods discussed here for graph algebras, Kirby Baker has been able to show that the algebra of is inherently nonfinitely based. In view of the reasoning in Theorem 4, most finite graph algebras turn out to be inherently nonfinitely based. Baker has also proven that Park's groupoid is inherently nonfinitely based.

TENSOR PRODUCTS OF BOOLEAN ALGEBRAS

R. S. Pierce

1. INTRODUCTION. For a Boolean algebra A, let $[A]$ be the isomorphism class of A. The set B of all isomorphism classes of countable Boolean algebras is a commutative semiring under the addition induced by the direct product and the multiplication induced by the tensor product. The class of the one element algebras is a zero in B, and the class of two element algebras is the unit in B. A basic problem in the theory of Boolean algebras is this: what is the structure of B? Recently Vera Trnková proved in [5] that if $t^n = t^m$ in B with $n < m$, then $t^n = t^{n+1}$. An alternative derivation of this result was given by Dobbertin in [1]. In this paper it is shown that Trnková's result is optimal: for each natural number n there exists an element $t \in B$ such that $t, t^2, \ldots, t^{n-1}, t^n$ are distinct and $t^n = t^{n+1}$.

The element t with the desired property will be found in a particular multiplicative subsemigroup of B. Let S be the set of isomorphism classes of countable, primitive Boolean algebras that are finitely structured. (See [2] or [3] for an elaboration of this definition.) It is shown in [3] that S is a subsemiring of B. A non-zero element $x \in S$ is pseudo-indecomposable if $x = y + z$ implies $x = y$ or $x = z$. The set I of all pseudo-indecomposable elements of S is a subsemigroup of the multiplicative semigroup of S. The unity element 1 of S belongs to I. So does the class 0 of all free Boolean algebras. Note that 0 is a multiplicative zero of I, but it is not the zero element of S. The natural ordering of S ($x \leq y$ if $y = x + z$ for some $z \in S$) is a partial ordering. With this relation, I becomes a partially ordered commutative monoid with a zero, that is, if $x \leq y$, then $xz \leq yz$ for all $x, y, z \in I$.

Define $I_1 = \{x \in I\colon\ x + x = x\}$ and $I_2 = I - I_1$. The distributivity of S implies that I_1 is a semigroup ideal of I. The results in Section 6 of [3] show that S can be reconstructed from the data in the pair (I, I_1), or even from I alone.

It is sometimes convenient to describe I_1 by its characteristic function. As in [3], define the mapping $\kappa\colon I \to \{1, 2\}$ by $\kappa(x) = 1$ if $x \in I_1$ and $\kappa(x) = 2$ if $x \in I_2$.

2. PROPERTIES OF I. The statement of the principal theorem in this section uses notation that is applicable to any partially ordered set.

For $x \in I$, denote $\delta(x) = \{y \in I\colon\ y \leq x\}$. It is possible to show that the ordered set $\delta(x)$ is the structure diagram associated with the primitive algebras in the class x (see [2]). By the definition of S, $\delta(x)$ is finite for every $x \in I$. Define $\gamma(x)$ to be the set of $y \in I$ such that x covers y. It follows that $\gamma(x)$ is a finite antichain in $\delta(x)$. The height $h(x)$ is defined as usual to be the maximum length of a chain below x. Thus, $h(x) = 0$ if and only if x is minimal in I.

For each set $W \subseteq I$ let $\mu(W)$ denote the collection of maximal elements in W. This notation will generally be used when W is finite and not empty. In this case, $\mu(W)$ is a non-empty, finite antichain. For $x, y \in I$ define $\Gamma(x, y) = \mu(x\gamma(y) \cup y\gamma(x))$.

Let Ω denote the collection of all finite antichains in I. If $W \in \Omega$, then $\gamma^{-1}(W) = \{x \in I\colon \ \gamma(x) = W\}$.

2.1 THEOREM. *The set* I *is a partially ordered, commutative monoid with* 0, *and* (I, I_1) *satisfies the axioms:*

A1. 0 *and* 1 *are minimal elements of* I *with* $\kappa(0) = 1$ *and* $\kappa(1) = 2$;

A2. *if* $0 \neq x \in I$, *then* $x \geq 1$;

A3. $\delta(x)$ *is finite for all* $x \in I$;

A4. $I-\{0\}$ *is distributive: if* $0 \neq x \leq y_1y_2$, *then there exists* $z_1 \leq y_1$ *and* $z_2 \leq y_2$ *such that* $x = z_1z_2$;

B. *For each* $W \in \Omega$, *if* $W = \{z\} \subseteq I_1$, *then* $\gamma^{-1}(W) = \emptyset$; *otherwise* $\gamma^{-1}(W) = \{x_W, y_W\}$, *where* $\kappa(x_W) = 1$ *and* $\kappa(y_W) = 2$;

C. *If* $\Gamma(x, y) = \{z\} \subseteq I_1$, *then* $xy = z$; *otherwise* $\gamma(xy) = \Gamma(x, y)$ *and* $\kappa(xy) = \min\{\kappa(x), \kappa(y)\}$.

Proof. Most of these properties of I were mentioned in [3]. The statement that I is a partially ordered, commutative monoid with zero 0 and the axiom A_2 are contained in [3; 10.6]. The first part of axiom A1 was noted on page 55 of [3]. It is clear from the definition of addition in S that $0 + 0 = 0$ and $1 + 1 \neq 1$, so that $\kappa(0) = 1$ and $\kappa(1) = 2$. Axiom A3 is a direct consequence of [3; 10.3]. A careful examination of the definitions in [3] shows that axiom B follows from [3; 9.6, 9.7, 10.2, and 10.3]. Finally, axiom A4 follows from the other axioms by induction on $h(x) + h(y)$.

2.2 COROLLARY. (a) *If* $x \in I - \{0\}$ *and* $y \in I$, *then* $xy \geq y$.

(b) *If* $x \in I - \{0\}$, *then* $1 \leq x \leq x^2 \leq x^3 \leq \cdots$; *if* $x^n = x^m$ *for some* $m > n$, *then* $x^n = x^{n+1} = \cdots$.

(c) *If* $x, y \in I$ *satisfy* $\gamma(x) = \gamma(y)$ *and* $\kappa(x) = \kappa(y)$, *then* $x = y$.

These facts follow directly from the theorem.

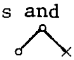
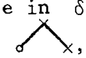
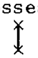
2.3 COROLLARY. *If* $x, y \in I$ *are such that there is an order isomorphism* $\phi\colon \ \delta(x) \to \delta(y)$ *satisfying* $\kappa(\phi(z)) = \kappa(z)$ *for all* $z \in \delta(x)$, *then* $x = y$.

Proof. If $h(x) = 0$, then $x = 0$ or 1 by axiom A2. In this case, $y =$

$\phi(x) = x$ by A1. Assume that the corollary is true for all $z \in I$ with $h(z) < h(x)$. In particular, $\phi(z) = z$ for all $z < x$. It follows from Corollary 2.2(c) that $y = \phi(x) = x$.

A more elaborate form of this argument shows that the axioms A, B, and C characterize the relational system $(I: \cdot, \leq, I_1)$. The proof of this fact is omitted because the result will not be used here.

By Corollary 2.3, each element $x \in I$ is uniquely determined by the Hasse diagram of $\delta(x)$ together with a labeling of the vertices in the diagram to distinguish $\delta(x) \cap I_1$ from $\delta(x) \cap I_2$. It is convenient to designate the vertices in $\delta(x) \cap I_1$ by small circles and those in $\delta(x) \cap I_2$ by crosses. For example,

, , , and 

represent all elements of height 1 in I.

3. TORSION ELEMENTS. Define the order of $x \in I - \{0, 1\}$ to be $O(x) = \sup\{n \leq \infty\colon\ x^{n-1} < x^n\}$. By convention, $O(0) = O(1) = 0$. The element $x \in I$ is a torsion element if $O(x) < \infty$. The set of all torsion elements in I is denoted by T.

It is clear from Corollary 2.2 that $x \in T$ if and only if there is an upper bound on the heights of the elements x^n. This observation and the commutativity of I imply the following result.

3.1 THEOREM. T *is an order convex submonoid of* I, *that is,* $y \leq x \in T$ *implies* $y \in T$.

An element $e \in T - \{0\}$ is idempotent if $e^2 = e$, that is $O(e) \leq 1$. Let E be the set of all idempotent elements in T. Clearly, E is a submonoid of T. Note that $0 \notin E$.

3.2 THEOREM. *With the ordering inherited from* T, E *is a distributive lattice in which the join is the semigroup product.*

This theorem is a special case of Corollary 3.7 in [4], since $I - \{0\}$ satisfies the axioms 1.1 of that paper.

The main theorems of this section and Section 4 refer to the elements that occur in the following Hasse diagram. The coverings that aren't shown in this figure are: $\gamma(p_j) = \{p_{j-1}\}$ for $2 \leq j \leq n+1$, $\gamma(e_k) = \{p_{k-1}, e_{k-1}\}$ for $1 \leq k \leq n+2$, $\gamma(s_i) = \{p_{n+1}, e_{i+1}\}$, $\gamma(f_i) = \{s_i, e_{n+2}\}$ for $i < n$; moreover, $\kappa(p_j) = 2$ for $2 \leq j \leq n+1$, $\kappa(e_k) = 1$ for $0 \leq k \leq n+2$, and $\kappa(s_i) = \kappa(f_i) = 1$ for $i < n$.

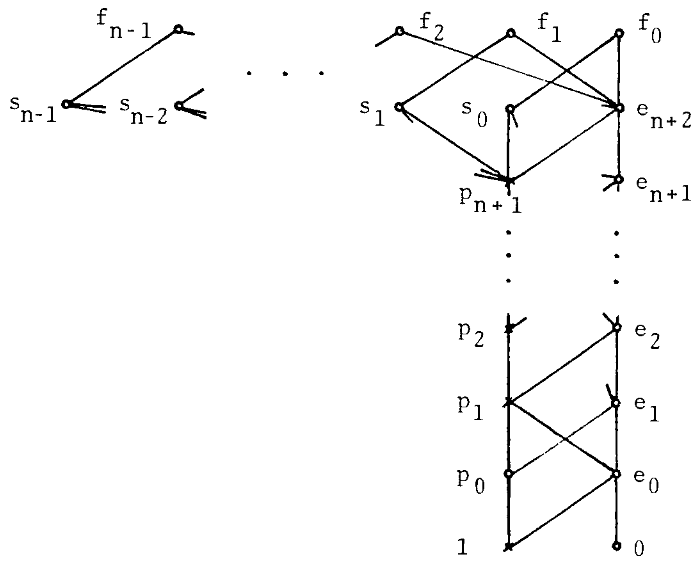


FIGURE 1

3.3. LEMMA. *Figure* 1 *is the diagram of a convex subset of* I. *Moreover:*

(a) $p_0^2 = p_0$, $e_0^2 = e_0$;

(b) $p_ie_0 = e_{i+1}$ *for* $i \leq n+1$;

(c) $p_ip_0 = e_{i+1}$ *for* $1 \leq i \leq n+1$;

(d) $p_ip_j = e_{j+1}$ *for* $1 \leq i \leq j \leq n+1$;

(e) $e_ip_j = e_{j+1}$ *for* $1 \leq i \leq j \leq n+1$; *and* $e_ip_j = e_i$ *for* $0 \leq j < i \leq n+2$;

(f) $e_ie_j = e_j$ *for* $0 \leq i \leq j \leq n+2$;

(g) $f_i = s_ip_j = s_ie_k = s_i^2 = f_ip_j = f_ie_k = f_is_i = f_i^2$ *for* $i < n$, $j \leq n$, *and* $k \leq n+2$.

Proof. Inspection of the diagram in Figure 1 shows that it satisfies the axioms A1, A2, A3, and B of Theorem 2.1. Thus, it is the Hasse diagram of an order convex subset of I. The equations (a) through (g) are obtained by successive application of the axioms A, B, and C. For example, $\Gamma(p_0, p_0) = \{p_0\} \subseteq I_1$ and $\Gamma(e_0, e_0) = \{e_0\} \subseteq I_1$ imply (a). Also, $\Gamma(p_0, e_0) = \{p_0, e_0\}$ yields $p_0e_0 = e_1$ by Corollary 2.2. Hence $\Gamma(p_1, e_0) = \mu\{p_0e_0, e_0^2, p_1, 0\} = \{p_1, e_1\}$, so that $p_1e_0 = e_2$. Induction on $j \geq 2$ gives $\Gamma(p_j, e_0) = \{p_j, e_j\}$. Hence, $p_je_0 = e_{j+1}$ for $j \leq n+1$. A similar argument proves (c). The equation (d) can be proved first in the case $i = 1$ by induction on j, then in general for $1 < i \leq j$ by induction on $i + j$. The equations of (e) follow from (a), (b), (c), and (d): if $i < j$, then $p_ie_j = p_ip_{j-1}e_0 = e_je_0 = p_{j-1}e_0^2 = p_{j-1}e_0 = e_j$; if $1 \leq j \leq i$, then $p_ie_j = p_ip_{j-1}e_0 = e_{i+1}e_0 = e_{i+1}$. The same argument gives (f). To obtain (g), note that $\Gamma(s_i, p_0) =$

$\mu\{s_i, e_{i+1}p_0, p_{n+1}p_0\} = \{s_i, e_{n+2}\} = \Gamma(s_i, e_0)$. Thus, $s_ip_0 = s_ie_0 = f_i$. Hence, $\Gamma(s_i, p_1) = \mu\{s_ip_0, s_ie_0, p_{n+1}p_1, e_{i+1}p_1\} = \{f_i\}$, and $s_ip_1 = f_i$. Induction on $j \geq 2$ then gives $s_ip_j = f_i$. Moreover, if $j \geq 1$, then $s_ie_j = s_ip_{j-1}e_0 = f_ie_0 = s_ie_0^2 = s_ie_0 = f_i$. Therefore, $\Gamma(s_i, s_i) = \mu\{s_ip_{n+1}, s_ie_{i+1}\} = \{f_i\}$, which implies $s_i^2 = f_i$. The rest of the equations in (g) follow from the earlier results: $f_ie_k = s_ie_0e_k = s_ie_k = f_i$, $f_ip_j = s_ie_0p_j = s_ie_{j+1} = f_i$, $f_is_i = s_i^2e_0 = f_ie_0 = f_i$, and $f_i^2 = s_i^2e_0^2 = f_ie_0 = f_i$.

This lemma shows that $\{e_{n+2}, f_0, f_1, \ldots, f_{n-1}\} \subseteq E$. Clearly, $f_i \wedge f_j = e_{n+2}$ in E, so that $\{f_0, f_1, \ldots, f_{n-1}\}$ generates a finite Boolean subalgebra of E. Indeed, it follows easily from the distributivity of E (Theorem 3.2) that the mapping $Y \to \Pi_{i\in Y}f_i$ is an injective lattice homomorphism from the Boolean algebra of all subsets of $\{0, 1, \ldots, n-1\}$ to E. This discussion proves the next result.

3.4 THEOREM. *For each natural number* n, E *contains a sublattice that is isomorphic to the finite Boolean algebra with* n *atoms.*

3.5 COROLLARY. *Every finite distributive lattice is isomorphic to a sublattice of* E.

The corollary follows from the theorem because every finite distributive lattice can be embedded in a finite Boolean algebra.

As Hans Dobbertin has pointed out in a private communication, Theorem 3.4 already settles the question of the existence of a countable Boolean algebra A such that $A^{\otimes i} \not\cong A^{\otimes j}$ if $i, j \leq n$ and $A^{\otimes n} \cong A^{\otimes(n+1)}$: let A be any algebra in the class $x = f_0 + f_1 + \ldots + f_{n-1} \in S$. In fact, since $f_i \in E$ for $i < n$, it follows from Theorems 3.2 and 3.4 that $x^i \neq x^j$ if $1 \leq i < j \leq n$, and $x^n = f_0f_1 \ldots f_{n-1} = x^{n+1}$. The construction in the next section yields an element in T that has the same property.

4. THE MAIN THEOREM.

4.1 THEOREM. *For every natural number* m *there exists* $t \in T$ *such that* $O(t) = m + 1$.

For $m = 1$ this result was established in Example 10.15 of [3]. Therefore, assume that $m \geq 2$.

The explicit construction of the desired $t \in T$ is based on Figure 1 and Lemma 3.3 with $n = 2m$. Denote $X = \{0, 1, \ldots, 2m - 1\}$. Define $f(Y) = \Pi_{i\in Y}f_i$ (in particular, $f(\emptyset) = 1$) and $g(Y) = f(X - Y)$ for each $Y \subseteq X$. Abbreviate $g(\{i_g, \ldots, i_k\})$ by $g(i_g, \ldots, i_k)$. Let $\Gamma = \{g(0), g(1, 2), g(1, 3, 4), \ldots, g(1, 3, \ldots, 2i-1, 2i), \ldots, g(1, 3, \ldots, 2m-3, 2m-2), g(1, 3, \ldots, 2m-3, 2m-1)\}$. By the proof of Theorem 3.4, Γ_m is an antichain in T. Thus, by axiom B, there is a unique element $t \in I$ such that $\gamma(t) = \Gamma$ and $\kappa(t) = 1$. The rest of this section is devoted to the proof that $O(t) = m + 1$.

The following useful observation is clear from Lemma 3.3 and the definition of g.

4.2 LEMMA. *If* $Y \subseteq X$ *and* $i \in X$, *then* $g(Y)f_i = g(Y)$ *if* $i \notin Y$ *and* $g(Y)f_i = g(Y - \{i\})$ *if* $i \in Y$.

Let $V = \delta(f_0 f_1 \cdots f_{2m-1})$. Plainly, V includes the elements in Figure 1, so that Lemma 3.3 gives some information about the multiplicative structure of this set. Somewhat more is needed.

4.3 LEMMA. (a) $s_i s_j = s_i f_j = f_i f_j$ *for all* $i, j < 2m$.

(b) *If* $Y = \{i_1, \ldots, i_k\}$ *with* $0 \le i_1 < \ldots < i_k < 2m$, $k \ge 2$, *then* $\gamma(f(Y)) = \{f(Y - \{i_1\}), \ldots, f(Y - \{i_k\})\}$; *moreover, if* $Y, Y' \subseteq X$, *then* $f(Y) \ge f(Y')$ *if and only if* $Y \supseteq Y'$.

(c) $V = \{0, 1\} \cup \{p_j\colon\ j \le 2m\} \cup \{e_k\colon\ k \le 2m + 1\} \cup \{s_i\colon i < 2m\} \cup \{f(Y)\colon Y \subseteq X\}$.

<u>Proof</u>. The case $i = j$ of (a) is contained in Lemma 3.3. Assume that $i \ne j$. By Lemma 3.3, $\Gamma(s_i, s_j) = \{f_i, f_j\}$. Hence, $\gamma(s_i s_j) = \{f_i, f_j\}$ and $\kappa(s_i s_j) = 1$. It follows that $\Gamma(s_i, f_j) = \{s_i s_j\}$, so that $s_i f_j = s_i s_j$. Moreover, $\Gamma(f_i, f_j) = \{f_i s_j, s_i f_j\} = \{s_i s_j\}$, so that $f_i f_j = s_i s_j$ also. To prove (b), note that (a), Lemma 3.3, and induction yield $\Gamma(f(Y - \{i_k\}), s_k) = \{f(Y - \{i_1\}), \ldots, f(Y - \{i_{k-1}\}), f(Y - \{i_k\})\}$. Thus $\gamma(f(Y)) = \gamma(f(Y - \{i_k\})s_k) = \{f(Y - \{i_1\}), \ldots, f(Y - \{i_k\})\}$, since $k \ge 2$. The second part of (b) restates the remark that was made in the proof of Theorem 3.4. Let U be the set on the right side of equation (c). Clearly, $U \subseteq V$. On the other hand, if $x \in U$, then $\gamma(x) \subseteq U$ by (b). Thus, U is order convex, and since $f_0 f_1 \cdots f_{2m-1} \in U$, it follows that $V \subseteq U$.

For each natural number r, define $V_r = \{t^r x\colon\ x \in V\}$ and let $V_0 = V$. The next lemma determines the order structure of V_1.

4.4 LEMMA. (a) $t \notin V$.

(b) $tp_j = te_k = t$ *for all* $j \le 2m$, $k \le 2m + 1$.

(c) $ts_i = tf_i$ *for all* $i < 2m$.

(d) $tf_{2m-2} = tf_{2m-1}$.

(e) *If* $Y, Y' \subseteq \{0, 1, \ldots, 2m - 2\}$, *then* $tf(Y)$ *covers* $tf(Y')$ *if and only if* Y *covers* Y' *(that is,* $Y \supseteq Y'$ *and* $|Y| = |Y'| + 1$*); moreover,* $tf(Y) \ge tf(Y')$ *if and only if* $Y \supseteq Y'$.

(f) $\gamma(t^2) = \{tg(0), tg(1, 2), \ldots, tg(1, 3, \ldots, 2m-5, 2m-4), tg(1, 3, \ldots, 2m-5, 2m-3)\}$.

<u>Proof</u>. By Lemma 4.3 and Figure 1, $\gamma(x) \ne \Gamma$ for all $x \in V$. Thus, $t \notin V$.

Induction on j and k together with Lemma 3.3 yields $\Gamma(t, p_j) = \Gamma(t, e_k) = \{t\}$ for all j and k. Since $\kappa(t) = 1$, this observation proves (b). To prove (c), note that by (b) and Lemma 4.3, $\Gamma(t, s_i) = \mu\{\Gamma s_i, t\} = \mu\{\Gamma f_i, t\}$. Hence, $\Gamma(t, f_i) = \mu\{\Gamma f_i, ts_i\} = \{ts_i\}$, and (c) follows by axiom C. It is clear from Lemma 4.1 and the definition of Γ that $\Gamma(t, s_{2m-2}) = \mu\{\Gamma f_{2m-2}, t\} = \{g(1, 3, \ldots, 2m-3), t\} = \Gamma(t, s_{2m-1})$. Thus, $\gamma(tf_{2m-2}) = \gamma(ts_{2m-2}) = \gamma(ts_{2m-1}) = \gamma(tf_{2m-1})$, which implies that $tf_{2m-2} = tf_{2m-1}$. More generally, Lemma 4.1 implies that $\Gamma(t, s_{2i}) = \{g(1, 3, \ldots, 2i - 1), t\}$ for $i < m$ and $\Gamma(t, s_{2i-1}) = \{t, g(1, 3, \ldots, 2i - 3, 2i), g(1, 3, \ldots, 2i - 3, 2i + 1, 2i + 2), \ldots\}$ for $1 \leq i < m$. Thus, by (c) $tf_0, tf_1, \ldots, tf_{2m-2}$ are distinct elements that cover t. This observation starts the induction that leads to (e). In fact, let $Y = \{i_1, \ldots, i_k\}$ with $0 \leq i_1 < \ldots < i_k < 2m - 1$ and $k \geq 2$. By Lemma 4.2, 4.3, and the induction hypothesis (on $|Y|$), $\Gamma(t, f(Y)) \cap V_1 = \mu(t\gamma(f(Y))) = \{tf(Y - \{i_1\}), \ldots, tf(Y - \{i_k\})\}$. Thus, $\gamma(tf(Y)) \cap V_1 = \{tf(Y - \{i_1\}), \ldots, tf(Y - \{i_k\})\}$, which is the first half of (e). Also, if Y and Y' are distinct sets of cardinality k, then $tf(Y)$ and $tf(Y')$ are distinct elements of height $k + h(t)$. It follows by induction that the mapping $Y \to tf(Y)$ is an order isomorphism on the sets of cardinality at most k in $\{0, 1, \ldots, 2m - 2\}$. Finally, by (d), (e), and Lemma 4.2, $\gamma(t^2) = \Gamma(t, t) = \{tg(0), tg(1, 2), \ldots, tg(1, 3, \ldots, 2m - 5, 2m - 4), tg(1, 3, \ldots, 2m - 5, 2m - 3)\}$.

This lemma shows that the mapping $Y \to tf(Y)$ is an order isomorphism from the lattice of subsets of $\{0, 1, \ldots, 2m - 2\}$ to V_1. For $1 \leq r \leq m$, the order structure of V_r is similar. This will be proved by induction on r. More notation is needed. For $1 \leq r \leq m$, let $X_r = \{0, 1, \ldots, 2m - 2r\}$.

4.5 LEMMA. *Let* $1 \leq r \leq m$.

(a) $t^r \notin V_{r-1}$.

(b) $t^r f_{2m-1} = t^r f_{2m-2} = \ldots = t^r f_{2m-2r+2} = t^r$.

(c) $t^r f_{2m-2r} = t^r f_{2m-2r+1}$.

(d) *If* $Y, Y' \subseteq X_r$, *then* $t^r f(Y)$ *covers* $t^r f(Y')$ *if and only if* Y *covers* Y'; *moreover,* $t^r f(Y) \geq t^r f(Y')$ *if and only if* $Y \supseteq Y'$.

(e) $\gamma(t^{r+1}) = \{t^r g(0), t^r g(1, 2), \ldots, t^r g(1, 3, \ldots, 2m - 2r - 3, 2m - 2r - 2), t^r g(1, 3, \ldots, 2m - 2r - 3, 2m - 2r - 1)\}$ *if* $r < m$; *and* $t^{m+1} = t^m f_0$.

<u>Proof</u>. Lemma 4.4 includes the case $r = 1$ of this lemma, since (b) is vacuous if $r = 1$. Assume that $r > 1$ and the lemma is true when $r - 1$ replaces r. Since $r \leq m$, the set X_{r-1} includes 0, 1, and 2. Thus, by the induction hypothesis, t^r covers $t^{r-1}g(0)$ and $t^{r-1}g(1, 2)$. Therefore (by $(d)_{r-1}$), t^r cannot have the form $t^{r-1}f(Y)$ for a subset Y of X_{r-1}. Consequently, $t^r \notin V_{r-1}$ by Lemma 4.4 and the induction hypothesis. By Lemmas 4.2, 4.4, and $(e)_{r-1}$, $\Gamma(t^r, f_{2m-2r+2}) = \{t^r\}$. Hence, $t^r f_{2m-2r+e} = t^r f_{2m-2r+2} = t^r$. Together with the

induction hypothesis, this equation yields (b). The use of $(e)_{r-1}$ and Lemmas 4.2, 4.3, and 4.4 gives $\Gamma(t^r, s_{2m-2r}) = \{t^r, t^{r-1}g(1, 3,\ldots, 2m - 2r - 1)\} = \Gamma(t^r, s_{2m-2r+1})$. Hence, $t^r f_{2m-2r} = t^r s_{2m-2r} = t^r s_{2m-2r+1} = t^r f_{2m-2r+1}$. A similar argument shows that the elements $t^r f_i$, $i \in X_r$, are distinct and each of them covers t^r. The statement $(d)_r$ then follows as in the proof of Lemma 4.4(e). If $r < m$, then $\{0, 1, 2\} \subseteq X_r$, and $\gamma(t^{r+1}) = \Gamma(t^r, t) = \{t^r g(0), t^r g(1, 2),\ldots, t^r g(1, 3,\ldots, 2m - 2r - 3, 2m - 2r - 2), t^r g(1, 3,\ldots, 2m - 2r - 3, 2m - 2r - 1)\}$ by $(e)_{r-1}$, $(b)_r$, $(c)_r$, and $(d)_r$. If $r = m$, then $\Gamma(t^m, t) = \{t^m f_0\}$; in this case $t^{m+1} = t^m f_0$. The induction is complete.

The proof of Theorem 4.1 follows easily from Lemma 4.5. Indeed, this lemma gives $t < t^2 <\ldots< t^m < t^m f_0 = t^{m+1}$, and $t^{m+2} = t^{m+1} f_0 = t^m f_0^2 = t^m f_0 = t^{m+1}$. Thus, $O(t) = m + 1$.

4.6 COROLLARY. *For each natural number* m, *there is a countable, primitive, finitely structured, pseudo-indecomposable Boolean algebra* A *such that* $A^{\otimes i} \not\cong A^{\otimes j}$ *if* $1 \le i < j \le m + 1$ *and* $A^{\otimes(m+1)} \cong A^{\otimes(m+2)}$.

REFERENCES

1. Dobbertin, H., On Vaught's criterion for isomorphisms of countable Boolean algebras, *Algebra Universalis* 14(1982), to appear.
2. Hanf, W., Primitive Boolean algebras, *Proc. Sym. Pure Math.*, vol. 25, Amer. Math. Soc., Providence, R.I., 1974.
3. Pierce, R. S., Compact zero-dimensional metric spaces of finite type, *Mem. Amer. Math. Soc.*, No. 130(1972).
4. Pierce, R. S., Arithmetic properties of certain partially ordered semigroups, *Semigroup Forum*, vol. 11(1975), 115-129.
5. Trnková, V., Isomorphisms of sums of countable Boolean algebras, *Proc. Amer. Math. Soc.* vol. 80(1980), 389-392.

University of Arizona
Tucson, Arizona 85721

G-PRINCIPAL SERIES OF STOCKS IN AN ALGEBRA

Francisco Poyatos

Let $\mathcal{A} = (A,F)$ be an algebra. F is allowed to have both finitary and infinitary operations. A subset $T \subseteq A$ is called a *stock* or *trunk* of $\mathcal{A}$ if for each $f \in F$ of arity α, $f(a_i : i < \alpha) \in T$ whenever $a_i \in T$ for at least one $i < \alpha$. The empty set is a stock and if F contains no nullary operations, then every stock is a subalgebra of $\mathcal{A}$. We say that $z \in A$ is a *distinguished element* of $\mathcal{A}$ if $\{z\}$ is a stock of $\mathcal{A}$. If F contains an operation with arity at least two, then the distinguished element is unique, if it exists.

PROPOSITION 1. *The set of all stocks of* $\mathcal{A}$ *forms a complete sublattice of the Boolean algebra of all subsets of* A.

Proof. Trivial.

We associate with each stock T of $\mathcal{A}$ a congruence $C(T)$ defined by $x\,C(T)\,y$ if and only if $x = y$ or $x,y \in T$. It is easy to see that $C(T)$ is a congruence, which we call the *Rees congruence* generated by T [8]. The only quotient algebras that we consider in this paper are of the form $A/C(T)$. We write A/T for $A/C(T)$ which can be identified with $(A - T) \cup \{z\}$ where z is the distinguished element of A/T.

The next two propositions are versions of the second and third isomorphism theorems. Their proofs are omitted.

PROPOSITION 2. *Let* T *be a stock of* $\mathcal{A}$ *and* $\mathcal{S} = (S,F)$ *a subalgebra then*

i) $\mathcal{T} = (T \cup S, F)$ *is a subalgebra of* $\mathcal{A}$,

ii) T *is a stock of* $\mathcal{T}$ *and* $T \cap S$ *is a stock of* $\mathcal{S}$,

iii) $\mathcal{T}/T \cong \mathcal{S}/(T \cap S)$.

PROPOSITION 3. *Let* K *be a stock of* $\mathcal{A}$ *and let* $h: A \to A/K$ *be the natural isomorphism. Then* h *induces a one-to-one correspon-*

dence between the lattice of all stocks of A *which contain* K *onto the lattice of all non-empty stocks of* A/K. *If* $P \supseteq K$ *is a stock, then* $(A/K)/(P/K) \cong A/P$.

For $x \in A$ let $J(x)$ be the stock generated by x. Define an equivalence relation J by $x\,J\,y$ if $J(x) = J(y)$. For $r \in A$ define $J_r = \{x \in A : J(x) = J(r)\}$ and set $I(r) = J(r) - J_r$ (note $J_r \subseteq J(r)$).

PROPOSITION 4. (i) $I(r) = \{x \in A : J(x) \subsetneq J(r)\}$ (ii) $I(r)$ *is a stock of* A *maximal in* $J(r)$.

Proof. The proof of (i) is easy. To prove (ii) we need to show $I(r)$ is a stock. If it were not there would be a $t \in I(r)$ and $f \in F$ with $z = f(a_i : i < \alpha) \notin I(r)$ for some $\{a_i : i < \alpha\}$ such that $t = a_i$ for some i. Since $t \in J(r)$, $z \in J(r) - I(r)$. Hence $J(z) = J(r)$, so $t \in J(z)$. Clearly $z \in J(t)$. Therefore $J(t) = J(z) = J(r)$, contradicting $t \in I(r)$.

Let B be a subset of A. We call $J(x)/I(x)$, $x \in B$ a *principal factor of* A *over* B. Let R and P be stocks of A with $P \subsetneq R$. We call a finite strictly decreasing chain

(1) $R = S_0 \supset S_1 \supset \cdots \supset S_k = P$

of stocks of A a G-*principal series of* A *from* R *till* P if each S_i is maximal in S_{i-1}. The algebras S_{i-1}/S_i are called the *factors* or *quotients* of the series. If

(2) $R = T_0 \supset T_1 \supset \cdots \supset T_n = P$

is another G-principal series from R till P we say that (1) and (2) are isomorphic if $k = n$ and there is a permutation π on $\{0,1,\ldots,k-1\}$ so that $S_i/S_{i+1} \cong T_{\pi(i)}/T_{\pi(i)+1}$.

THEOREM 1. *Let* $A = (A,F)$ *be any algebra. Let* (R,P) *be a pair of stocks of* A *which admits a* G-*principal series* (1). *The factors of* (1) *are isomorphic (taken in a certain order) to the principal quotients over* R-P. *In particular, any two* G-*principal series from* R *till* P *are isomorphic.*

Proof. We begin with any factor of (1), S_i/S_{i+1}, $i \in \{0,1,\ldots,k-1\}$. Let $m \in S_i - S_{i+1}$, then $J(m) \cup S_{i+1}$ is a trunk of A by proposition (1), so that m belongs to it and it contains S_{i+1}. It contains strictly S_{i+1} and is contained in S_i, so

(3) $J(m) \cup S_{i+1} = S_i$, for all $m \in S_i - S_{i+1}$.

We will now show

(4) $I(m) \subseteq S_{i+1}$.

Let $p \in I(m)$. If p were in $S_i - S_{i+1}$, then by (3) $J(p) \cup S_{i+1} = S_i$ and from this would follow $J(p) = J(m)$, that is $p \notin I(m)$, contradiction. So (4) is valid.

Let us prove that

(5) $I(m) = J(m) \cap S_{i+1}$

From (4) it follows that $I(m) \subseteq J(m) \cap S_{i+1}$. Let $c \in J(m) \cap S_{i+1}$, then $J(c) \subseteq J(m)$, $J(c) \subseteq S_{i+1}$, and for this reason $J(c) \subsetneq J(m)$. By proposition 4 (i), $c \in I(m)$, and we have proved (5).

We now apply the proposition 2, making $T = S_{i+1}$, $S = J(m)$, and obtain in combination with equalities (3) and (5)

$$S_i/S_{i+1} \approx J(m)/I(m), \quad m \in S_i - S_{i+1}.$$

We take in account this easy property of set theory: let B, C, D subsets of the set A such that $C \subseteq B$ and $D \cap (B - C) = \emptyset$, then $B - C = (B \cup D) - (C \cup D)$. As $S_{i+1} \cap J_m = \emptyset$. where $m \in S_i - S_{i+1}$, calling $B = J(m)$, $C = I(m)$, $D = S_{i+1}$, by the above property and formulas (3) and (4), we get

(6) $J_m = J(m) - I(m) = (J(m) \cup S_{i+1}) - (I(m) \cup S_{i+1}) = S_i - S_{i+1}$.

We call $\{S_0 - S_1, S_1 - S_2, \cdots, S_{k-1} - S_k\}$ the partition of R-P originated by the G-principal series (1). It coincides with the classification of R-P modulo J by (6). This is valid for any other G-principal series from R till P, as (2). We compare the partitions of R-P originated by (1) and (2), and obtain that $k = n$ and

$$m_i \in J_{m_i} = S_i - S_{i+1} = T_j - T_{j+1} = T_{\pi(i)} - T_{\pi(i)+1}.$$

So π must be a permutation of $\{0,1,2,...,k-1\}$ and

$$S_i/S_{i+1} \approx J(m_i)/I(m_i) \approx T_{\pi(i)}/T_{\pi(i)+1}$$

for all $i \in \{0,...,k-1\}$.

Given any algebra $A = (A,F)$ and a pair of trunks of it (R,P) so that $R \supsetneq P$ and admits a G-principal series such as (1), we define $\ell_G(R,P) = k$ (length from R till P) (number of terms of the series minus 1). We establish the convention $\ell_G(R,R) = 0$. If $(A,\emptyset)$ admits a G-principal series, then we say that A is of finite G-length, and $\ell_G(A) = \ell_G(A,\emptyset)$. A is G-simple if and only if $\ell_G(A) = 1$.

PROPOSITION 5. *Let*

(7) $R_0 \supseteq R_1 \supseteq R_2 \supseteq \cdots \supseteq R_{p-1} \supseteq R_p$

be a finite decreasing (not necessarily strict) chain of stocks of A.

i) If (R_i,R_{i+1}) *admits* G-*principal series for all* $i \in \{0,1,\dots,p-1\}$ *then* (R_0,R_p) *admits* G-*principal series.*

ii) If (R_0,R_p) *admits* G-*principal series, then* (R_i,R_{i+1}) *admits* G-*principal series for all* $i \in \{0,1,\dots,p-1\}$, *and in both cases:*

iii) $\ell_G(R_0,R_p) = \sum_{i=0}^{p-1} \ell_G(R_i,R_{i+1})$.

Proof. Trivial, consequence of theorem 1.

PROPOSITION 6.

i) Every group with operators (definition in [6]) is G-*simple.*

ii) Every lattice with maximum (or minimum) is G-*simple.*

iii) Every quasigroup (definition in [1]) is G-*simple.*

Proof. Trivial.

An algebra $A = (A,F)$ is G-noetherian (G-artinian), iff the lattice of all its stocks satisfies the ascending (descending, respectively) chain condition [3].

PROPOSITION 7. *If* A *is noetherian (artinian, of finite* G-*length), then every homomorphic image of* A *is noetherian (artinian, of finite length, respectively).*

REFERENCES

[1] S. Burris and H. P. Sankappanavar, A Course in Universal Algebra, Springer, 1981.

[2] A. Clifford and G. Preston, The Algebraic Theory of Semigroups, I. American Math. Society, 1964.

[3] P. Dubreil and M. L. Dubreil-Jacotin, Lecons d'algebre moderne, Dunod, 1961.

[4] G. Grätzer, Universal Algebra, second edition, Springer-Verlag, 1979.

[5] J. A. Green, "On the structure of semigroups", Annals of Math., 54 (1951), 163-172.

[6] A. G. Kurosh, Lectures on General Algebra, Chelsea, 1963.

[7] F. Poyatos, "Generalización de un teorema de J. A. Green a Algebras Universales", Revista Matemática Hispano-Americana, 4a. serie, tomo XL, nº 5,6 (1980), 193-205.

[8] D. Rees, "On semi-groups", Proc. Cambridge Phil. Soc., 36 (1940), 387-400.

Madrid,
Instituto "Jorge Juan" de
Matemáticas
C.S.I.C.
c/ Serrano, 123
MADRID-6

ALGEBRAS OF FUNCTIONS FROM PARTIALLY ORDERED SETS INTO DISTRIBUTIVE LATTICES

Anna Romanowska

In 1979, in a letter to J. D. H. Smith [10], I. G. Rosenberg proposed as a possible example of a meet-distributive bisemilattice the set of functions from a poset P into a distributive lattice L, with join defined pointwise and a multiplication, called convolution, defined as follows: for $f : P \to L$, $g : P \to L$ and $p \in P$, $p(f \circ g) = \sum_{q \le p} [(pf)(qg)+(qf)(pg)]$. (A related kind of convolution was considered in I. G. Rosenberg [9].) This note is devoted to the investigation of such algebras of functions in the case that P and L are finite. In particular a condition is given for the convolution to be associative (precisely in this case the algebras in question are meet-distributive bisemilattices), and the structure of these algebras (both in the genera and in the associative case) is described, using as a starting-point a (join) retraction from the lattice of functions from P into L onto the lattice of order preserving functions from P to L.

1. THE LATTICE $(L^{|P|};+,\cdot)$ OF FUNCTIONS OF P IN L AND THE OPERATION OF CONVOLUTION. For a finite distributive lattice $(L;+,\cdot)$ and a finite partially ordered set $(P;\le)$, let $L^{|P|}$ denote the set of all maps of P to L. Define $f+g$ and fg by

(1.1) $$p(f+g) := pf + pg\ ,$$

(1.2) $$p(fg) := (pf)(pg)\ .$$

It is well known that $(L^{|P|};+,\cdot)$ is a distributive lattice. We define another binary operation - <u>convolution</u> - on the set $L^{|P|}$:

(1.3) $$p(f\circ g) := \sum_{q\le p} [(pf)(qg)+(qf)(pg)]\ .$$

For $l \in L$ let $\underline{l}$ denote the constant map $P \to L$ with value l. Some properties of convolution on $L^{|P|}$ are collected in the following.

PROPOSITION 2.1. *The operation $\circ$ is idempotent, commutative, dis-*

tributes over $+$ *, satisfies the identity*

$$(1.4)\qquad (f\circ g)\circ g = f\circ g$$

and $f\circ \underline{0} = \underline{0}$ *for all* $f \in L^{|P|}$ *.*

Proof. The idempotence of $\circ$ follows from the following: $p(f\circ f) = \sum_{q\le p}(qf)(pf) = pf + \sum_{q<p}(qf)(pf) \ge pf$ and on the other hand (because of distributivity of L) $\sum_{q\le p}(qf)(pf) = (pf)\sum_{q\le p}(qf) \le pf$. Hence $f\circ f = f$. The commutativity of $\circ$ is evident. Now we check the identity (1.4):

$$\begin{aligned}
p((f\circ g)\circ g) &= \sum_{q\le p}[(q(f\circ g))(pg)+(p(f\circ g))(qg)]\\
&= \sum_{q\le p}[(pg)\sum_{r\le q}[(rf)(qg)+(qf)(rg)]+(qg)\sum_{s\le p}[(sf)(pg)+(pf)(sg)]]\\
&= \sum_{r\le q\le p}(pg)(rf)(qg) + \sum_{r\le q\le p}(pg)(qf)(rg) +\\
&\quad \sum_{s,q\le p}(qg)(sf)(pg) + \sum_{s,q\le p}(qg)(pf)(sg)\\
&= \sum_{r\le p}(pg)(rf) + \sum_{r\le p}(pf)(rg) = p(f\circ g)
\end{aligned}$$

the penultimate equality following from $(pg)(sf)(qg) \le (pg)(sf)$ and $(qg)(pf)(sg) \le (pf)(sg)$. We show that $\circ$ distributes over $+$:

$$\begin{aligned}
p(f\circ(g+h)) &= \sum_{q\le p}[(qf)p(g+h)+(pf)q(g+h)]\\
&= \sum_{q\le p}[(qf)(pg+ph)+(pf)(qg+qh)]\\
&= \sum_{q\le p}[(qf)(pg)+(qf)(ph)+(pf)(qg)+(pf)(qh)]\\
&= \sum_{q\le p}[(qf)(pg)+(pf)(qg)] + \sum_{q\le p}[(qf)(ph)+(pf)(qh)]\\
&= p(f\circ g) + p(f\circ h) = p(f\circ g+f\circ h)
\end{aligned}$$

(where, as usual, $f\circ g+f\circ h$ denotes $(f\circ g)+(f\circ h)$). □

An algebra $(A;+,\circ)$ satysfying the conditions of Proposition 1.1 with $(A;+)$ a semilattice will be called a quasiring. In the case tha it contains an element 0 with $a+0 = a$ and $a\circ 0 = 0$, it will be called pointed. Thus, $(L^{|P|};+,\circ,\underline{0})$ is a pointed quasiring.

In general neither of the operations $\circ$ and $\cdot$ distributes over the other. Take for example $P = L = \{0,1\}$, where $0 < 1$ and the functions $\underline{0}$, g, $h \in L^{|P|}$ with $1g = 0h = 1$ and equal 0 otherwise. Then $g\circ h = g$, $g\circ(gh) = g\circ\underline{0} = \underline{0} \ne (g\circ g)(g\circ h) = gg = g$ and $g(g\circ h) = gg = g \ne (gg)\circ(gh) = g\circ\underline{0} = \underline{0}$.

The algebra $(L^{|P|};+,\cdot,\circ)$ can be considered as a lattice ordered groupoid (because $f \le g$ implies $f\circ h \le g\circ h$ for arbitrary f, g, h

$\in L^{|P|}$) with zero $\underline{0}$ i.e. it is a <u>groupoid-lattice</u> as defined by O. Steinfeld [11]. (His representation for algebraic groupoid-lattices is completely different from our approach.)

In general the operation of convolution is not associative. P is a <u>tree</u> if $\downarrow p = \{q \in P \mid q \leq p\}$ is a chain for each $p \in P$. A <u>forest</u> is a disjoint union of trees.

PROPOSITION 1.2. *The convolution* $\circ$ *is associative if and only if the poset* P *is a forest.*

<u>Proof</u>. ($\Leftarrow$) Let $f_1, f_2, f_3 \in L^{|P|}$. Then

$$\begin{aligned} p((f_1\circ f_2)\circ f_3) &= \sum_{q\leq p} [(q(f_1\circ f_2))(pf_3)+(p(f_1\circ f_2))(qf_3)] \\ &= \sum_{q\leq p} [(pf_3) \sum_{r\leq q} [(rf_1)(qf_2)+(qf_1)(rf_2)] + \\ &\quad (qf_3) \sum_{s\leq p} [(sf_1)(pf_2)+(pf_1)(sf_2)]] \\ &= \sum_{r\leq q\leq p} (rf_1)(qf_2)(pf_3) + \sum_{r\leq q\leq p} (qf_1)(rf_2)(pf_3) + \\ &\quad \sum_{q,s\leq p} (sf_1)(pf_2)(qf_3) + \sum_{q,s\leq p} (pf_1)(sf_2)(qf_3) \\ &= \sum_{r\leq q\leq p} \sum_{(i,j,k)\in S_3} (rf_i)(qf_j)(pf_k) , \end{aligned} \tag{1.5}$$

where S_3 is the set of permutations of $\{1,2,3\}$. Now (1.5) does not depend on the order of f_1, f_2, f_3 proving the associativity.

($\Rightarrow$) Suppose P is not a forest. Then there are elements $p, q, r \in P$ with p and q uncomparable and $p < r$, $q < r$. Let $a, b \in L$, $a < b$. Let $f, g, h \in L^{|P|}$ satisfy $pf = qg = rh = b$ and take the value a otherwise. Then $f\circ g = \underline{a}$, $\underline{a}\circ h = \underline{a}$, $f\circ h = h$, $g\circ h = h$ and $(f\circ g)\circ h = \underline{a}\circ h = \underline{a} \neq h = f\circ h = f\circ(g\circ h)$. $\square$

Algebras of the form $(A;+,\circ)$, where both reducts $(A;+)$ and $(A;\circ)$ are semilattices and $\circ$ distributes over $+$ were studied, among others, in [5], [6] and [7] under the name <u>meet-distributive</u> (or $\cdot$-distributive) <u>bisemilattices</u>. Thus the algebra $(L^{|P|};+,\circ)$ is a meet-distributive bisemilattice if and only if P is a forest.

Let us remark that $(L^{|P|}; +,\cdot,\circ)$ gives a generalization of algebras considered by B. H. Arnold [1] and later by J. Jakubik and M. Kolibiar [2].

2. A CONSTRUCTION OF QUASIRINGS. In this section $(L;+,\cdot)$ is a distributive lattice and ℓ its $+$-endomorphism such that:

(i) each congruence class of $\lambda := \ker\ell$ has a greatest element d

and $d\ell = d$;

(ii) the set D of greatest elements of λ-classes is a sublattice of L.

Note that $a \leq a\ell$ for $a \in L$. Moreover, $\ell^2 = \ell$ and each congruence class of λ is a $+$-subsemilattice of L. We define an additional binary operation $\circ$ on L as follows:

$$a \circ b := a(b\ell)+b(a\ell) \ . \tag{2.1}$$

PROPOSITION 2.1. *The algebra* $(L;,+,\circ)$ *is a quasiring.*

<u>Proof</u>. Only (1.4) and the distributivity of $\circ$ over $+$ need to be checked. First, using $b \leq b\ell$, we have

$$\begin{aligned}(a\circ b)\circ b &= (a(b\ell)+b(a\ell))\circ b\\ &= (a(b\ell)+b(a\ell))(b\ell)+((a\circ b)\ell)b\\ &= a(b\ell)+b(a\ell)+((a\circ b)\ell)b \ .\end{aligned}$$

Now it suffices to show that $((a\circ b)\ell)b \leq (a\ell)b$. First $((a\circ b)\ell)b = ((a(b\ell)+b(a\ell))\ell)b = ((a(b\ell))\ell)b+((b(a\ell))\ell)b$. From $a(b\ell) \leq a$ we have $((a(b\ell))\ell)b \leq (a\ell)b$ and from $b(a\ell) \leq a\ell$ also $((b(a\ell))\ell)b \leq ((a\ell)\ell)b = (a\ell)b$.

Now we prove distributivity:

$$\begin{aligned}a\circ(b+c) &= a(b+c)\ell+(a\ell)(b+c)\\ &= a(b\ell)+a(c\ell)+b(a\ell)+c(a\ell)\\ &= a(b\ell)+b(a\ell)\\ &= (a(b\ell)+b(a\ell))+(a(c\ell)+c(a\ell))\\ &= a\circ b+a\circ c \ . \quad \square\end{aligned}$$

Note that for $a, b \in D$, $a\circ b$ is just equal to ab. Indeed, in this case $a = a\ell$, $b = b\ell$ and $a\circ b = ab+ba = ab$. If a, b are in the same λ-class, i.e. $a\ell = b\ell$, then $a\circ b = a(a\ell)+b(b\ell) = a+b$. It follows that $(D;+,\circ)$ coincides with $(D;+,\cdot)$. The λ-classes considered as algebras with fundamental operations $+$ and $\circ$ are semilattices (i.e. bisemilattices satisfying the identity $x+y = x\circ y$). Now we can easily see that the algebra $(L;+,\circ)$ is in the product class $\mathcal{S}*\mathcal{D}$, where $\mathcal{S}$ is the class of semilattices (considered as bisemilattices), and $\mathcal{D}$ is the class of distributive lattices. (For the definition of a product class see [4], and in the case of bisemilattices [7].)

Note that in most cases $(D;+,\circ)$ is not the only subalgebra of $(L;+,\circ)$ that is a lattice. In general, quasirings, and particulary quasirings costructed by means of the construction described in this section, have "many" subalgebras that are lattices or semilattices. To get some hold on the problem, consider the free idempotent commutative groupoid satisfying (1.4) on two generators x, y and the free quasiring on two generators x, y. By standard calculations one can show that the first is a semilattice with 3 elements $x, y, x\circ y$, and the second is a meet-distributive bisemilattice with 6 elements $x, y, x\circ y, x+y, x+x\circ y, y+x\circ y$ (see [5] and [6]). (In the proof, one uses the identities $x+y = (x+y)\circ(x+y) = x+y+x\circ y$ and $x\circ y = (x\circ y)\circ(x+y)$.)

Let a, b be elements of a quasiring. Define $a \leq_\circ b$ if and only if $a\circ b = a$. Write $a \prec_\circ b$ if $a \leq_\circ b$, $a \neq b$, and there is no $c \neq a, b$ such that $a \leq_\circ c \leq_\circ b$.

LEMMA 2.2. *Let* a, b *be elements of a quasiring. If* $a \prec_\circ b$ *or* b *covers* a, *i.e.* $a \prec b$, *then* $(\{a,b\};+,\circ)$ *is a lattice or a semilattice (i.e. bisemilattice with* $x\circ y = x+y$ *)*.

Proof. It follows from [6, Cor. 2.5], since the free quasiring on two generators is a bisemilattice. □

Now consider once more the quasiring $(L;+,\circ)$ constructed at the beginning of this section.

LEMMA 2.3. *Let* $a, b \in L$. *If at least two of the conditions* $a \leq_\circ b$, $a \geq b$, $a\ell = b\ell$ *hold, then all three are satisfied.*

Proof. Let $a\ell = b\ell$. As mentioned before we have $a\circ b = a+b$ and therefore $a \leq_\circ b \Longleftrightarrow a \geq b$. Let $a \leq_\circ b$ and $a \geq b$. Since b is a lower bound for both a and $b\ell$, we have $b(a\ell) = b \leq a(b\ell)$ and $a = a\circ b = a(b\ell)+b(a\ell) = a(b\ell)+b = a(b\ell) \leq b\ell$. Thus $a\ell \leq b\ell^2 = b\ell$ and on account of $b \leq a$ also $b\ell \leq a\ell$ proving $a\ell = b\ell$. □

LEMMA 2.4. *Every convex sublattice of* $(L;+,\cdot)$ *is a subalgebra of* $(L;+,\cdot,\circ)$.

Proof. Apply $ab \leq a\circ b \leq a+b$. □

LEMMA 2.5. *Let* $a, b \in L$. *If* $a \prec b$, *then* $(\{a,b\};+,\circ)$ *is*
(i) the two element lattice $(\{a,b\};+,\cdot)$ *if* $a\ell \neq b\ell$ *or*
(ii) the two element semilattice $(\{a,b\};+,+)$ *if* $a\ell = b\ell$.

Proof. Lemmas 2.3 and 2.4. □

The relation $\leq_\circ$ may be described intrinsically as follows.

LEMMA 2.6. *Let* $a, b \in L$. *Then* $a \leq_\circ b$ *if and only if* $a\ell \leq b\ell$ *and* $(a\ell)b \leq a$.

Proof. $(\Rightarrow)$ From $a = a\circ b = a(b\ell)+b(a\ell) \le b\ell+b \le b\ell$ it follows $a\ell \le b\ell^2 = b\ell$. Using $a \le a\ell \le b\ell$ we get $a = a(b\ell)+b(a\ell) = a+b(a\ell)$ proving $(a\ell)b \le a$.
$(\Leftarrow)$ $a\circ b = a(b\ell)+b(a\ell) = a+b(a\ell) = a$. □

Note that if $a \le_{\circ} b$, then $ab = a(a\ell)b = (a\ell)b$.

LEMMA 2.7. *Let* $a, b \in L$ *and* $a \prec_{\circ} b$. *Then* $(\{a,b\};+,\circ)$ *is*
(i) the two element semilattice $(\{a,b\};+,+)$ *if* $a\ell = b\ell$ *or*
(ii) the two element lattice $(\{a,b\};+,\cdot)$ *if* $a\ell \ne b\ell$.

Proof. If $a\ell = b\ell$, then by Lemma 2.3 $a > b$ and hence $a+b = a\circ b$. Let $a\ell \ne b\ell$. By Lemma 2.6 $a\ell < b\ell$, which implies $a < b$, since $b < a$ would imply $b\ell < a\ell$. □

Now suppose that the congruence λ satisfies the following additional condition:

(iii) each element of D belongs to a maximal chain of $(L;+,\cdot)$ that is entirely contained in D.

LEMMA 2.8. *If the condition (iii) is satisfied in the finite lattice* $(L;+,\cdot)$, *then each* λ*-class is closed with respect to the operation* $\cdot$.

Proof. Let $a, b \in L$ and $a\ell = b\ell$. We only need to show that for uncomparable a and b, $(ab)\ell = a\ell$. Let us suppose that, on the contrary, $(ab)\ell \ne a\ell$. Then, evidently $(ab)\ell < a\ell$. Now the elements $a+(ab)\ell$, $b+(ab)\ell$ and $a+b+(ab)\ell$ are in the λ-class containing a. Moreover $(a+(ab)\ell)+(b+(ab)\ell) = a+b+(ab)\ell$, and $(a+(ab)\ell)(b+(ab)\ell) = ab+a(ab)\ell+b(ab)\ell+(ab)\ell = ab+(ab)\ell = (ab)\ell$. Hence, $(ab)\ell$, $a+(ab)\ell$, $b+(ab)\ell$ and $a+b+(ab)\ell$ form a sublattice of L and are pairwise distinct.

Now, by the condition (iii), there is a $d \in D$ such that $(ab)\ell < d \prec a\ell$. Next, $(a+(ab)\ell)(b+(ab)\ell)d = (ab)\ell d = (ab)\ell$ and

$$\begin{aligned}(a+(ab)\ell)+(b+(ab)\ell)d &= (a+(ab)\ell+b+(ab)\ell)(a+(ab)\ell+d)\\ &= (a+b+(ab)\ell)(a+d)\\ &= (a+b+(ab)\ell)a\ell\\ &= a+b+(ab)\ell.\end{aligned}$$

Hence $(ab)\ell$, $a+(ab)\ell$, $b+(ab)\ell$, $a+b+(ab)\ell$ and $(b+(ab)\ell)d$, if all different, form a nondistributive sublattice of $(L;+,\cdot)$, a contradiction. Hence, since $(ab)\ell \le (b+(ab)\ell)d \le b+(ab)\ell$, it follows that either $(ab)\ell = (b+(ab)\ell)d$ or $(b+(ab)\ell)d = b+(ab)\ell$. If $(b+(ab)\ell)d = b+(ab)\ell$, i.e. $b+(ab)\ell \le d \prec a\ell$, then $d = d\ell = a\ell$, a contradiction.

Consequently $(b+(ab)\ell)d = (ab)\ell$. Similarly, considering the elements $(ab)\ell$, $a+(ab)\ell$, $b+(ab)\ell$, $a+b+(ab)\ell$ and $(a+(ab)\ell)d$, one can show that $(a+(ab)\ell)d = (ab)\ell$. Now, $(ab)\ell$, $a+(ab)\ell$, $b+(ab)\ell$, $a+b+(ab)\ell$, $a\ell$ and d form a sublattice of $(L;+,\cdot)$. If $a+b+(ab)\ell = a\ell$, then $(ab)\ell$, $a+(ab)\ell$, $b+(ab)\ell$, d and $a\ell$ form a modular (nondistributive) lattice; if $a+b+(ab)\ell \neq a\ell$, then $(ab)\ell$, $a+(ab)\ell$, $a+b+(ab)\ell$, $a\ell$ and d form a nonmodular lattice. Both cases give a contradiction. □

If all three conditions (i), (ii) and (iii) are satisfied, the construction of the quasiring $(L;+,\circ)$ from the distributive lattice $(L;+,\cdot)$ thus described will be called the G-construction (G for geometrical - the reason for the name will become clearer at the end of this section). It will play an essential role in the description of the structure of the algebra $(L^{|P|};+,\circ)$ in section 3.

In the last part of this section, consider the case that $(L;+,\circ)$ is a bisemilattice. The next lemma gives a simple sufficient condition for $(L;+,\circ)$ to be a bisemilattice.

LEMMA 2.9. *If the mapping* ℓ *is a* $\circ$*-homomorphism, then* $(L;+,\circ)$ *is a meet-distributive bisemilattice.*

Proof. Indeed,
$$\begin{aligned}(a\circ b)\circ c &= (a(b\ell)+b(a\ell))(c\ell)+(a\circ b)\ell c\\ &= a(b\ell)(c\ell)+b(a\ell)(c\ell)+c(a\ell)(b\ell)\\ &= a(b\circ c)\ell+(a\ell)(b(c\ell)+(b\ell)c)\\ &= a(b\circ c)\ell+(a\ell)(b\circ c)\\ &= a\circ(b\circ c)\ . \quad \square\end{aligned}$$

In the case that all three conditions (i), (ii) and (iii) are satis fied and $(L;+,\circ)$ is a finite bisemilattice, the ordering and covering relations determined by $\circ$ can be characterized by means of the covering relation $\prec$. Let

$$\prec_s \ := \ \prec \ \cap \ \bigcup_{d\in D} (\ell^{-1}(d))^2$$

and

$$\prec_1 \ := \ \prec \ \setminus \ \prec_s \ .$$

PROPOSITION 2.10. *If all three conditions (i), (ii) and (iii) are satisfied and* $(L;+,\circ)$ *is a finite bisemilattice, then* $\prec_\circ$ *is contained in the union of* $\prec_1$ *and the convers* $\succ_s$ *of* $\prec_s$.

Proof. Let $a, b \in L$ and $a \prec_\circ b$. By Lemma 2.7, if $a\ell = b\ell$, then $b \prec a$, and if $a\ell \neq b\ell$, then $a < b$. If both a and b are in D , then it is easy to see that $a \prec b$. Suppose at least one of a and b is not in D , and $a\ell \neq b\ell$. By Lemma 2.6 $a\ell < b\ell$. If

$a\ell \prec b\ell$, then $a \prec b$. Indeed, in this case $a\ell+b = b\ell$, and by Lemma 2.6, $a\ell\cdot b = ab = a$. Since $(L;+,\cdot)$ is distributive, this implies $a \prec b$. Now only the case $a\ell \not\prec b\ell$ remains to be considered. We will show that there is no c such that $a < c < b$. Let us suppose, on the contrary, that such c exists. First note that by (1.4) $a\circ(c\circ a)+a\circ b = c\circ a+a = (c+a)\circ a = c\circ a$. On the other hand $c\circ a \le c+a < b$ implies $a\circ(c\circ a+b) = a\circ b = a$. Hence, by distributivity, $a = c\circ a$, i.e. $a <_\circ c$. This implies $a\ell \neq c\ell$. Evidently $a\ell < c\ell \le b\ell$. Now we consider two cases.

Case 1: $c\ell \neq b\ell$. Since $(L;\circ)$ is a semilattice, $a <_\circ c$ and $a \prec_\circ b$ imply $c\circ b = a$. Now $c\circ(c+b) = c\circ b = a$ and $c\circ c+c\circ b = c+a = c \neq a$, a contradiction.

Case 2: $c\ell = b\ell$. Because of the condition (iii), and since $a\ell \not\prec b\ell$, we can assume that there is a $d \in D$ such that $a\ell < d \prec b\ell$. Now since each λ-class contains only one element of D , both $(cd)\ell$ and $(bd)\ell$ are distinct from $b\ell$. Suppose both $(cd)\ell$ and $(bd)\ell$ are equal to $a\ell$. Then $bd \le a\ell$ and $cd \le a\ell$ imply $bd \le a\ell\cdot b = a$ and $cd \le a\ell\cdot c = a$ (see Lemma 2.6). On the other hand $a\ell < d$ implies $a = a\ell\cdot b \le db$ and $a = a\ell\cdot c \le dc$. Consequently $bd = cd = a$. Now since $d \prec b\ell$, $d+b = d+c = b\ell$. It follows that in the case $b \neq b\ell$, the elements $a, b, c, d, b\ell$ form a non-distributive sublattice of $(L;+,\cdot)$, a contradiction. If $b = b\ell$, then $a\ell \le_\circ a \prec_\circ b$ and $a \le a\ell < b$. Hence $a = a\circ(a\ell+b) = a\circ a\ell+a\circ b = a\ell+a = a\ell$ and $a = a\ell <_\circ d \prec_\circ b\ell = b$, contradicting $a \prec_\circ b$. It follows that $(bd)\ell \neq a\ell$. Consequently $a\ell < (bd)\ell < b\ell$, and we have the situation of case 1 . □

Let $\mathrm{Tr}(\prec_1 \cup \succ_s)$ denote the transitive closure of the union of $\prec_1$ and the converse $\succ_s$ of $\prec_s$. Write $a <_\circ b$ if $a \le_\circ b$ and $a \neq b$.

PROPOSITION 2.11. *Under the same assumptions as in Proposition 2.10,* $<_\circ = \mathrm{Tr}(\prec_1 \cup \succ_s)$.

<u>Proof</u>. The relation $<_\circ \supseteq \mathrm{Tr}(\prec_1 \cup \succ_s)$ follows directly from Lemma 2.5. We will show that $<_\circ \subseteq \mathrm{Tr}(\prec_1 \cup \succ_s)$. Let $a <_\circ b$. Then $a = a_0 \prec_\circ a_1 \prec_\circ \dots \prec_\circ a_{n-1} \prec_\circ a_n = b$. By Lemma 2.2, it follows that there are $i_1, i_2, \dots$ such that $a = a_0 < a_1 < \dots < a_{i_1} > a_{i_1+1} > \dots > a_{i_2} < a_{i_2+1} < \dots \lessgtr a_n = b$. Now if $a_j \prec_\circ a_{j+1}$ and $a_j < a_{j+1}$, then by Proposition 2.10, $a_j \prec a_{j+1}$ and hence $a_j \prec_1 a_{j+1}$; if $a_j \prec_\circ a_{j+1}$ and $a_j > a_{j+1}$, then once more by Proposition 2.10, $a_j \succ a_{j+1}$, and hence $a_j \succ_s a_{j+1}$. It follows that $<_\circ \subseteq \mathrm{Tr}(\prec_1 \cup$

$>\!\!-_s)$. □

Proposition 2.10 gives a simple "geometrical" method of obtaining the diagram of $(L;\circ)$ from the diagram of $(L;+,\cdot)$. First, the diagram of $(D;\circ)$ coincides with the diagram of $(D;+,\cdot)$. Moreover D forms a convex subset in $(L;\circ)$. The λ-classes are semilattices $(x\circ y = x+y)$, so their diagrams in $(L;\circ)$ will be dual to those in $(L;+,\cdot)$ (i.e. drawn "upside down") . What other edges of the diagram of $(L;+,\cdot)$ will be kept in the diagram of $(L;\circ)$? To answer this question, consider elements $a, b, c, d \in L$ that are not all in the same λ-class, not all in D and moreover such that $a -\!\!< b -\!\!< d$ and $a -\!\!< c -\!\!< d$. Because of Lemma 2.8, we can assume without loss of generality that in this case we have just three possibilities:

1. $c\ell = d\ell$ and $a\ell$, $b\ell$, $c\ell$ are distinct;
2. $c\ell = d\ell$, $a\ell = b\ell$ and $a\ell \neq c\ell$;
3. all $a\ell$, $b\ell$, $c\ell$ and $d\ell$ are distinct.

Now using Lemma 2.5, it is easy to see that in case 1, $a <_\circ b <_\circ d -\!\!<_\circ c$, i.e. $a <_\circ c$ but $a \not-\!\!<_\circ c$; in case 2, $b -\!\!<_\circ a <_\circ c$ and $b <_\circ d -\!\!<_\circ c$; in case 3, $a <_\circ b <_\circ d$ and $a <_\circ c <_\circ d$. If $x = x_0 -\!\!<_\circ x_1 -\!\!<_\circ \dots -\!\!<_\circ x_{k-1} -\!\!<_\circ x_k = y$ and $x -\!\!< y$, then by Proposition 2.10, one has $x -\!\!< x_1 -\!\!< \dots -\!\!< x_i >\!\!- x_{i+1} >\!\!- \dots >\!\!- x_k = y$ for some $1 \le i \le k$ By Lemma 2.3, $x_i\ell = x_{i+1}\ell = \dots = y\ell$, and for $j, k < i$, $x_j\ell \neq x_k\ell$. It follows by the case analysis above that the diagram of $(L;\circ)$ has exactly tne same edges as that of $(L;+,\cdot)$, with the exception of edges connecting elements a and c belonging to a subbisemilattice $\{a,b,c,d\}$ described unter case 1 .

3. THE STRUCTURE OF $(L^{|P|};+,\circ)$. In this section it will be shown that the algebra $(L^{|P|};+,\circ)$ can be obtained from $(L^{|P|};+,\cdot)$ by means of the G-construction. As in section 1, P is a finite poset and L a finite distributive lattice. Let L^P denote the subset of $L^{|P|}$ containing all order preserving functions. Note that for order preserving functions $f, g \in L^P$ clearly $f\circ g = fg \in L^P$, so $(L^P;+,\circ)$ is a subalgebra of $(L^{|P|};+,\circ)$ and of $(L^{|P|};+,\cdot)$, and, as is well known, is a (distributive) lattice. Many references for L^P are for example in [3].

Let $f \in L^{|P|}$. The function $f^o := \Pi\{g \in L^P \mid g \ge f\}$ is evidently the least order preserving function such that $f \le f^o$. Some properties of f^o are collected in the following:

LEMMA 3.1. *Let* $f, g \in L^{|P|}$, $p \in P$. *Then* *(i)* $pf^{o} = \sum_{q\le p} qf$;

(ii) $f\circ g = gf^{o}+fg^{o}$;

(iii) $f\circ g = f^{o}g^{o}(f+g)$.

Proof. (i) For each $p \in P$ define $ph := \sum_{q\le p} qf$. It is evident that $f \le h$. We will show that $h \in L^{P}$. Let $s \le p$. Then $sh = \sum_{q\le s} qf \le \sum_{r\le p} rf = ph$. Thus $f \le f^{o} \le h$. Now, it is enough to show that $h \le f^{o}$. Indeed since f^{o} is order preserving and $f \le f^{o}$, it follows that $q \le p$ implies $qf \le qf^{o} \le pf^{o}$, whence $ph = \sum_{q\le p} qf \le \sum_{q\le p} qf^{o} \le pf^{o}$. Consequently $h \le f^{o}$.

(ii) Because of (i), we have the following: for any $p \in P$, $f, g \in L^{|P|}$, $p(f\circ g) = \sum_{q\le p} [(qf)(pg)+(qg)(pf)]$

$$= (pg) \sum_{q\le p} (qf) + (pf) \sum_{q\le p} (qg)$$

$$= (pg)(pf^{o})+(pf)(pg^{o})$$

$$p(qf^{o}+fg^{o}) \ .$$

(iii) Follows from (ii) and $f^{o}f = f$, $g^{o}g = g$. □

LEMMA 3.2. *The mapping* $^{o}: L^{|P|} \to L^{P}$ *is a surjective* $+$*-homomorphism. Moreover, it is also a* $\circ$*-homomorphism if and only if* P *is a forest.*

Proof. Let $f, g \in L^{|P|}$. Since $f, g \le f+g \le (f+g)^{o}$, it follows that $f^{o}+g^{o} \le (f+g)^{o}$. On the other hand from $f+g \le f^{o}+g^{o} \in L^{P}$ we have $(f+g)^{o} \le f^{o}+g^{o}$. Evidently ^{o} is surjective.

Now, let P be a forest, $f, g \in L^{|P|}$, $p \in P$. Using $f^{o}\circ g^{o} = f^{o}g^{o}$ and Lemma 3.1 then $p(f^{o}\circ g^{o})$

$$= (pf^{o})(pg^{o})$$

$$= (\sum_{q\le p} qf)(\sum_{r\le p} rg)$$

$$= \sum_{q,r\le p} (qf)(rg)$$

$$= \sum_{q\le r\le p} [(qf)(rg)+(rf)(qg)]$$

$$= \sum_{r\le p} [\sum_{q\le r} [(qf)(rg)+(rf)(qg)]]$$

$$= \sum_{r\le p} r(f\circ g)$$

$$= p(f\bullet g)^{o}$$

Hence $f^{o}\bullet g^{o} = (f\circ g)^{o}$.

If P is not a forest, it contains a, b, c with $a < c$ and b

$< c$. Define $f, g \in L^{|P|}$ by $af = bg = 1$ and equal 0 otherwise. Then $f \circ g = \underline{0}$ whence $(f \circ g)^{\circ} = \underline{0}$ whereas from $af^{\circ} = cg^{\circ} = 1$ we get $c(f^{\circ} \circ g^{\circ}) = 1$.

Note that $^{\circ}$ need not be a $\cdot$-homomorphism for a general poset P . In the previous example $(fg)^{\circ} = \underline{0}^{\circ} = \underline{0}$ and $f^{\circ}g^{\circ} = f^{\circ} \circ g^{\circ} \neq \underline{0}$.

Next remark, that by Lemma 3.2, $(L^{P};+)$ is a retract of $(L^{|P|};+)$, and if P is a forest, then $(L^{P};+,\circ)$ is a retract of $(L^{|P|};+,\circ)$.

THEOREM 3.3. *For an arbitrary finite poset* P *and arbitrary finite distributive lattice* L *, the quasiring* $(L^{|P|};+,\circ)$ *can be obtained from the lattice* $(L^{|P|};+,\cdot)$ *by means of the* G-*construction.*

<u>Proof</u>. For the lattice $(L^{|P|};+,\circ)$, take $D = L^{P}$ and $\ell = {}^{\circ}$. The conditions (i), (ii) and (iii) of the definition of G-construction can be easily checked using lemmas 3.1, 3.2 and elementary properties of $(L^{|P|};+,\cdot,\circ)$. □

In particular, if P is a forest, $(L^{|P|};+,\circ)$ is a bisemilattice, the ordering relation $\leq_{\circ}$ implied by the $\circ$-semilattice structure of $L^{|P|}$ is described by Proposition 2.11, and the diagram of $(L^{|P|};\circ)$ can be obtained from the diagram of $(L^{|P|};+,\cdot)$ by the procedure described after Proposition 2.11.

Let us note that there is another class of meet-distributive bisemilattices that have a structure similar to that described by the G-construction (although (2.1) does not hold any more and the equivalent of $(L;+,\cdot)$ is semimodular and not distributive in general). This is the class of bisemilattices of pointed subsemilattices of semilattices (see [7] and [8]). In particular Propositions 2.10 and 2.11 hold also in this case.

Acknowledgement. This paper was written while the author held a fellowship from the Alexander von Humboldt Foundation at the Technische Hochschule Darmstadt in West Germany. The author is grateful to I. G. Rosenberg, J. D. H. Smith and R. Wille for helpful discussions and to the reviewer for many valuable suggestions.

REFERENCES

[1] B. H. Arnold, Distributive lattices with a third operation defined, Pac. J. Math., 1(1951), 33-41.

[2] J. Jakubík, M. Kolibiar, Lattices with a third distributive operation, Math. Slovaca, 27(1977), 287-292.

[3] B. Jónsson, Arithmetic of ordered sets, in *Ordered Sets*, ed. I.

Rival, D. Reidel Publ. Company, Dodrecht, 1982.

[4] A. I. Mal'cev, *The methamathematics of algebraic systems*, Collected papers, 1936 - 1967, Studies in Logic and the Foundations of Mathematics, Vol. 66, North-Holland Publishing Co., Amsterdam - London, 1971.

[5] A. Romanowska, On distributivity of bisemilattices with one distributive law, Colloq. Math. Soc. Janos Bolyai, Vol. 29, *Universal Algebra,* Esztergom (Hungary), 1977, 653 - 661.

[6] A. Romanowska, Subdirectly irreducible .-distributive bisemilattices, I, Demonstr. Math., 13(1980), 767 - 785.

[7] A. Romanowska, J. D. H. Smith, Bisemilattices of subsemilattices, J. Algebra, 70(1981), 78 - 88.

[8] A. Romanowska, J. D. H. Smith, On the structure of subalgebra systems of idempotent entropic algebras, preprint.

[9] I. G. Rosenberg, A generalisation of semigroup rings, preprint.

[10] I. G. Rosenberg, a letter to J. D. H. Smith.

[11] O. Steinfeld, Some remarks on algebraic groupoid-lattices, Colloq. Math. Soc. Janos Bolyai, Vol. 14, *Lattice Theory,* Szeged (Hungary), 1974, 413 - 420 .

Anna Romanowska
Warsaw Technical University, Institute of Mathematics, 00 661 Warsaw, Poland
and
Technische Hochschule Darmstadt, Fachbereich Mathematik AG 1, 6100 Darmstadt, West Germany

GALOIS THEORY

FOR PARTIAL ALGEBRAS

I.G.Rosenberg

Most of the results need lengthy definitions and so cannot be adequately described in the introduction. The paper essentially describes the subalgebra systems of direct powers of partial algebras and the partial clones related to them and gives a solution to the joint concrete representation problem (subalgebras-congruences-endomorphisms) for partial algebras.

As a background and to provide an easier introduction to this not widely known topic, we start with a brief review of Krasner's abstract Galois theory for permutation groups, his endotheory for monoids of selfmaps and the polytheory for clones of finitary operations. Here we have a fixed universe A and an index set I and the concept of preservation of a relation (subset of A^I) by a permutation of A, selfmap of A and finitary operation on A and the groups, monoids and clones are just the closed sets in the Galois connection. For the operations the closed sets of relations are the subalgebra systems of the I-th direct power of algebras.

In this paper we study the Galois connection for partial algebras. This seems to be a natural step in the hierarchy of Galois theories which began with the "abstract" theory for permutations [12,13,14,16] followed by the "endotheory" for finitary (finite and infinite) universal algebras [3,7,37] and infinitary universal algebras.

The closed sets of partial operations are partial clones containing all suboperations of its members. On the relational side the subalgebra systems of the I-th direct power of partial algebras can be reasonably well described as algebraic closure systems on A^I closed under special operators called surjective mutations. Such a closure generated by $S \subseteq A^I$ can be built in three steps: first we take all the surjective mutations of members of S; then just close under all intersections and finally under all directed unions. For full algebras and $|I| < |A|$ a similar closure is obtained as a projection from a closure on A^A. This is not necessary for partial algebras and so the closures are much simpler to construct. Thus without much trouble we solve the joint concrete representation problem for subalgebras, congruences and partial endomorphisms of partial algebras.

Some of the results were known earlier [4,7,9] but, in spite of their possible importance, seem to have received only scant attention. Also the situation may be more complicated than it seems at first sight; for example in the very interesting particular case of heterogeneous algebras (touched but far from solved in [22,24, 34]) we lack an explicit Galois theory. Although individual concrete characterizations are known for algebras the analogue of Theorem 3.11 for full algebras remains unknown.

The paper is intended to be self-contained as much as it is possible. As often the case in this field it is somewhat heavy on the terminological and notational side.

The author is grateful to I.Fleischer for many interesting conversations. The partial financial support provided by the NSERC-Canada operating grant A-9128 and FCAC Québec 'subvention d'équipe' E-539 is gratefully acknowledged.

1. PRELIMINARIES.

1.1. Let A be a fixed nonempty universe, I a nonempty index set and A^I the set of maps from I to A (for I finite we identify A^I with the set $A^{|I|}$). A subset ρ of A^I is called an I-*relation* on A. Let S_A denote the set of all permutations of A. We say that $f \in S_A$ *preserves* $\rho \subseteq A^I$ if $f\circ r \in \rho$ for all $r \in \rho$ i.e. if f is an automorphism of ρ. In the Galois connection between S_A and $\underset{\sim}{P}(A^I)$ induced by the correspondence "f preserves ρ" the closed subsets of S_A are the sets of the form

$$\text{Aut } R \ := \ \{f \in S_A\text{: } f \text{ preserves all } \rho \in R\}$$

($R \subseteq \underset{\sim}{P}(A^I)$). The sets Aut R are clearly permutation groups on A and if $|I| \geq |A|$ they comprise all permutation groups on A (M.Krasner 1935 [12-14,16,18]).

1.2. The closed subsets of $\underset{\sim}{P}(A^I)$ are

$$\text{Inv}_I F \ := \ \{\rho \subseteq A^I : f \text{ preserves } \rho \text{ for all } f \in F\}$$

($F \subseteq S_A$). We describe intrinsically the sets $\text{Inv}_I F$. First observe that for a permutation χ of I and $\rho \in \text{Inv}_I F$ the relation

$$\rho\circ\chi \ := \ \{r\circ\chi : r \in \rho\}$$

also belongs to $\text{Inv}_I F$. More generally, we not only can permute coordinate places but also may keep certain coordinates and free the others in the following sense. Let χ be a partial selfmap of I with domain K and $\rho \subseteq A^I$. The mutation $\rho\circ\chi$ is the relation

$$\rho\circ\chi \ := \ \{f \in A^I : f{\restriction}K = r\circ\chi \text{ for some } r \in \rho\}$$

(where $f{\restriction}K$ is the restriction of f to K and $(r\circ\chi)k = r(\chi(k))$ for all $k \in K$). For example, if $I = K = \{1,2\}$ and $\chi(1) = 2$, $\chi(2) = 1$, then $\rho\circ\chi$ is the inverse ρ^{-1} of the binary relation ρ. On the other hand, if $\chi : \{1\} \to \{1,2\}$ is defined by $\chi(1) = 1$, then $\rho\circ\chi = D(\rho)\times A$ where the domain $D(\rho)$ of ρ is defined by

$$D(\rho) \ := \ \{x \in A : (x,a) \in \rho \text{ for some } a \in A\}.$$

Thus the mutations encompass both permuting of coordinates and allowing the values in specific coordinates to become unrestricted. M.Krasner [16] showed that the sets of the form $\mathrm{Inv}_I F$ are exactly the mutation closed complete boolean subalgebras of $(\underset{\sim}{P}(A^I); \subseteq)$. In other words, the sets $\mathrm{Inv}_I F$ are exactly the subsets of $\underset{\sim}{P}(A^I)$ closed under all mutations, the complementation and arbitrary set-theoretical intersections and unions. The above characterizations of the sets Aut R and $\mathrm{Inv}_I F$ is the essence of Krasner's *abstract Galois theory.*

1.3. Some thirty years later Krasner [15-17] studied the same problem for selfmaps of A. In this *Galois endotheory* "f preserves ρ" means that f is an endomorphism of ρ, i.e. $f\circ r \in \rho$ for all $r \in \rho$. For $R \subseteq \underset{\sim}{P}(A^I)$ put

$$\text{End } R \ := \ \{f \in A^I : f \text{ preserves all } \rho \in R\}.$$

The sets of the form End R are submonoids of the symmetric monoid $\langle A^I;\circ\rangle$ and for $|I| \geq |A|$ they comprise all submonoids of $\langle A^I;\circ\rangle$. For $F \subseteq A^I$ define $\mathrm{Inv}_I F$ in the same way as above. This time $\mathrm{Inv}_I F$ need not be closed under complementation and the sets of the form $\mathrm{Inv}_I F$ are exactly the mutation closed complete sublattices of $(\underset{\sim}{P}(A^I); \subseteq)$ [16].

1.4. The next step is to replace selfmaps by finitary operations. This was done for finite algebras by Bodnarčuk et al. [3] and quite independently of Krasner's work by Geiger [7] (the relational constructions were already effectively applied in [28-30]).

Let $\mathbb{N}$ denote the set $\{0,1,\ldots\}$ of non-negative integers. For $n \in \mathbb{N}$ let $\underline{n} = \{0,1,\ldots,n-1\}$ and let $\mathcal{O}^{(n)}$ stand for the set of all n-ary operations on A (i.e. maps $A^n \to A$). Put $\mathcal{O} := \bigcup_{n\in\mathbb{N}} \mathcal{O}^{(n)}$ and for $X \subseteq \mathcal{O}$ and $n \in \mathbb{N}$ write $X^{(n)} := X \cap \mathcal{O}^{(n)}$. We say that $f \in \mathcal{O}^{(n)}$ *preserves* $\rho \subseteq A^I$ (or is a *polymorph* of ρ, *stable* or *admissible* with respect to ρ [19]) if $fr_0\ldots r_{n-1} \in \rho$ whenever all $r_j \in \rho$ (here $r = fr_0\ldots r_{n-1} \in A^I$ is defined by $ri = f(r_0 i)\ldots(r_{n-1}i)$ for every $i \in I$), i.e. if ρ is a subalgebra of the direct power $\langle A;f\rangle^I$. (For n=0 the zero operation f preserves ρ if the constant map with value f belongs to ρ.) For example let $|I| = 2$ and let $\leq$ be a partial order on A. Then f preserves $\leq$ iff f is *monotone* (isotone) with respect to $\leq$, i.e. $fa_1\ldots a_n \leq fb_1\ldots b_n$ whenever $a_i \leq b_i$ for all $i=1,\ldots,n$. Similarly f preserves an equivalence θ on A iff θ is a congruence of $\langle A;f\rangle$ and f preserves $\{(a,\varphi a) : a \in A\}$, φ selfmap of A, iff φ is an endomorphism of $A;f\rangle$.

1.5. For $R \subseteq \underset{\sim}{P}(A^I)$ set

$$\text{Pol } R \ := \ \{f \in \mathcal{O} : f \text{ preserves all } \rho \in R\}.$$

In other words, Pol R is the largest subset F of $\mathcal{O}$ such that R is a subalgebra of

$<A;F>^I$. Each set Pol R is a *clone* (or *polynomial* or *term class*, *Post algebra* or *iterative algebra with identity*) i.e. a composition closed subset of $\mathbb{O}$ containing all projections (for a more detailed definition see 2.2). Moreover, for $|I| \geq |A| \geq \aleph_0$ each clone is of the form Pol R for some $R \subseteq \underset{\sim}{P}(A^I)$ [37] (in fact, of the form Pol ρ for some $\rho \in A^I$ [31]). For A finite it is preferable to use simultaneously relations of all finite artities, e.g. each clone is of the form Pol R where R is a set of finitary relations. For simplicity and because it is closer to the partial case we stick to the case of A infinite.

The set $\underset{\sim}{L}$ of clones ordered by $\subseteq$ is known to be an algebraic lattice whose infinitary meets are the set-theoretical intersections. Relatively little is known otherwise (e.g. for A infinite both $\underset{\sim}{L}$ and the set of dual atoms of $\underset{\sim}{L}$ have cardinality 2exp 2exp$|A|$ [35]).

1.6. On the relational side the closed subsets of $\underset{\sim}{P}(A^I)$ are

$$\mathrm{Inv}_I F = \{\rho \subseteq A^I : f \text{ preserves } \rho \text{ for all } f \in F\}$$

$(F \subseteq \mathbb{O})$ called *subdirect closure systems* on A^I [37]. In other words, $\mathrm{Inv}_I F$ is the subalgebra system $\mathrm{Sub}<A;F>^I$ of the direct power $<A;F>^I$, and as such an algebraic closure system on A^I (i.e. a family of subsets of A^I closed under arbitrary intersections and unions of (up)-directed families [8,p.24]). For their intrinsic description we start with $|I| \geq |A|$. In this case the subdirect closure systems are exactly the mutation closed algebraic closure systems Σ on A^I such that every $f \in \bigcap\Sigma$ is a constant map. For $0 < |I| < |A|$, choose $J \supset I$ such that $|J| = |A|$ and for $\rho \subseteq A^J$ put $\rho^- := \{f \in A^I := g\restriction I$ for some $g \in \rho\}$. The subdirect closure systems on A^I are exactly the restrictions (projections) $S^- := \{\rho^- : \rho \in S\}$ of a subdirect closure system S on A^J [37].

1.7. For $Y \subseteq \underset{\sim}{P}(A^I)$ let [Y] denote the least subdirect closure system on A^I containing Y. Subdirect closure systems play a role in concrete representation problems. For example, consider selfmaps of A as binary relations on A (i.e. identify $f \in A^A$ with its digraph $\{(a,fa): a \in A\}$ and set $I = \underline{2}$. Then a subset X of A^A is the endomorphism monoid of an algebra on A iff $X = A^A \cap [X]$. To construct [X] we must extend the binary relations of X into $|A|$-ary relations, form the subdirect closure system and then project back into binary relations (these constructions are discussed in [38]). The difficulties involved in performing this indicate a reason why the characterization of endomorphism monoids is a hard problem (see e.g. [41]).

Perhaps we could mention now why we think that the above relational approach to clones is not useless. Except for a few very simple cases it is not easy to describe explicitly the clone $\bar{F}$ of term operations of $<A;F>$ (i.e. the least clone containing F), and so a description in the form Pol ρ or Pol R seems to be reasonable. Moreover, some clones are naturally given in the form Pol ρ. This happens for most maximal clones for A finite [28,29,36]; e.g. it would be difficult to define the clone of monotone operations (1.4) in another way. For clones $X_i = \mathrm{Pol}\ R_i$ ($i=1,2$) we have $X_1 \subseteq X_2$ iff $R_2 \subseteq [R_1]$. This observation gives a natural way to construct superclones of a given clone (e.g. the 8 proper superclones of the square of a primal algebra [39] or submaximal clones [40]).

1.8. In this paper we extend the above *Galois polytheory* to partial operations which is the next step in the hierarchy of Galois theories. For a finite A and I this has already been done in [7], for I finite in [9], for operations with finite domains in [26] and some of the results of this paper are in [4]. A natural adaptation of "f preserves ρ" gives a Galois connection which on the side of partial operations has strict partial clones that are the composition closed sets of partial operations containing all projections and closed under the formation of suboperations. On the relational side we have subsets of $\underset{\sim}{P}(A^I)$ which we call weak subdirect closure systems (wscs). They are still algebraic closure systems but are closed only under special mutations (called surjective). Thus in the hierarchy of Galois theories this time the order properties (in $\underset{\sim}{P}(A^I)$, $\subseteq$) remain unchanged but much less is required for mutations. Concretely for $I = \underline{2}$ we have algebraic closure systems Σ on A^2 containing ρ^{-1}, $\rho^* = \{(x_1,x_2) \in A^2 : (x_1,x_1) \in \rho\}$ and $\rho \cap \mathrm{id}_A$ whenever $\rho \in \Sigma$. The mutation $D(\rho)\times A$ (1.2) is missing and there are no projections from systems on A with $|J| = |A|$. To underline this difference consider the relational product $\rho\circ\sigma$ of two binary relations given by the usual

$$\rho\circ\sigma \ := \ \{(x_1,x_2) \in A^2 : (\exists u)\ (x_1,u) \in \rho, \ \ (u,x_2) \in \sigma\}.$$

It is well known and not difficult to prove that for a full algebra <A;F> the subdirect closure system $\mathrm{Inv}_{\underline{2}}F$ contains $\rho\circ\sigma$ whenever it contains both ρ and σ. This is not guaranteed for partial algebras. For example, let $\underline{\underline{A}}$ be a partial algebra and φ a selfmap of A such that $\varphi \in \mathrm{Sub}\ \underline{\underline{A}}^2$. Then the equivalence

$$\ker\varphi \ := \ \varphi\circ\varphi^{-1} \ = \ \{(x_1,x_2) \in A^2 : \varphi x_1 = \varphi x_2\}$$

may not be a congruence of A (e.g. take $<\underline{3};f>$ where the unary operation satisfies $f0 = 0$, $f1 = 2$ and $f2$ undefined and $\varphi 0 = \varphi 1 = 2$, $\varphi 2 = 0$). Similarly $\varphi\circ\varphi$ may not be a subalgebra of $\underline{\underline{A}}^2$.

1.9. For $S \subseteq A^I$ we build the wscs generated by S in three steps. First we close up S under all surjective mutations, then under arbitrary intersections and finally under directed unions. We use this special feature of wscs's for a concrete representation problem for partial algebras discussed in section 3. There we completely characterize the triples G,H,K such that $G = \mathrm{Sub}\ \underline{\underline{A}}$, $H = \mathrm{Con}\ \underline{\underline{A}}$ and $K = \text{P-end}\ \underline{\underline{A}}$ for a partial algebra on A (K is a subset of the set Q of partial selfmaps of A and $\text{P-end}\ A = Q \cap \mathrm{Sub}\ \underline{\underline{A}}^2$). The fact that this was obtained in a relatively straightforward way underlines the difference between full and partial algebras. Another interesting feature is that the partial endomorphisms need not compose.

2. PARTIAL CLONES.

2.1. As usual, for $n \in \mathbb{N}$ an n-ary *partial* operation on A is a map from a subset D_f of A^n (called the *domain* of f) into A. The set of partial operations is denoted $\mathbb{P}^{(n)}$ and $\mathbb{P}$ stands for $\bigcup_{n\in\mathbb{N}} \mathbb{P}^{(n)}$. We say that $f \in \mathbb{P}^{(n)}$ is a *sub-operation* of $g \in \mathbb{P}^{(n)}$, in symbols $f \prec g$, if $g \upharpoonright D_f = f$ i.e. if $D_f \subseteq D_g$ and $fx = gx$ for all $x \in D_f$. For $X \subseteq \mathbb{P}$ the pair $\langle A;X\rangle$ is called a *partial algebra* and we write $X^{(n)}$ for $X \cap \mathbb{P}^{(n)}$ $(n \in \mathbb{N})$.

2.2. Even for full algebras the composition of operations has been formally defined in many ways. Our description of the composition of partial operations is a variation of Mal'cev's preiterative algebras [20] which seems to be as good as any other description. First we define three unary operations ζ, τ and Δ on $\mathbb{P}$. For $n > 1$ and $f \in \mathbb{P}^{(n)}$ put

$$(\zeta f)x = fx_2\ldots x_n x_1 \quad \text{for} \quad x \in D_{\zeta f} := \{(y_n,y_1,\ldots,y_{n-1}) : y \in D_f\},$$

$$(\tau f)x = fx_2x_1x_3\ldots x_n \quad \text{for} \quad x \in D_{\tau f} := \{(y_2,y_1,y_3,\ldots,y_n): y \in D_f\},$$

$$(\Delta f)x = fx_1x_1x_2\ldots x_{n-1} \quad \text{for} \quad x \in D_{\Delta f} := \{(y_1,\ldots,y_{n-1}) : (y_1,y_1,y_2,\ldots,y_{n-1}) \in D_f\}.$$

For $n \le 1$ and $f \in \mathbb{P}^{(n)}$ we set $\zeta f = \tau f = \Delta f = f$. An appropriate successive application of ζ and τ to f will get us any operation which differs from f only by the order of variables. Similarly, ζ, τ and Δ can produce any fusion (identification) of variables.

The composition $\bullet$ is defined as follows. Let $f \in \mathbb{P}^{(m)}$ and $g \in \mathbb{P}^{(n)}$. Put $r := m+n-1$, for $x \in A^r$ set $x' := (x_1,\ldots,x_m)$ and if $x' \in D_g$ put $x'' := (gx',x_{m+1},\ldots,x_r)$. Put $(f\bullet g)x := fx''$ for all $x \in D_{f\bullet g} := \{x \in A^r : x' \in D_g, x'' \in D_f\}$. Denote by e_i^n the i-th n-ary full projection (i.e. $e_i^n x = x_i$ for all $x \in A^n$) and e_1^2 the zero or nullary operation on P with value e_1^2. A subuniverse of $\langle P;\zeta,\tau,\Delta,e_1^2,\bullet\rangle$ is called a *partial clone*. It is easy to see that a partial clone contains all projections. The set of partial clones, ordered by inclusion, is clearly an algebraic lattice.

2.3. We introduce a "partial Galois theory" which is a natural member of the hierarchy of such theories. For $n \in \mathbb{N}$, $n > 0$, $f \in \mathbb{P}^{(n)}$ and $\rho \subseteq A^I$ we say that f *preserves* ρ if $fr_1\ldots r_n \in \rho$ whenever $r_1,\ldots,r_n \in \rho$ are such that $r_i := (r_1 i,\ldots,r_n i)$ belongs to D_f for all $i \in I$. A zero operation f preserves ρ if the constant map $A \to I$ with value f belongs to ρ. The closed sets in the Galois connection induced by "f preserves ρ" are

$$\mathrm{Polp}\ R := \{f \in \mathbb{P} : f \text{ preserves all } \rho \in R\},$$

$$\mathrm{Invp}_I F := \{\rho \subseteq A^I : f \text{ preserves } \rho \text{ for all } f \in F\}$$

$(R \subseteq \underset{\sim}{P}(A^I),\ F \subseteq \mathbb{P})$. Clearly, $\mathrm{Inv}\ p_I F$ is the subalgebra of the direct power $\underline{\underline{A}}^I$ of the partial algebra $\underline{\underline{A}} := \langle A;F\rangle$. Out of the several subalgebra concepts [8, p.80], we are using the following. A subset S of A is a *subalgebra* (more precisely the carrier of a subalgebra) of $\langle A;X\rangle$ if $fx \in S$ whenever $f \in X^{(n)}$ and $x \in D_f \cap S^n$. The direct power is defined in the standard way with the provision that the domain of the operation f' on A^I corresponding to $f \in X^{(n)}$ is

$$D_{f'} := \{(g_1,\ldots,g_n) \in (A^I)^n : (g_1 i,\ldots,g_n i) \in D_f \quad \forall i \in I\}.$$

2.4. It is easy to see that the sets Polp R are partial clones. If $f \in$ Polp R and g a suboperation of f then $g \in$ Pol R. Partial clones with this property will be called *strict*. (For a single relation ρ if $F \subseteq \text{Polp}\ \rho$ is directed in $(\mathbf{P},\prec)$, then Polp ρ contains the operation g with $D_g := \bigcup\{D_f : f \in F\}$, and $gx := fx$ for each $x \in D_g$ and any $f \in F$ with $x \in D_f$). The following is essentially a restatement of [4, Thm 1] and an extension of similar results for A finite or I finite [7,9,26].

2.5. PROPOSITION. *For* $R \subseteq A^I$ *the set* Pol pR *is a strict partial clone. Moreover, for* $|I| \geq |A| \geq \aleph_0$ *each strict partial clone* C *is of the form* Pol pR *for some* $R \subseteq A^I$ *of cardinality* $|R| \leq 2^{|A|}$.

Proof. For $n \in \mathbb{N}\setminus\{0\}$ and $D \subseteq A^n$ fix a surjection χ_D of A onto D and put

$$\rho_D := \{f\circ\chi_D : f \in C^{(n)} \text{ and } D_f = D\}, \quad R := \{\rho_D : n \in \mathbb{N}\setminus\{0\},\ D \subseteq A^n\}.$$

Using $|A^n| = |A|$ and $|C^{(n)}| \leq 2^{|A|}$ it is easy to see that $|R| \leq 2^{|A|}$.

We prove that $C \subseteq$ Polp R. Let $g \in C^{(m)}$ and $D \subseteq A^n$. To show that g preserves ρ_D let $r_i \in \rho_D$ $(i=1,\ldots,m)$ be such that $(r_1 a,\ldots,r_m a) \in D_g$ for all $a \in A$. By the definition of ρ_D we have $r_i = f_i\circ\chi_D$ for some $f_i \in C^{(n)}$ with $D_{f_i} = D$ $(i=1,\ldots,m)$. Define $h \in P^n$ by setting $hx = g(f_1 x)\ldots(f_m x)$ for every $x \in D_h := D$. The operation h is correctly defined because for each $x \in D$ with $x = \chi_D a$ we have

$$(f_1 x,\ldots,f_m x) = ((f_1\circ\chi_D)a,\ldots,(f_m\circ\chi_D)a) = (r_1 a,\ldots,r_m a) \in D_g \tag{1}$$

Clearly h belongs to the clone C and therefore $h\circ\chi_n \in \rho_D$. By the definition and (1) we have the required

$$g r_1\ldots r_m = g(f_1\circ\chi_D)\ldots(f_m\circ\chi_D) = h\circ\chi_D \in \rho_D.$$

It remains to show that Polp $R \subseteq C$. Let $f \in$ Pol pR be n-ary. Let $\pi_i \in \mathbf{P}^{(n)}$ satisfy $D_{\pi_i} = D := D_f$ and $\pi_i x = x_i$ for all $x \in D$ $(i=1,\ldots,n)$. The partial projections π_i belong to C, hence $\pi_i\circ\chi_D \in \rho_D$ $(i=1,\ldots,n)$ and from $f \in$ Polp ρ_D

$$f\circ\chi_D = f(\pi_1\circ\chi_D)\ldots(\pi_n\circ\chi_D) \in \rho_D$$

proving $f\circ\chi_D = g\circ\chi_D$ for some $g \in C$ with $D_g = D$. Since χ_D maps A onto D we have the required $f = g \in C$. □

2.6. REMARK. Every clone C of full operations may be easily turned into a strict partial clone C' by adding all suboperations of operations from C. The condition $|I| \geq |A|$ in Prop. 2.5 cannot be weakened because there are clones requiring it [37]. What are conditions for strict partial clones to be of the form

Polp ρ? (Cf. [31,44] for infinite clones.)

2.7. We turn to a characterization of the subsets of $\underset{\sim}{P}(A^I)$ of the form $\mathrm{Invp}_I F$. Observing that $\mathrm{Invp}_I F = \mathrm{Inv}_I F$ if F is a set of full operations, clearly $R := \mathrm{Invp}_I F$ should be an extension of subdirect closure system. It should still be a closure system and therefore we should restrict mutations. Note that $f \in \mathbb{P}^2$ preserves trivially every $\rho \subseteq A^2 \setminus D_f$ but not necessarily $D(\rho)\times A$. However, if $f \in \mathbb{P}$ preserves a binary relation ρ, then it preserves ρ^{-1}, $\rho \cap \mathrm{id}_A$ and $\rho^* := \{(x_1,x_2) \in A^2 : ((x_1,x_1) \in \rho\}$ (indeed for $x \in D_f$ with $(x_i,x_i) \in \rho$ $(i=1,\dots,n)$ we have $(fx,fx) \in \rho$ proving $(fx,fv) \in \rho^*$ for every $y \in D_f$). This leads to the following definition:

For I fixed let E denote the set of equivalences on I. For $\varepsilon \in E$ the relation $\Delta_\varepsilon := \{f \in A^I\colon \ker f \supseteq \varepsilon\}$ is said to be *diagonal*. For $\varepsilon \in E$, χ map of $K \subseteq I$ onto $L \subseteq I$ such that L meets each block of ε, and $\rho \subseteq A^I$ the relation

$$\rho \circ_\varepsilon \chi \;:=\; (\rho\cap\Delta_\varepsilon)\circ\chi \;=\; \{f \in A^I : f\restriction K = r\circ\chi \text{ for some } r \in \rho\cap\Delta_\varepsilon\}$$

is called a *surjective mutation* of ρ. An algebraic closure system Σ on A^I closed under all surjective mutations and such that each $f \in \bigcap\Sigma$ is a constant map is called a *weak subdirect closure system* (wscs).

For $F \subseteq E$ put $\Delta_F := \bigcup_{\varepsilon\in F}\Delta_\varepsilon$. If F is a subsemilattice of $\langle E;\cap\rangle$ the relation Δ_F is called *trivial*. (Note that ϕ is trivial.) It is known [32] and not difficult to prove that $\mathrm{Pol}\rho = \mathbb{O}$ if and only if ρ is trivial. First the terminology is justified by:

2.8. FACT. *Every subdirect closure system is a weak subdirect closure system. Every weak subdirect closure system contains all trivial relations.*

Proof. Let Σ be a subdirect closure system and $\varepsilon \in E$. It is known that $\Delta_\varepsilon \in \Sigma$ [32]; hence for $\rho \in \Sigma$ we have $\rho \cap \Delta_\varepsilon \in \Sigma$ and $(\rho\cap\Delta_\varepsilon)\circ\chi \in \Sigma$.

Let Σ be a weak subdirect closure system on A^I and E' a subsemilattice of $\langle E;\cap\rangle$. For $\varepsilon \in E'$ we have $\Delta_\varepsilon = (A^I\cap\Delta_\varepsilon)\circ \mathrm{id}_I \in \Sigma$ and in view of $\{\Delta_\varepsilon : \varepsilon \in E'\}$ directed finally $\Delta_{E'} := \bigcup\{\Delta_\varepsilon : \varepsilon \in E'\} \in \Sigma$. □

We need also:

2.9. FACT. *Let* χ *and* τ *be partial selfmaps of* I *and* $\rho \subseteq A^I$. *Then*

$$\rho\circ(\chi\circ\tau) = (\rho\circ\chi)\circ\tau.$$

For a fixed closure system Σ on A^I and $\rho \subseteq A^I$ put $\langle\rho\rangle := \bigcap\{\sigma \in \Sigma\colon \sigma \supseteq \rho\}$. We relate surjective mutations and $\langle\;\rangle$:

2.10. LEMMA. *Let* Σ *be a weak subdirect closure system on* A^I, χ *a map of* $K \subseteq I$ *onto* $L \subseteq I$ *and* $\rho \subseteq A^I$. *Then* $\langle\rho\rangle\circ\chi \subseteq \langle\rho\circ\chi\rangle$. *If, moreover,* L *meets each block of* $\varepsilon := \bigcup_{r\in\rho}\ker r$, *then* $\langle\rho\circ\chi\rangle = \langle\rho\rangle\circ\chi$.

Proof. Set $\zeta = \langle\rho\circ\chi\rangle$ and choose $\psi\colon L \to I$ so that $\chi\circ\psi = \mathrm{id}_L$. Since $\rho\circ\mathrm{id}_L = \{f \in A^I : f\restriction L = r\restriction L \text{ for some } r \in \rho\} \supseteq \rho$, applying Fact 2.9 we get

$$\rho\circ \mathrm{id}_L = \rho\circ(\chi\circ\psi) = (\rho\circ\chi)\circ\psi \subseteq \zeta\circ\psi. \tag{2}$$

Put $\eta = \ker\chi$. We have $\rho\circ\chi \subseteq \Delta_\eta \in \Sigma$, hence $\zeta \subseteq \Delta_\eta$ and $\zeta\circ\psi = (\zeta\cap\Delta_\eta)\circ\psi = \zeta\circ_\eta\psi \in \Sigma$ because im ψ meets each block of η. From (2) we get $<\rho> \subseteq \zeta\circ\psi$. On account of $\zeta \subseteq \Delta_\eta$ we can write $\zeta = \lambda\circ\chi$ for some $\lambda \subseteq A^I$. Using $\chi\circ\psi = \mathrm{id}_L$, the fact that $\lambda\circ\mathrm{id}_L$ agrees with λ on L, and Fact 2.9 we obtain the required

$$<\rho>\circ\chi \subseteq (\zeta\circ\psi)\circ\chi = \lambda\circ\chi\circ\psi\circ\chi = \lambda\circ\mathrm{id}_L\circ\chi = \lambda\circ\chi = \zeta.$$

Suppose that L meets each block of ε. From $\rho \subseteq \Delta_\varepsilon \in \Sigma$ again $<\rho> \subseteq \Delta_\varepsilon$ and therefore $\rho\circ\chi \subseteq <\rho>\circ\chi = <\rho>\circ_\varepsilon\chi \in \Sigma$ shows $\zeta \subseteq <\rho>\circ\chi$. □

Note that if Σ is a subdirect closure system, then $<\rho>\circ\chi = <\rho\circ\chi>$ for every mutation [37]. Borrowing the main idea from [2] (see also [37]) we prove the main result of this section.

2.11. THEOREM. *A subset Σ of $\underset{\sim}{P}(A^I)$ is the subalgebra system of the* I-*th direct power of a partial algebra on* A *if and only if Σ is a weak subdirect closure system on* A^I.

<u>Proof</u>. For $n \in \mathbb{N}\setminus\{0\}$ and $(r_1,\dots,r_n) \in (A^I)^n$ define $\hat{r}: I \to A^n$ by $\hat{r}i := (r_1 i,\dots,r_n i)$ for all $i \in I$ and denote $(r_1,\dots,r_n)$ by $\tilde{r}$.

Necessity: Let $X \subseteq P$ and $\Sigma = \mathrm{Sub}<A;X>^I$. It is well known that Σ is an algebraic closure system. Let $\sigma \in \Sigma$, $\sigma \subseteq \Delta_\varepsilon$ and χ a surjection from $K \subseteq I$ onto $L \subseteq I$ such that L meets each block of ε.

We prove that $\sigma\circ\chi \in \Sigma$. Consider first $f \in X^{(0)}$. Then the constant map $\varphi: I \to \{f\}$ belongs to $\cap\Sigma \subseteq \sigma$ and whence to $\sigma\circ\chi$. Let $n > 0$, let $r_i \in \sigma\circ\chi$ $(i=1,\dots,n)$ and $f \in X^{(n)}$ satisfy $\mathrm{Im}\,\hat{r} \subseteq D_f$. Then $r_i\restriction K = s_i\circ\chi$ for some $s_i \in \sigma$, hence $(f\circ\hat{r})\restriction K = f\circ\hat{s}\circ\chi$. Since each block of ε meets L and $\hat{r} = \hat{s}\circ\chi$, we have $\mathrm{Im}\,\hat{s} \subseteq \mathrm{Im}\,\hat{r} \subseteq D_f$ whence $f\circ\hat{s} \in \sigma$ (on account of σ subalgebra of $<A;X>^I$ and $f \in X$) and $f\circ\hat{r} \in \sigma\circ\chi$.

Sufficiency: Let Σ be a weak subdirect closure system. We construct a partial algebra $\langle A;X\rangle$ as follows. For each $g \in \cap\Sigma$ we define a nullary operation γ where γ is the value of the constant map g. Let $X^{(0)}$ be the set of all these nullary operations. Let $n \in \mathbb{N}\setminus\{0\}$ and $r_1,\dots,r_n \in A^I$. Put $\varepsilon := \ker\hat{r}$ and choose $\chi \in I^I$ so that $\ker\chi = \varepsilon$ and $(i,\chi_i) \in \varepsilon$ for all $i \in I$. Now $r_j =$ $(j=1,\dots,n)$ shows $\tilde{r} \subseteq \Delta_\varepsilon\circ\chi \in \Sigma$ proving $<\tilde{r}> \subseteq \Delta_\varepsilon\circ\chi$ and $<\tilde{r}> = \rho\circ\chi$ for $\rho \subseteq \Delta_\varepsilon$. For each $b \in <\tilde{r}>$ define a partial n-ary operation $f := f^b_{\hat{r}}$ by setting $D_f = \mathrm{Im}\,\hat{r}$ and $fx = bi$ whenever $x \in D_f$ satisfies $x = ri$ for some $i \in I$ (due to $b \in <\tilde{r}>$ and $\ker r = \varepsilon = \ker\chi \subseteq \ker b$ this definition is consistent). Let $X^{(n)}$ be the set of all such operations $f^b_{\hat{r}}$ and $X := \bigcup_{n\in\mathbb{N}} X^{(n)}$.

We prove $\Sigma \subseteq \mathrm{Sub}<A;X>^I$. By the definition each $\sigma \in \Sigma$ is closed under the nullary operations $X^{(0)}$. Let $n > 0$ and let $r_1,\dots,r_n,b,s_1,\dots,s_n \in A^I$ be such that $\mathrm{Im}\,\hat{s} \subseteq \mathrm{Im}\,\hat{r}$ and $b \in <\tilde{r}>$. Taking into account that Σ is an algebraic closure system it suffices to show that $h := f^b_{\hat{r}}\circ s \in <\tilde{s}>$. Put $J := \mathrm{Im}\,\hat{r}$ and choose $p: J \to I$ so that $\hat{r}\circ p = \mathrm{id}_J$. By its definition $h = b\circ p\circ\hat{s}$. Setting $\chi := p\circ\hat{s}$ by Lemma 2.10

we have $h \in \langle\tilde{r}\rangle\circ X \subseteq \langle\tilde{r}\circ X\rangle$. Now from $\hat{r}\circ X = \hat{r}\circ p\circ\hat{s} = id_J\circ\hat{s} = \hat{s}$ we obtain $r_j\circ X = s_j$ $(j=1,\ldots,n)$ i.e. $\tilde{r}\circ X = \tilde{s}$ and finally $h \in \langle\tilde{s}\rangle$.

It remains to prove $\mathrm{Sub}\langle A;X\rangle^I \subseteq \Sigma$. For $C \subseteq A^I$ let $C^{\#}$ stand for the subalgebra of $\langle A;X\rangle^I$ generated by C. By definition $\phi^{\#} = \bigcap\Sigma = \langle\phi\rangle$. Next let $\tilde{r} = \{r_1,\ldots,r_n\}$ be a finite subset of A^I. For each $b \in \langle\tilde{r}\rangle$ we have $b = f^b_{\hat{r}}\circ\hat{r} \in \tilde{r}^{\#}$ proving $\langle\tilde{r}\rangle \subseteq r^{\#}$.

Since both Σ and $\mathrm{Sub}\langle A;X\rangle^I$ are algebraic, it follows that $\langle C\rangle \subseteq C^{\#}$ for all $C \subseteq A^I$, in particular, $C \subseteq \langle C\rangle \subseteq C^{\#} = C$ for every $C \in \mathrm{Sub}\langle A;X\rangle^I$. □

2.12. In the next section we shall need the wscs $[S]$ on $\mathbf{A}^I$ generated by a subset S of A^I. The set $[S]$ can be constructed in three steps: (i) Let $S_{(1)}$ consist of all surjective mutations $\sigma\circ_\varepsilon X$ with $\sigma \in S$ and of diagonal relations, (ii) let $S_{(2)}$ consist of all intersections of subfamilies of $S_{(1)}$, and (iii) let $S_{(3)}$ be the set of directed unions of subsets of $S_{(2)}$. We have:

2.13. PROPOSITION. *For* $S \subseteq A^I$ *the set* $S_{(3)}$ *is the weak subdirect closure system* $[S]$ *generated by* S.

<u>Proof</u>. Clearly $S \subseteq S_{(1)} \subseteq S_{(2)} \subseteq S_{(3)} \subseteq [S]$ and therefore it suffices to show that $S_{(3)}$ is a wscs. Since $\Delta_{I^2} \in S_{(1)} \subseteq S_{(3)}$ each $f \in \bigcap S_{(3)}$ is a constant map. It is relatively simple matter to show that for any $S_{(1)}$ the set $S_{(3)}$ is a closure system. By its definition it is also algebraic and therefore it remains to show that $S_{(3)}$ is closed under surjective mutations. First we show that $S_{(1)}$ is closed under surjective mutations. Consider $(\sigma\circ_{\varepsilon_1}X_1)\circ_{\varepsilon_2}X_2$ where $X_i\colon K_i \to L_i$ $(i=1,2)$. In each block B of ε_2 intersecting K_1 select and element b. Let K be the set of $k \in K_2$ such that the block B of ε_2 containing X_2k intersects K_1. If to k we assign X_1b where b is the preselected element of B we obtain a map $X\colon K \to L_1$ such that $(\sigma\circ_{\varepsilon_1}X_1)\circ_{\varepsilon_2}X_2 = \sigma\circ_{\varepsilon_1}X$.

Now we prove that $S_{(2)}$ is closed under surjective mutations. Let X be a map from $K \subseteq I$ onto $L \subseteq I$ and ε an equivalence on I such that L meets each block of ε. Consider $\rho_i \in S_{(1)}$ $(i \in I)$ and $\rho := \bigcap_{i\in I}\rho_i$. A direct check shows that $\rho\circ X \subseteq \bigcap_{i\in I}(\rho_i\circ X)$ which together with $\rho \cap \Delta_\varepsilon = \bigcap_{i\in I}(\rho_i\cap\Delta_\varepsilon)$ gives $\rho\circ_\varepsilon X \subseteq \bigcap_{i\in I}(\rho_i\circ_\varepsilon X)$. For the converse let $f \in \bigcap_{i\in I}(\rho_i\circ_\varepsilon X)$. Then there are $r_i \in \rho_i\cap\Delta_\varepsilon$ such that $f\restriction K = r_i\circ X$ for all $i \in I$. Since L meets each block of ε, there is an r such that $r_i = r$ for all $i \in I$. Clearly $r \in \bigcap_{i\in I}(\rho_i\cap\Delta_\varepsilon) = \rho\cap\Delta_\varepsilon$ proving $f \in \rho\circ_\varepsilon X$.

Let ρ be the directed union of $\{\rho_i : i \in I\} \subseteq S_{(2)}$. It presents no difficulty to show that $\rho\circ_\varepsilon X = \bigcup_{i\in I}(\rho_i\circ_\varepsilon X)$ where $\{\rho_i\circ_\varepsilon X : i \in I\}$ is directed. Thus $\rho\circ_\varepsilon X \in S_{(3)}$ completing the proof. □

3. CONCRETE REPRESENTATION.

3.1. We apply the Galois connection to concrete representation problems for partial algebras. For simplicity we consider only unary and binary problems. (The results are therefore already a consequence of [9]). The problems considered are the following:

(i) Under what conditions is a subset G of $\underset{\sim}{P}(A)$ the subalgebra system of a partial algebra on A?

(ii) Let E be the set of equivalence relations on A. Under what conditions is a subset H of E the set of congruences of a partial algebra on A?

(iii) Let M be a set of partial selfmaps of A. Under what conditions is a subset K of M equal to $M \cap$ P-end A (defined in 1.8 and discussed in 3.5)?

For simplicity of exposition we consider the problems first separately and then together (joint representation problem). Note the following almost immediate fact. If $G = \mathrm{Sub}\langle A;F\rangle$, then $G = \mathrm{Sub}\langle A;L\rangle$ where L is the strict clone generated by F and the same holds for (ii) and (iii). Thus without loss of generality we can study concrete representation via wscs's (e.g. if [G] denotes the wscs on A generated by G, then an answer to (i) is G satisfying $G = \underset{\sim}{P}(A) \cap [G]$).

3.2. Consider the case (i). For $|I| = 1$ the mutations are trivial and $[G] = G_{(3)}$ is just the algebraic closure system on A generated by G. Thus we have the well known result ([8], §16): $G = \mathrm{Sub}\,\underline{\underline{A}}$ iff G is an algebraic closure system on A. As a curiosity note that Polp G is the strict partial clone generated by Pol G.

3.3. In (ii) and (iii) we have weak subdirect closure systems on A^2. If we consider the 8 partial selfmaps of $\underline{2}$ with nonempty domain and the two equivalences on $\underline{2}$ we obtain the following 5 surjective mutations of a binary relation on A: $\rho, \rho^{-1} := \{(x_2,x_1) : (x_1,x_2) \in \rho\}$, $\rho^* := \{(x_1,x_2) \in A^2 : (x_1,x_1) \in \rho\}$, ρ^{*-1}, $\rho_{id} := \rho \cap id_A$.

3.4. Recall that $\theta \in E$ is a *congruence* of partial algebra $\underline{\underline{A}} := \langle A;F\rangle$ if $\theta \in \mathrm{Sub}\,\underline{\underline{A}}^2$ (i.e. if for $f \in F^{(n)}$, $a,b \in D_f$ with $(a_i,b_i) \in \theta$ we have $(fa,fb) \in \theta$).

Let $H \subseteq E$. Observing that $\theta^{-1} = \theta$, $\theta_{id} = id_A$ and $\theta^* = A^2$ for every $\theta \in E$, we have $H_{(1)} = H \cup \{id_A, A^2\}$ and $[H] = H_{(3)}$ is the algebraic closure system in $(E,\subseteq)$ generated by $H_{(1)}$. Thus we have the result from [9] Thm.5: $H = \mathrm{Con}\,\underline{\underline{A}}$ for a partial algebra on A iff H is an algebraic closure system on A^2 and $id_A \in H$. Note that in this case not only $H = E \cap [H]$ but even $H = [H]$. Also Polp H is an analogue of finite hemi-primal algebras. Observe also that the result was obtained without exhibiting a single partial operation, e.g. we have no knowledge about their domains (if H is not the congruence lattice of a full algebra Polp H must contain partial operations that are not full). For full algebras the situation is far more complex [45].

3.5. For the ease of expression we consider partial selfmaps of A also as binary relations on A. This is used mainly in the construction while we use the standard notation when dealing with morphisms.

Let Q denote the set of partial selfmaps of A. If we wish to apply the wscs's we must define a morphism as $\varphi \in Q \cap \mathrm{Sub}\,\underline{\underline{A}}^2$. This leads to the following definition [43]: For $\varphi \in Q$ and $a = (a_1,\ldots,a_n)$ with $a_1,\ldots,a_n \in D := \mathrm{Dom}\,\varphi$ put $\varphi a := (\varphi a_1,\ldots,\varphi a_n)$. We say that φ is a *partial endomorphism* of $\langle A;F\rangle$ if for each $f \in F^{(n)}$ we have $fa \in D$ and $\varphi fa = f\varphi a$ whenever $a \in D_f \cap D^n$ and $\varphi a \in D_f$. The set of partial endomorphisms of A is denoted P-endA. A partial endomorphism is more general than the more usual *quomorphism* (cf. [47] for various other names) in which $a \in D_f \cap D^n$ implies $\varphi a \in D_f$, $fa \in D$ and $\varphi fa = f\varphi a$ (i.e. φ maps each D_f into itself).

In general we have no *a priori* knowledge of the domains of $f \in \mathrm{Polp}\,R$ (cf. 3.4) and so are unable to treat quomorphisms in this way.

For $K \subseteq Q$ denote the common fixed points of K by $\mathrm{Fix}\,K := \{x \in A : (x,x) \in k$ for all $k \in K\}$. Further let $K°$ denote the set of all

$$(\mathrm{Fix}\,K_1 \times \mathrm{Fix}\,K_2) \cap \cap K_3 \cap \cap K_4^{-1} \tag{3}$$

where $K_1,\ldots,K_4 \subseteq K$ satisfy

$$K_1 \neq \phi = K_3 = K_4 \Rightarrow |\mathrm{Fix}\,K_2| = 1. \tag{4}$$

The following characterization of partial endomorphism sets of partial algebras may seem surprising because it involves no composition of endomorphisms.

3.6. PROPOSITION. *Let* $\mathrm{id}_A \in M \subseteq Q$. *If* $K \subseteq M$, *then* $K = M \cap \mathrm{P\text{-}end}\underline{\underline{A}}$ *for a partial algebra* $\underline{\underline{A}}$ *on* A *if and only if* $\mathrm{id}_A \in K$ *and* K *contains every* $\mu \in M$ *that is the directed union of a subfamily of* $K°$.

<u>Proof</u>. We have

$$K_{(1)} = \{\mathrm{id}_A, A^2\} \cup K \cup K^{-1} \cup \{\mathrm{id}_{\mathrm{Fix}\,\varkappa} : \varkappa \in K\} \cup \{\mathrm{Fix}\,\varkappa \times A : \varkappa \in K\} \cup \{A \times \mathrm{Fix}\,\varkappa : \varkappa \in K\}. \tag{5}$$

It is not hard to see that $Q \cap K_{(2)} = K°$. Indeed note that

$$\mathrm{Fix}\,K_1 \times \mathrm{Fix}\,K_2 = \cap_{\varkappa \in K_1}(\mathrm{Fix}\,\varkappa \times A) \cap \cap_{\varkappa \in K_2}(A \times \mathrm{Fix}\,\varkappa).$$

Choosing K_1 or K_2 equal to $\{\mathrm{id}_A\}$ we can obtain $A \times \mathrm{Fix}\,K_1$ or $\mathrm{Fix}\,K_2 \times A$. The maps $\mathrm{id}_{\mathrm{Fix}\,K_3}$ are obtained by setting $K_1 = K_2 = K_3 = \{\mathrm{id}_A\}$, $K_4 = \phi$. The restriction (4) guarantees that (3) always belongs to Q. Finally $Q \cap K_{(3)}$ contains every $\rho \in Q$ which is the directed union of a subfamily of $Q \cap K_{(2)}$. □

3.7. REMARK. Let I be the set of partial injective selfmaps of A. For $M \subseteq I$ the condition (4) simplifies to

$$K_3 = K_4 = \phi \Rightarrow |\mathrm{Fix}\,K_1| = |\mathrm{Fix}\,K_2| = 1. \tag{4'}$$

3.8. Among the various choices for M in P.3.6 we look at A^A and S_A. For simplicity call a partial endomorphism $f \in A^A$ ($f \in S_A$) of A a *weak endomorphism (automorphism)* of A (it is called full-homomorphism in [43] but this term is usually reserved for a special type of quomorphisms and denote the respective sets by W-endA (w-autA). From P.3.6 we obtain:

3.9. COROLLARY. *A subset* K *of* A^A (S_A) *is the set of weak endomorphisms (automorphisms) of a partial algebra on* A *if and only if* $id_A \in K$ *and* K *contains every* $\mu \in A^A$ $(\mu \in S_A)$ *that is the directed union of a subfamily of* $K°$.

For A finite the directed unions are trivial:

3.10. COROLLARY. *For* A *finite a subset* K *of* A^A (S_A) *is the set of weak endomorphisms (automorphisms) of a partial algebra on* A *if and only if* $id_A \in K$.

Now we can formulate a joint concrete representation result. For $G \subseteq \underset{\sim}{P}(A)$, $H \subseteq E$ and $K \subseteq Q$ put

$$\Lambda_{GHK} := \{id_\gamma : \gamma \in G\} \cup \{\theta \cap \kappa : \theta \in H,\ \kappa \in K\}. \tag{6}$$

3.11. THEOREM. *Let* G *be a family of subsets of* A, H *a set of equivalence relations on* A *and* K *a set of partial selfmaps of* A. *Then*

$$G = \mathrm{Sub}\underline{\underline{A}},\quad H = \mathrm{Con}\underline{\underline{A}},\quad K = \text{P-end}\underline{\underline{A}}$$

for a partial algebra $\underline{\underline{A}}$ *on* A *if and only if*

(i) G *is an algebraic closure system on* A *containing all sets* Fix κ $(\kappa \in K)$,

(ii) H *is an algebraic closure system on* A^2 *containing* id_A, A^2 *and every equivalence on* A *that is the directed union of a family* $\{\gamma_i^2 \cap \zeta_i : i \in I\}$ *with* $\gamma_i \in G$ *and* $\zeta_i \in H$ *for all* $i \in I$, *and*

(iii) $id_A \in K$ *and* K *contains each partial selfmap of* A *that is the directed union of a subfamily of* Λ°_{GHK}.

The statement remains true if partial selfmaps are replaced by selfmaps (permutations) and P-endA *by* W-endA *or* (W-autA).

<u>Proof</u>. The proof will be simpler if we replace G by $G' := \{id_\gamma : \gamma \in G\}$. This is quite legitimate and allows us to work entirely within A^2. Thus we assume that we have $H \subseteq E$ and $K' := K \cup G'$. The closure of $L := H \cup K'$ under the surjective mutations is

$$L_{(1)} = \{id_A, K^2\} \cup H \cup K' \cup K'^{-1} \cup \{id_{\mathrm{Fix}\kappa} : \kappa \in K'\} \cup \{\mathrm{Fix}\kappa \times A : \kappa \in K'\} \cup \{A \times \mathrm{Fix}\kappa : \kappa \in K'\}. \tag{7}$$

Consider the set $Q \cap L_{(2)}$ (of intersections of subfamilies of $L_{(1)}$ which are partial self-maps of A). Comparison of (7) and the definition of Λ_{GHK} shows

$$Q \cap L_{(2)} = \Lambda^\circ_{GHK}. \tag{8}$$

It is not difficult to prove from (7) and (3) that for $B \subseteq A$

$$id_B \in L_{(2)} \Rightarrow B = \mathrm{Fix}\, K_1 \tag{9}$$

for some $K_1 \subseteq K'$.

Necessity: From 3.5 we know that H is an algebraic closure system on A^2 containing id_A. We have $\gamma^2 \cap \zeta \in L_{(2)}$ for $\gamma \in G$ and $\zeta \in H$ (in (3) choose $K_1 = K_2 = \{id_\gamma\}$ and $K_3 = K_4 = \phi$) and therefore (ii) holds. Next (iii) follows directly from (8). For (i) use (9) and observe that $P := \{C : id_C \in L_{(3)}\}$ forms a algebraic closure system on A

Sufficiency: From (8) we have $Q \cap L_{(3)} = K$. For the proof of $E \cap L_{(3)} = H$ let

θ be the directed union of $T \subseteq L_{(2)}$. First we show that θ is the directed union of some $T' \subseteq T \setminus Q$. Let $(a_1,a_2) \in \theta \setminus id_A$. Then $(a_1,a_2) \in \tau_1$ and $(a_2,a_1) \in \tau_2$ for some $\tau_1,\tau_2 \in T$. Let $\tau_{a_1a_2}$ be an element of T containing $\tau_1 \cup \tau_2$. It is easy to see that $T' := \{\tau_{a_1a_2} : (a_1,a_2) \in \theta \setminus id_A\}$ is the required set. Now it suffices to observe that each $\tau \in L_{(2)} \setminus Q$ is of the form $\tau = (\mathrm{Fix}\ K_1 \times \mathrm{Fix}\ K_2) \cap \zeta$ with $K_1,K_2 \subseteq K'$ and $\zeta \in H$ (use (3) where $K_3 = K_4 = \phi$). From (ii) it follows that $\theta \in H$. □

For finite algebras we obtain:

3.12. COROLLARY. *Let* A *be finite,* G *a family of subsets of* A, H *is a set of equivalences on* A *and* K *a set of selfmaps on* A. *Then*

$$G = \mathrm{Sub}\underline{\underline{A}},\quad H = \mathrm{Con}\underline{\underline{A}},\quad K = W\text{-}\mathrm{end}\underline{\underline{A}}$$

for a partial algebra $\underline{\underline{A}}$ *on* A *if and only if*

(i) G *is closed under intersections and contains all* Fix $\varkappa$ $(\varkappa \in K)$,

(ii) H *is closed under intersections and* id_A, $A^2 \in H$,

(iii) K *contains* id_A *and each constant map with value* a *where* $\{a\} = \mathrm{Fix}\ L$ *for some* $L \subseteq K$.

A similar statement holds for $K \subseteq S_A$ *with* W-autA *instead of* W-endA *and (iii')* $id_A \in K$ *instead of (iii).*

REFERENCES.

1. Andréka,H.; Burmeister,P.; Németi,I., Quasivarieties of partial algebras - A unified approach towards a two-valued model theory for partial algebras. Preprint No.557, Techn.Hochschule Darmstadt, July 1980.
2. Birkhoff,G., Frink,O., Representation of lattices by sets. Trans.Am.Math. Soc. 64 (1948), 299-316. MR10 #279.
3. Bodnarčuk,V.G.; Kalužnin,L.A.; Kotov,V.N.; Romov,B.A., Galois theory for Post algebras.(Russian) Kibernetika (Kiev) Part I: 3 (1969) 1-10; Part II: 5 (1969) 1-9. English translation Cybernetics 5 (1969) 243-252, 531-539, MR46 #55.
4. Fleischer,I.; Rosenberg,I.G., The Galois connection between partial functions and relations. Pacific J.Math. 79 No.1 (1978) 93-98.
5. Freĭvald,R.V., Completeness criteria for partial functions of the algebra of logic and many-valued logics.(Russian) Dokl.Akad.Nauk SSSR 167 No.6 (1966) 1249-1250.
6. Freĭvald,R.V., Functional completeness for not everywhere defined functions of the algebra of logic.(Russian) Diskret.Analiz, Novosibirsk, No.8 (1966) 55-68.
7. Geiger,D. Closed systems of functions and predicates. Pacific J.Math. 27 No.1 (1968) 95-100. MR38 #3207.
8. Grätzer,G., Universal algebra. D. Van Nostrand 1968; 2nd ed., Springer-Verlag, New York 1979.
9. Iskander,A.A., Subalgebra systems of powers of partial universal algebras. Pacific J.Math. 38 (1971) 457-463. MR46 #5212.
10. Janov,Ju.I.; Mučnik,A.A., Existence of k-valued closed classes without a finite basis . (Russian) Dokl.Akad.Nauk SSSR 127 (1959) 44-46. MR21 #7174.
11. Kalužnin,L.A., Klin,M.H., Certain subgroups of symmetric and alternating groups.(Russian) Math.USSR-Sb 16 (1972) 95-124, MR45 #6906.
12. Krasner,M., Remarque au sujet de "Une generalisation de la notion de corps", Journ.de Math. (1938) 367-385. J.Math.Pures Appl. 18 (1939) 417-418, MR1 p.198

13. Krasner,M., Generalisation abstraite de la theorie de Galois. Colloques internationaux du Centre National R.S. XXIV 1949, Paris. Algèbre et théorie des nombres, 163-165, Paris, CNRS, 1950, MR12 p.796.
14. Krasner,M., Generalisation abstraite de la théorie de Galois. Proceedings of the International Congress of Mathematics 1950, Cambridge Vol.1, pp.331-332, Providence AMS 1952.
15. Krasner,M., Endotheorie de Galois abstraite. Congres international des mathématiciens, Moscou, 1966, Résumés 2, Algèbre p.61, Moscou ICM 1966.
16. Krasner,M., Endotheorie de Galois abstraite. Seminaire P.Dubreil, M.L.Dubreil, L.Lesieur et C.Pisot (Algèbre et théorie des nombres) 22ieme annee, Fasc.1, 1968/69, no.6 (19 pages) MR44 #45.
17. Krasner,M., Endotheorie de Galois abstraite et son théorème d'homomorphie. C.R.Acad.Sci.Paris 282 (1976) 683-686.
18. Krasner,M., Abstract Galois theory and endotheory. Manuscript Paris 1980.
19. Kuznecov,A.V. Fortv years of Soviet Mathematics (Russian) T.1, p.102-115, Moscou 1957.
20. Mal'cev,A.I. Iterative algebras and Post's varieties (Russian). Algebra i Logika 5 (1966) 5-24. English translation: Mal'cev, The metamathematics of algebraic systems, pp.396-415, North-Holland 1971.
21. Murskiǐ,V.L., The existence in the three-valued logic of a class with a finite basis having no finite basis of identities (Russian). Doklady Akad. Nauk.SSSR 163 (1965) 815-818. MR 32 #3998.
22. Pöschel,R., Postsche Algebren von Funktionen uber einer Famille endlicher Mengen. Z.Math.Logik Grundlagen Math. 19 (1973) 37-74.
23. Pöschel,R.; Kalužnin,L.A., Funktionen und Relationenalgebren. Math.Monographien 15 VEB Deutscher Verlag d. Wissenschaften Berlin 1979 and Math.Reihe B.67. Birkhäuser Verlag Basel,Stuttgart 1979.
24. Romov,B.A., Local characteristics of Post algebras.(Russian) Part I: Kibernetika (Kiev) No.5 (1976) 38-45. Part II: ibid No.1 (1977) 12-20. English translation: Cybernetics (1977).
25. Romov,B.A., The Galois correspondence between Post's iterative algebras and relations on an infinite set . (Russian) ibid No.3 (1977) 62-64. English translation: Cybernetics (1977).
26. Romov,B.A., The algebra of partial functions and their invariants.(Russian) ibid no.2 March-April 1981, 1-11. English translation: Cybernetics (1981) 157-167.
27. Post,E., The two valued iterative systems of mathematical logic. Annals of Math.Studies 5, Princeton 1951.
28. Rosenberg,I.G., La structure des fonctions de plusieurs variables sur un ensemble fini. C.R.Acad.Sci.Paris. Ser.A-B 260 (1965) 3817-3819. MR31 #1185.
29. Rosenberg,I.G., Über die funktionale Vollständigkeit in der mehrwertigen Logiken. Rozpravy Československé Akad.Věd., Řada Mat.Přír.Věd. 80, 4 (1970) 1-93. MR45 #1732.
30. Rosenberg,I.G., Algebren und Relationen. Elektron.Informationsverarbeitung Kybernetik 6 (1970) 115-124, MR42 #48.
31. Rosenberg,I.G., A classification of universal algebras by infinitary relations, Algebra Universalis 1 (1972) 350-354. MR45 #6732.
32. Rosenberg,I.G., Universal algebras with all operations of bounded range. Colloq.Math. 30, Fasc.2 (1974) 177-185.
33. Rosenberg,I.G., Special types of universal algebras preserving a relation. Portugaliae Math.Vol. 34 Fasc.3 (1975) 174-188.
34. Rosenberg,I.G., Functional completeness in heterogeneous multiple-valued logics Proc.1975 Int.Symp.on Multiple-Valued Logics, 36-44. Bloomington,Ind. 1975.
35. Rosenberg,I.G., The set of maximal closed classes of operations on an infinite set A has card $2^{2^{A}}$. Archiv.d.Math. 27 (1976) 561-568.
36. Rosenberg,I.G., Completeness properties of multiple-valued logic algebras. In Computer Science and Multiple-Valued Logic, Theory and Applications (D.C.Rine, ed.) North-Holland, Amsterdam-New York-Oxford 1977, 144-186.
37. Rosenberg,I.G., Subalgebra systems of direct powers. Algebra Universalis 8/2 (1978) 221-227.
38. Rosenberg,I.G., On a Galois connection between algebras and relations and its

applications. Contrihutions to general algehra (Proc.of the Klagenfurt conference 1978; H.Kautschitsch,W.B., Müller,W., Nöbauer,eds.) Verlag J.Heyn Klagenfurt 1979, 273-289.
39. Rosenberg,I.G., Clones containing the direct square of a primal algebra. Proc. 12th Intern.Symposium Multiple-valued Logic. CNAM Paris (1982) 30-34.
40. Rosenberg,I.G., Szendrei,Á., Submaximal clones with a prime order automorphism, CRMA-732, Montreal 1981 (20p.) submitted.
41. Sauer,N., Stone,M.G., The algebraic closure of a semigroup of functions. Algebra Universalis 7 (1977) 219-233.
42. Sauer,N., Stone,M.G., A Galois correspondence between algebras and endomorphisms, Colloq.Math.Soc.J. Bolyai 29 (1977) 691-695.
43. Słominski,J., On mappings between quasi-algebras. Coll.Math. 21 (1970), 5-21.
44. Szabó,L., Concrete representation of related structures of universal algebras. Acta Sci.Math. (Szeged) 40 (1978) 175-184.
45. Werner,H., Which partition lattices are congruence lattices, Colloq.Math.Soc. J. Bolyai 14 (1974), 433-453.
46. Wojdyło,B., Remarks on lattices of congruences relations of quasialgebras. Coll.Math. 27 (1973) 187-191.
47. Burmeister,P., Wojdyło,B., Properties of homomorphisms and quomorphisms. Preprint No. 657, Technische Hochschule Darmstadt 1982 (26 p.)

Centre de recherche de mathématiques appliquées
Université de Montréal
Montréal, Québec, Canada H3C 3J7

EVERY FINITE ALGEBRA WITH CONGRUENCE LATTICE M_7 HAS PRINCIPAL CONGRUENCES

N. Sauer, M.G. Stone and R.H. Weedmark

1. INTRODUCTION. Each finite lattice is known to be isomorphic to the congruence lattice of some algebra; it is not known however if this algebra itself can be chosen to be finite. The recent solution to Whitman's problem by Pudlák and Tuma ([6]) shows that each finite lattice can be represented as a 0,1-sublattice of the lattice of equivalence relations of a finite set. For many lattices at least some of those representations fail to be the congruence lattice of any algebra ([12]). The only finite lattices for which every such representation is the congruence lattice of an algebra are the finite distributive lattices (cf.[5], [7]).

If L is a finite lattice and A is a finite set then $L_A = \langle A, L\rangle$ is a *finite representation* (FR) of L on A iff L is a 0,1-sublattice of $E(A)$, the lattice of all equivalence relations on A, and L is isomorphic to L. If L_A is a FR of L on A and L is also the congruence lattice of some algebra with base set A, we say L_A is a finite algebraic representation (FAR). Thus every finite lattice has a FR, and it is unknown whether every finite lattice has a FAR. Among those finite lattices *not* known to have FAR's perhaps the M_n's (modular lattices of length two with n atoms) provide the most natural class of examples. Some M_n's (viz. M_{p^k+1} with p prime) are known to have FAR's. The lattice M_7 is the smallest M_n not of that type, and the existence problem (cf. [3]) remains* unsettled for M_7. An earlier paper [9] explores the general structure of FAR's of M_n's; here we investigate M_7 and prove the title result (Theorem 6.0). Theorems 3.2, 4.0 and 5.0 were presented at the IVth U.A. and L.T. Congress (Puebla, 1982) in a talk "On representing M_n's by congruence lattices of finite algebras".

2. BACKGROUND. Before proceeding to the proof of our result, we recall enough of the definitions and facts from [9] to be able to place the theorem in a meaningful context. We view each relational structure $L_A = \langle A, L\rangle$ which is a FR of an M_n as a colored graph; that is each of the equivalence relations which represent an atom of M_n is interpreted as a partial edge coloring of a graph whose

vertices are A, (cf. fig. (i)) and whose edges are the pairs in that equivalence relation. Thus *homomorphisms* of similar FR's are edge (color) preserving maps. A non-trivial homomorphic image is an image which does not consist of a single point. The set of all homomorphisms from L_A into L_A is denoted by Hom L_A. We denote the least and greatest elements of a FR L_A by 0_A and 1_A (the diagonal and universal relations on A) respectively. If $B \subseteq A$ then L_B denotes the *subgraph of* L_A *generated by* B, that is $L_B = \langle B, \{\theta_B | \theta \in L,\ \theta_B = \theta \cap B^2\}\rangle$.

A *characteristic subgraph* of a finite representation of M_n is a subgraph of L_A obtained in the following way: among all non-trivial homomorphic images of L_A in L_A, $\{\alpha A | \alpha \in \text{Hom } L_A\}$ choose those of minimal (vertex) cardinality; from these αA with $|\alpha A|$ minimal select a subgraph $L_{\alpha A}$ generated by αA which contains a largest (maximal) number of "colored edges" (edges which belong to relations used to represent atoms). Clearly such a subgraph contains no non-trivial proper homomorphic images of itself, and we say it is *irreducible*. It is less obvious that this characteristic subgraph of L_A is also a FR of M_n, that it is uniquely determined up to isomorphism, and that the characteristic subgraph of a FAR of M_n is also a FAR of M_n. These facts are established in [9]. In particular we will make use of (Proposition 3 of [9]):

THEOREM 2.0 *If* L_A *is a FAR of* M_n $(n \geq 3)$ *then the characteristic subgraph of* L_A *is an irreducible FAR of* M_n.

Each irreducible FAR of M_n will be called an IFAR. The IFAR's provide a means of classification for FAR's of M_n: two FAR's of M_n are equivalent if they have isomorphic characteristic subgraphs. The known FAR's of M_n's for $n \geq 4$ are easy to describe in this way, since their characteristic subgraphs are of one of only two types:

(i) *For* M_{p^k+1} *(prime) let* L *be the congruence lattice of the two dimensional vector space over* $GF(p^k)$; $L_A = \langle A, L\rangle$ *is an IFAR of* M_{p^k+1} *on* $A = GF(p^k) \times GF(p^k)$.

(ii) *For* M_{p+1} *(p prime) let* $A = \{a_1,\dots,a_p,b_1,\dots b_p\}$ $|A| = 2p$, *and let* $L = \{\theta_1,\dots,\theta_{p+1},0_A,1_A\}$ *where* θ_{p+1} *has exactly two equivalence classes* $\{a_1,\dots,a_p\}$, $\{b_1,\dots,b_p\}$ *and* θ_k *has two-element classes* $(k \neq p+1)$, $\{a_i,b_j\}$, *with* $j-1 \equiv k$ *mod* p. $L_A = \langle A, L\rangle$ *is an IFAR of* M_{p+1}. *Observe for* p *fixed and* $k = 1$ *that (i) and (ii) are non-equivalent FAR's of* M_{p+1}. *Further in this same direction we will need to make use of the following (Proposition 7 of* [9]).

THEOREM 2.1 *If* L_A *is an IFAR (irreducible finite algebraic representation) of* M_n *and some two atoms are represented by partitions with two-element equivalence classes, then* $n = p+1$ *for some prime* p *and* L_A *is of type (ii) above.*

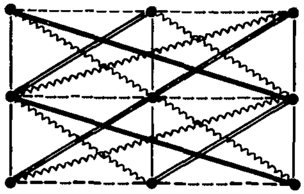


figure (i)

Type (i) IFAR of M_4 on $|A| = 3\times 3$

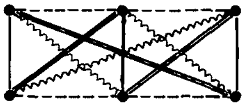


figure (ii)

Type (ii) IFAR of M_4 on $A = 2\cdot 3$

Each of the IFAR's known to the authors for M_n *has the property that every edge is colored by some atom. We say a FR of* M_n *on* A *is complete provided every edge* $(x,y) \in A^2$ *belongs to one of the relations used to represent some atom. Thus the known IFAR's of* M_n *are complete. It is possible that every IFAR of an* M_n *is complete, but that appears far from being settled.*

PROBLEM 1. Does there exists an IFAR for some M_n ($n \geq 4$) which is not complete? Our result shows that if M_7 has a finite algebraic representation, then there must be at least one (and it follows a great many!) edges in A^2 which are not used in the representation of atoms. If it can be shown that every IFAR of M_7 is complete, then of course our result would show that no finite algebraic representation is possible for M_7. The result in the title states that M_7 has no complete FAR.

The proof that M_7 has no complete FAR is essentially combinatorial. We will make heavy use of the high degree of regularity established for IFAR's of M_n in Proposition 4 of [9] (See also [2]):

THEOREM 2.2. *If* L_A *is an IFAR of* M_n $(n \geq 4)$ *then* L_A *satisfies*

(i) *(vertex transitivity) For each* $a, b \in A$ *there is an automorphism* $\alpha \in Hom\ L_A$ *with* $\alpha(a) = b$.

(ii) *(uniformity) For each* $\theta \in L$ *there is a number* k_θ *so that every* θ*-class has exactly* k_θ *elements.*

3. COMPLETE FAR's OF M_n's. Our first step toward showing there are no complete FAR's of M_7 depends essentially on the following combinatorial fact:

THEOREM 3.1. *(cf.* [1]*) There are no two orthogonal Latin squares of order six.*

The goal of this section is to prove:

THEOREM 3.2. *If* $L_A = \langle A, L\rangle$ *is a complete FAR of* M_7 *then either:*

(i) *The seven non-trivial partitions of L all have five blocks of three elements; or*

(ii) *six of the non-trivial partitions of L have five blocks of four elements and one has ten blocks of two elements.*

We break the proof of Theorem 3.2 into a series of Lemmas which appeared originally in [11], with some minor modifications.

LEMMA 3.3 For $n \geq 3$, each complete FAR of M_n is an IFAR of M_n.

Proof. Consider $L_{\alpha A}$ a characteristic subgraph of L_A, where L_A is any complete FAR of M_n ($n \geq 3$). Since $L_{\alpha A}$ is an IFAR of M_n, it suffices to see $\alpha A = A$. Suppose $|\alpha A| < |A|$, thus for some $x,y \in A$ with $x \neq y$ we have $\alpha x = \alpha y = a$. Since L_A is complete, there is some atom θ with $(x,y) \in \theta$. Next fix $Z \in A$ with $(Z,x) \notin \theta$. Again using the completeness of L_A select atoms π and γ with $(Z,x) \in \pi$ and $(Z,y) \in \gamma$. Thus $(\alpha Z,\alpha x) = (\alpha Z,a) \in \pi$ and $(\alpha Z,\alpha y) = (\alpha Z,a) \in \gamma$. From $(\alpha Z,a) \in \pi \cap \gamma$ we conclude either $\alpha Z = a$ or $\pi = \gamma$. But $\pi = \gamma$ yields $(x,y) \in \pi$ and $(x,y) \in \theta$, thus $\pi = \theta$ and $(Z,x) \in \theta$ contrary to the choice of Z. Hence $\alpha Z = a$. It follows that all of αA is contained in the θ-class of a. But $L_{\alpha A}$ is (by Theorem 2.0) in IFAR of M_n, so $\pi \cap (\alpha A)^2$ is not the diagonal relation, and this contradicts $\pi \cap (\alpha A)^2 \subseteq \theta$. Thus $|\alpha A| = |A|$, $\alpha A = A$ and L_A is itself an IFAR of M_n. □

Now we may assume in Theorem 3.2 that L_A is an IFAR of M_7, and hence (by Theorem 2.2) that L_A is vertex transitive, and for each $\theta \in L$ that there is a uniform blocksize for the θ-classes.

LEMMA 3.4. Let $L_A = \langle A,L\rangle$ be a complete IFAR of M_n ($n \geq 3$). Suppose $\theta \in L$ has the maximum block size of all the non-trivial $\theta_j \in L$. Then $|A| \leq (n-i) + (n-1)(n-i-1)-r$ where $(n-i)$, $1 \leq i \leq n-2$, is the block size of θ and $r < (n-i)$ satisfies $r \equiv (n-1)(n-i-1) \pmod{n-i}$.

Proof. This holds for $L = E(\{1,2,3\})$. So assume $L \neq E(\{1,2,3\})$. Suppose θ has k blocks of $(n-i)$ elements. Then for any $a \in A$, there are $(k-1)(n-i)$ elements of A not related to a by θ. a must get related to each of these elements, individually in each of the remaining $(n-1)$ non-trivial partitions of L (otherwise the join of these non-trivial partitions would be something less than A^2). Therefore $(k-1)\ (n-i) \leq (n-i-1)\ (n-1)$. Hence $(k-1)(n-i) + (n-i) \leq (n-i-1)(n-1) + (n-i)$. Therefore $|A| = k(n-i) \leq (n-i) + (n-1)\ (n-i-1)$. Hence, as it must be the case that $(n-i)$ devides $|A|$, $|A| \leq (n-i) + (n-1)(n-i-1)-r$ where $r \equiv (n-1)(n-i-1) \pmod{n-i}$ and $r < (n-i)$. □

Let $\theta \in L$ be an atom whose block size is maximal for all the block sizes of atoms in L. Observe that this block size can be at most six, otherwise an element of one θ-block must be related to some two elements in another θ-block by one of the other six colors (recall that every edge belongs to one of the seven atoms), and by transitivity it would follow that some edge belongs to two atoms. We next distinguish five cases according to whether the maximal block size for θ above is 6, 5, 4, 3, or 2, and we derive Theorem 3.2 by eliminating all of the other possibilities below.

LEMMA 3.5. The block size of θ is not 6.

Proof. If the block size of θ is six then $|A| \leq 6 + (6\times 5) = 36$ (by Lemma 3.4). Hence one has the following possibilities:

a) $|A| = 36$.

Then $\theta = (a_1,\ldots,a_6)(b_1,\ldots,b_6)(c_1,\ldots,c_6)(d_1,\ldots,d_6)(e_1,\ldots,e_6)(f_1,\ldots,f_6)$. Let the remaining non-trivial partitions of L be denoted by $\alpha_1,\ldots,\alpha_6$. Consider a_1. As L is complete, a_1 must be "paired" with 30 other elements in $\alpha_1,\ldots,\alpha_6$. The maximum number of new elements a_1 can be paired with in each α_i is 5. Therefore each α_i must pair a_1 with exactly 5 elements, and each α_i must have 6 blocks of 6 elements.

Label the blocks of α_i $B_{i1}, B_{i2},\ldots,B_{i6}$ in such a way that $a_k \in B_{ik}$ for $k = 1,\ldots 6$ for each $i = 1,\ldots 6$. Form the 6×6 array of blocks whose ij entry is the block B_{ij}. Observe that the derived 6×6 array composed of elements $b_1,\ldots,b_6$ whose ij entry is the unique b_k with $b_k \in B_{ij}$ is in fact a Latin square. Moreover the 6×6 array composed of elements $\{c_1,\ldots,c_6\}$ whose ij entry is the unique c_k with $c_k \in B_{ij}$ is likewise a Latin square. Now since $b_i = b_j$ iff $i = j$ and $c_i = c_j$ iff $i = j$, we can produce two Latin squares on the set $\{1,2,\ldots,6\}$ simply by suppressing the letters b and c in each of the Latin squares above, retaining only the "subscript" as entries. It is moreover easy to see that the two 6×6 Latin squares obtained in this way are distinct and orthogonal. Given any pair (x,y) with $\{x,y\} \in \{1,2,\ldots 6\}$ and $x \neq y$ we have $(b_x,c_y) \notin \theta$; since the IFAR is complete we have (b_x,c_y) in exactly one block B_{ij} of some partition α_i, and it follows that x is the ij entry and y is the ij entry for the two Latin squares for precisely one row i and one column j. The resulting orthogonal Latin squares contradict Theorem 3.1, and hence we cannot have $|A| = 36$.

b) $|A| = 30$.

Then $\theta = (a_1,\ldots,a_6)(b_1,\ldots,b_6)(c_1,\ldots,c_6)(d_1,\ldots,d_6)(e_1,\ldots,e_6)$. a_1 must be paired with 24 other elements, at most 4 at a time (no α_i can have a 6 element block). Therefore each of the remaining atoms $\alpha_1,\ldots,\alpha_6$ must have

6 blocks of 5 elements.

The construction in a) above again produces a pair of 6x6 orthogonal Latin squares and shows we cannot have $|A| = 30$.

c) $|A| = 24$.

Then $\theta = (a_1,\ldots,a_6)(b_1,\ldots,b_6)(c_1,\ldots,c_6)(d_1,\ldots,d_6)$. a_1 must be paired with 18 other elements at most 3 at a time. Therefore for the remaining atoms each $\alpha_1,\ldots,\alpha_6$ must have 6 blocks of 4 elements.
The construction in a) above again suffices.

d) $|A| = 18$.

Then $\theta = (a_1,\ldots,a_6)(b_1,\ldots,b_6)(b_1,\ldots,b_6)$. a_1 must be paired with 12 other elements at most 2 at a time. Therefore it is paired with exactly two at a time and each $\alpha_1,\ldots,\alpha_6$ must have 6 blocks of 3 elements.
The construction in a) above again suffices.

e) $|A| = 12$.

Then $\theta = (a_1,\ldots,a_6)(b_1,\ldots,b_6)$. Hence each $\alpha_1,\ldots,\alpha_6$ has 6 blocks of 2 elements. Therefore by Theorem 2.1, L must be a FAR of some M_{p+1} where p is a prime. But $7 \neq p + 1$. This is a contradiction, hence it is not the case that $|A| = 12$.

Therefore a, b, c, d, e combine to show that the block size of θ could not be 6. □

LEMMA 3.6 The block size of θ is not 5.

Proof. If the block size of θ is five then $|A| \leq 5+ (6\times 4) - 4 = 25$ (by Lemma 3.4). Hence one has the following possibilities:

a) $|A| = 25$.

Then $\theta = (a_1,\ldots,a_5)(b_1,\ldots,b_5)(c_1,\ldots,c_5)(d_1,\ldots,d_5)(e_1,\ldots,e_6)$. Each $\alpha_1,\ldots,\alpha_6$ must have 5 blocks of 5 elements. Therefore a_1 gets paired with 24 other elements. Hence a_1 must get paired with some element twice by $\alpha_1,\ldots,\alpha_6$. This is a contradiction. Therefore it is not the case that $|A| = 25$.

b) $|A| = 20$.

Then $\theta = (a_1,\ldots,a_6)(b_1,\ldots,b_6)(c_1,\ldots,c_6)(d_1,\ldots,d_6)$. Each $\alpha_1,\ldots,\alpha_6$ has at most 4 element blocks (but not 3 as 3×20). Therefore each α_i has either 2 or 4 element blocks. Let X = number of α_i's with 4 element blocks and Y = number of α_i's with 2 element blocks. As a_1 must be paired with exactly 15 elements by $\alpha_1,\ldots,\alpha_6$, the following equations must be satisfied by X and Y:

$$X + Y = 6 \quad \text{and} \quad 3 \; + Y = 15.$$

But this gives the contradiction that $X = 9/2$. Therefore it is not the case that $|A| = 20$.

c) $|A| = 15$.

Then $\theta = (a_1,\ldots,a_5)(b_1,\ldots,b_5)(c_1,\ldots,c_5)$. $\alpha_1,\ldots,\alpha_6$ must all have 5 blocks of 3 elements. Therefore α_1 is paired with 12 elements by $\alpha_1,\ldots,\alpha_6$. Hence a_1 must get paired with some element twice, a contradiction. Therefore it is not the case that $|A| = 15$.

d) $|A| = 10$.

Then $\theta = (a_1,\ldots,a_5)(b_1,\ldots,b_5)$. Each $\alpha_1,\ldots,\alpha_6$ must have 5 blocks of 2 elements. Hence a_1 is paired with some element twice. Therefore it is not the case that $|A| = 10$.

Therefore a, b, c, d combine to show that the block size of θ could not be 5. □

LEMMA 3.7. If the block size of θ is 4, then six of the atoms have five blocks of four elements and one of the atoms has ten blocks of two elements.

Proof. We have $|A| \leq 4 + (6\times 3) - 2 = 20$ (by Lemma 3.4). Hence one has the following possibilities:

a) $|A| = 20$.

Then $\theta = (a_1,\ldots,a_4)(b_1,\ldots,b_4)(c_1,\ldots,c_4)(d_1,\ldots,d_4)(e_1,\ldots,e_4)$. Each $\alpha_1,\ldots,\alpha_6$ must have either 2 or 4 element blocks. Let X = number of α_i's with 4 element blocks and Y = number of α_i's with 2 element blocks. As a must be paired with exactly 16 elements by $\alpha_1,\ldots,\alpha_6$, the following equations must be satisfied by X and Y:

$$X + Y = 6 \qquad \text{and} \qquad 3X + Y = 16.$$

Therefore $X = 5$ and $Y = 1$. Hence five α_i's must have 5 blocks of 4 elements and one α_i has 10 blocks of 2 elements.

b) $|A| = 16$.

Then $\theta = (a_1,\ldots,a_4)(b_1,\ldots,b_4)(c_1,\ldots,c_4)(d_1,\ldots,d_4)$. Each $\alpha_1,\ldots,\alpha_6$ has either 2 or 4 element blocks. Let X = number of α_i's with 4 element blocks and Y = number of α_i's with 2 element blocks. Then the following equations must be satisfied by X and X:

$$X + Y = 6 \qquad \text{and} \qquad 3X + Y = 12.$$

Therefore $X = 3$ and $Y = 3$. Hence three α_i's have 4 blocks of 4 elements and three of the α_i's have 8 blocks of 2 elements. Therefore by Theorem 2.1, L must be a FAR of some M_{p+1} where p is a prime. This is a contradiction, hence it is not the case that $|A| = 16$.

c) $|A| = 12$.

Then $\theta = (a_1,\ldots,a_4)(b_1,\ldots,b_4)(c_1,\ldots,c_4)$. Each $\alpha_1,\ldots,\alpha_6$ has either 2- or 3-element blocks. Let X = number of α_i's with 3-element blocks and Y = number of α_i's with 2-element blocks. Then the following equations must be satisfied by X and Y:

$$X + Y = 6 \qquad \text{and} \qquad 2X + Y = 8.$$

Therefore $X = 2$ and $Y = 4$. Hence two α_i's have 4 blocks of 3 elements and four of the α_i's have 6 blocks of 2 elements. By Theorem 2.1, this results again in a contradiction and it is not the case that $|A| = 12$.

d) $|A| = 8$.

Then $\theta = (a_1,\ldots,a_4)(b_1,\ldots,b_4)$. Clearly one cannot form the required $\alpha_1,\ldots,\alpha_6$. Therefore it is not the case that $|A| = 8$.

Thus only (a) remains as a possibility when the block size of θ is four. □

LEMMA 3.8. If the block size of θ is 3, then all seven atoms have five blocks of three elements.

Proof. Note $|A| \leq 3 + (6\times 2) = 15$, using Lemma 3.4. We then have the following possibilities:

a) $|A| = 15$.

Then $\theta = (a_1,a_2,a_3)(b_1,b_2,b_3)(c_1,c_2,c_3)(d_1,d_2,d_3)(e_1,e_2,e_3)$. Hence $\alpha_1,\ldots,\alpha_6$ must also have 5 blocks of 3 elements.

b) $|A| = 12$.

Then $\theta = (a_1,a_2,a_3)(b_1,b_2,b_3)(c_1,c_2,c_3)(d_1,d_2,d_3)$. Each $\alpha_1,\ldots,\alpha_6$ has either 2- or 3-element blocks. Let X = number of α_i's eith 3-element blocks and Y = number of α_i's with 2-element blocks. Then the following equations must be satisfied by

X and Y:

$$X + Y = 6 \qquad \text{and} \qquad 2X + Y = 9.$$

Therefore $X = 3$ and $Y = 3$. Hence three α_i's have 4 blocks of 3 elements and three α_i's have 6 blocks of 2 elements. By Theorem 2.1, this results again in a contradiction and it is not the case that $|A| = 12$.

c) $|A| = 9$.

Then $\theta = (a_1,a_2,a_3)(b_1,b_2,b_3)(c_1,c_2,c_3)$. Clearly one cannot form the required $\alpha_1,\ldots,\alpha_6$. Therefore it is not the case that $|A| = 9$.

d) $|A| = 6$.

Then $\theta = (a_1,a_2,a_3)(b_1,b_2,b_3)$ and one cannot form the required $\alpha_1,\ldots,\alpha_6$. Therefore it is not the case that $|A| = 6$.

Thus only (a) remains as a possibility when θ has block size three.

LEMMA 3.9. The block size of θ is not 2.

Proof. Suppose the block size of θ is two. Then each possible L must have at least two partitions with 2-element blocks. Hence by Theorem 2.1, L must be an IFAR of M_{p+1}; a contradiction. □

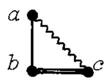
Therefore the only possible configurations for a complete FAR of M_7 are those given by conditions (1) and (2) of Theorem 3.2. Each of these possibilities will be disposed of separately in §4, and §5, thereby completing the proof of the result stated in the title of this paper.

4. KIRKMAN'S SCHOOLGIRL PROBLEM. Kirkman's schoolgirl problem (cf. [4],[8]) can be phrased as follows: "Fifteen girls are to march in five rows, three abreast, in such a way that no girl marches in the same row as another on more than one day of the seven days of the week".

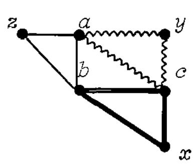
Observe that an IFAR of M_7 on a fifteen element set in which each of the seven atoms in represented by five blocks of three elements each is in fact a vertex transitive solution to Kirkman's schoolgirl problem. We show that there is no IFAR of the type described in (1) of Theorem 3.2 by proving:

THEOREM 4.0. *No solution to Kirkman's schoolgirl problem is vertex transitive.*

Proof. For any solution to Kirkman's schoolgirl problem the five rows for a given day partition the set of girls into classes of three. The seven partitions obtained in this way have pairwise trivial intersections, since each girl marches with two different girls on each of the seven days. Moreover clearly each girl marches with every other girl exactly once. It is also easy to argue that the pairwise join of any two of these partitions is the universal relation on all fifteen girls (left as an exercise to the reader). Thus <u>each</u> solution to Kirkman's problem is in fact a FR of M_7. Suppose that $\underline{L}_A = \langle A, L\rangle$, one of these solutions, in a *vertex transitive* FR of M_7. It suffices to consider three of the atoms whose partition relations we will represent by the "colors" θ_1, θ_2 and θ_3. We have without loss of generality for some $a,b,c \in A$

the configuration , and we label the other elements

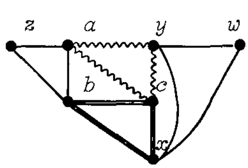
of the θ_i classes by:



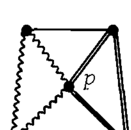
we distinguish the two cases $(x,y) \in \theta_1$ and $(x,y) \notin \theta_1$ and argue in each case that vertex transitivity produces a contradiction.

<u>CASE 1.</u> $(x,y) \in \theta_1$.

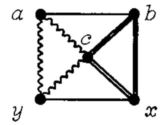
Thus we have



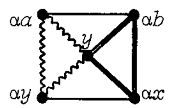
where a, b, c, w, x, y, z are all distinct points. We shall use vertex transitivity in the following way: since each point can be sent to every other point by a suitable automorphism, each colored graph located at any one point must occur somehow in the representation located at each other point. Thus the colored graph



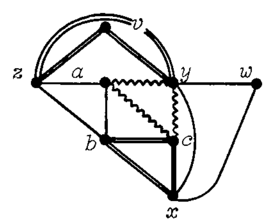
that sits on $p = c$ must also sit on the representation when $p = y$, since the automorphism which maps c to y must take



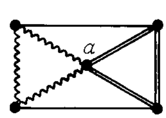
to an isomorphic subgraph:



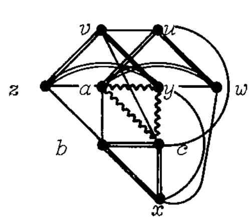
Note if αa and αx are <u>both</u> new points (different from a, b, c, w, y, z) then an edge a —— αb or a —— αx is forced, which is impossible. Hence at least one of the points αb or αx belongs to $\{a,b,c,w,y,z\}$. Inspection reveals that z is the only possibility and that αb or αx equals z and the other of them must be a "new" point v. Thus we have



The same diagram



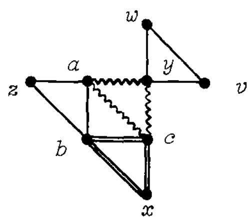
with $p = a$ forces by similar reasoning the configuration



where u is a new point as well. This last configuration is a proper subset of the fifteen element set whose θ_1 and θ_2 classes are entirely within the subset. This shows that θ_1, θ_2 (as equivalence relations) have join less than one, contradicting the fact that two atoms in a solution to Kirkman's schoolgirl problem must join to yield $\theta_1 \vee \theta_2 = 1$. This disposes of Case 1.

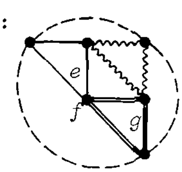
CASE 2. $(x,y) \notin \theta_i$.

Thus we have new points w, v related to $abcxyz$ as follows:

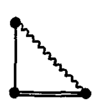


(If either of w or v were z or x, the argument in Case 1 applies interchanging the roles played by θ_1, θ_2; moreover it is not possible that w or v equals a, b, c, or y).

Observe further that we have the following "*exclusion principle*" forced on the representation by Case 1:

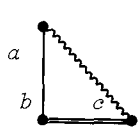


None of the dashed edges can be colored so as to form a triangle

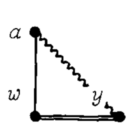


(otherwise we can apply the argument of Case 1). A similar exclusion principle applies to any such figure for other colors as well, since the argument in Case 1 could again be applied to those colors.

Now from

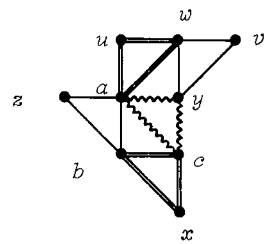


if we map a to y by an automorphism α, we force

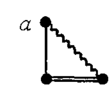


and it is easy to see that the third point u in the θ_2 class of y and w must be new

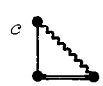
Thus we have as a subgraph of the representation the graph:



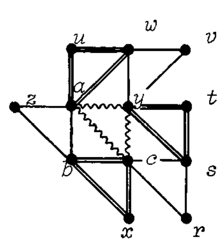
Next using the exclusion principle (applied to triangles $efg = abc$ and $efg = ywa$) it is easy to see that the θ_2 class of y and the θ_1 class of c must be points other than those we already have. Also since a lies on a triangle



c must lie on such a triangle

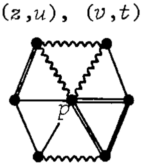


and it follows that the θ_1 class of c and the θ_2 class of y share exactly one element. Thus we have the subgraph



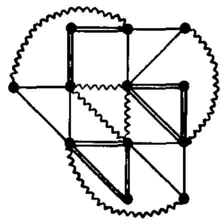
Using the exclusion principle again it is easy to see that the θ_3 class of z must include either (z,u) or (z,w), the θ_3 class of v must include either (v,t) or (v,s), and the θ_3 class of r must include either (r,x) or (r,b).

If any one of (z,u), (v,t) or (r,x) belongs to θ_3 then they all do, since the subgraph



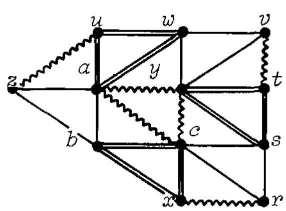
can be located at one of the points $p = a$, y or c and hence at all of them.

Let us first investigate the situation of none of (z,u), (v,t) or (r,x) belong to θ_3. Then we have the diagram:

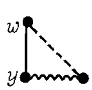


But this is impossible since it remains to place two θ_1 classes of three elements each and one θ_3 class of three elements among the remaining six points which do not have a θ_3 edge of the representation in the diagram presented here.

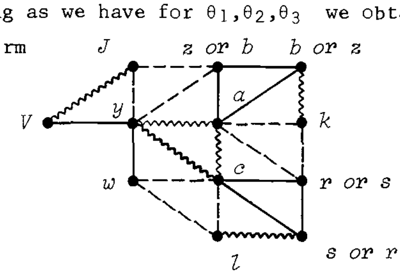
Thus we may assume that all of (z,u), (v,t) and (r,x) belong to θ_3 and the situation is pictured in the following diagram:



Now edge (w,c) is colored by some atom $\theta_4 \neq \theta_1$, θ_2, θ_3, and



where we have colored θ_4 by •----• . Since we could argue as in Case 1 on $\theta_1,\theta_3,\theta_4$ otherwise, we may assume that Case 2 obtains for these colors as well. Arguing as we have for $\theta_1,\theta_2,\theta_3$ we obtain a subgraph of the representation of the form



The θ_1 and θ_3 classes are fixed, enabling one to label the graph. Clearly j, k, l are not among a, b, c, r, s, z and we can only have j, k,l new points or possibly $l = x$, or $k = u$ or $J = t$. In fact $l = x$, $k = u$, $j = t$ each lead to a contradiction: $l = x \Rightarrow (l,c) \in \theta_4$ and $(l,c) = (x,c) \in \theta_3$; $k = u \Rightarrow (u,a) \in \theta_2 \cap \theta_4$; $j = t \Rightarrow (y,t) \in \theta_2 \cap \theta_4$. Thus j, k, l are all new elements.

Observe that the θ_3 class of v is $\{v,t,j\}$. Thus the θ_3 class of w cannot contain j or a, u, y, v, t, z, c, l because of other colorings, and cannot contain b or s because of the exclusion principle. Hence the θ_3 class of w can contain only elements x, r or k.

But w cannot be θ_3 related to r (as can be seen from the last diagram employing the exclusion principle). Hence w cannot be θ_3 related to x either, and thus the θ_3 class of w includes at most $\{k, w\}$, contradicting the fact that it must contain three elements. This concludes the argument for Case 2 and the proof that no solution to Kirkman's schoolgirl problem is vertex transitive. □

5. THE REMAINING CASE.

THEOREM 5.0. *There is no complete FAR of* M_7 *on a set of twenty elements such that one of the seven atoms is represented by ten two-element blocks and the other six are each represented by five four-element blocks.*

PROOF. From Lemma 3.3 we conclude such a FAR is actually an IFAR of M_7. Thus, assume to the contrary that $\langle A, M_7\rangle$ is such an IFAR and let us agree to color the ten two-element blocks by color 1 and the pairs in the other six equivalence relations consecutively by colors, 2, 3, 4, 5, 6 and 7. Denote the automorphism group of $\langle A, M_7\rangle$ by G and for each $a \in A$ let $f(a) \neq a$ be that element of A for which $(a, f(a))$ is 1-colored. Now if $\{x,y,u,v\}$ is one of the $i \geq 2$ colored blocks, then note that $f(\{x,y,u,v\}) = \{f(x), f(y), f(u), f(v)\}$ is disjoint from $\{x,y,u,v\}$ and that the i-colored edges induce an equivalence relation on $f(\{x,y,u,v\})$. Also $f(\{x,y,u,v\})$ can not be an i-block, otherwise the join of 1 and i would not be A^2. Using vertex transitivity then, we deduce that $f(\{x,y,u,v\})$ contains either exactly 2 non-adjacent i-colored edges (case 1) or no i-colored edges at all (case 2).

CASE 1: In order to dispose of case 1 we need to make the following more general observations. G acts on the set S_i of blocks of any color i . If $T \subset S_i$ is a *primitive* block, that is $G(T) = T$ or $G(T) \cap T = \emptyset$, then $\bigcup T$ is also a primitive block of A . This means that the sets $G(\bigcup T)$ form a G invariant equivalence relation on A. Hence T consists either of a single block or $T = S_i$.

Now if $\{x,y,u,v\}$ is an i-block with exactly 2 non-adjacent edges within $f(\{x,y,u,v\})$ then, because of vertex transitivity, each i-block B has exactly 2 i-colored edges in $f(B)$. If we define a graph on the i-blocks as vertices by stipulating that the i-blocks B,C are connected by an edge iff $|f(B) \cap C| = 2$, then this graph consists of disjoint circles. Indeed it can only be one circle, otherwise the atoms 1 and i would not join to A^2. So the diagram for the colors 1 and i looks as follows.

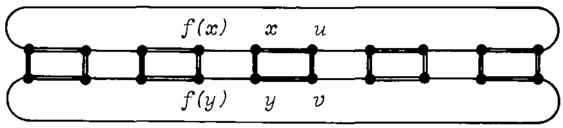
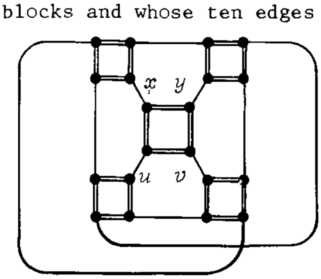


Figure 5.1

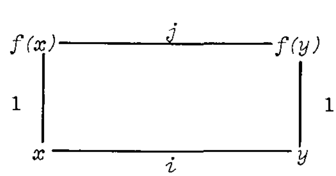
Now observe that if $\{x, y, u, v\}$ is an i-block and $(f(x), f(y))$ is i-colored then $\{x, y, f(x), f(y)\}$ is a primitive block of the automophism group H of the graph in colors 1 and i shown in fig. 5.1. Because $G \subset H$, $\{x, y, f(x), f(y)\}$ is also a primitive block of G and thus we can conclude that case 1 does not occur for any color i.

CASE 2. The number of 1-colored edges between any two i-colored blocks for any $i > 1$ is at most one and because the complete graph on five vertices has ten edges this number must be exactly one. This means that the 1 and i-colored blocks within A looks like a complete graph on five vertices whose vertices are the five i-colored blocks and whose ten edges are the ten 1-colored blocks (see figure 5.2).



LEMMA 5.1. If $\{x, y, z, u\}$ is an i-block and $f(\{x, y\})$ has color j, then $f(\{z, u\})$ has also color j.

PROOF. $x, y, f(x), f(y)$ form a quadrilateral whose edges are colored as indicated:



Because of vertex transistivity there must exist an identical colored quadrilateral containing z (x can be mapped to z). So either

$$\begin{tikzcd} f(z) \arrow[r, dash, "j"] \arrow[d, dash, "1"'] & f(u) \arrow[d, dash, "1"] \\ z \arrow[r, dash, "i"'] & u \end{tikzcd} \quad \text{or} \quad \begin{tikzcd} f(z) \arrow[r, dash, "j"] \arrow[d, dash, "1"'] & f(x) \arrow[d, dash, "1"] \\ z \arrow[r, dash, "i"'] & x \end{tikzcd}$$

$$\text{or} \qquad \begin{tikzcd} f(z) \arrow[r, dash, "j"] \arrow[d, dash, "1"'] & f(y) \arrow[d, dash, "1"] \\ z \arrow[r, dash, "i"'] & y \end{tikzcd}$$

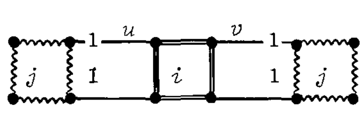
In the final case $(f(z),f(u))$ has color j as desired. Neither of the other cases in fact can arise.

In the second case, by transitivity, $\{f(x),f(y),f(z)\}$ is part of j-colored block. But then the fourth vertex of that block has to be $f(u)$ which can be seen by applying an automorphism from G which maps x to u. Similarly the third case can be seen to produce a contradiction in the edge coloring. □

LEMMA 5.2. If $\{x,y,z,u\}$ is an i-block then $f(\{x,y,z,u\})$ is a block for some color j.

<u>PROOF</u>. Let $(f(x),f(y))$ be j-colored, then we know from Lemma 5.1, that $(f(z),f(u))$ is also j-colored. Each j-colored block contains four elements. Let a,b be the other 2 elements such that $\{f(z),f(u),a,b\}$ is a j-colored block. If $\{a,b\} \cap \{x,y,u,v\} \neq \emptyset$ then we can assume without loss of generality that $a = x$ That means that x is contained in a j-block B_x such that $|B \cap f(\{x,y,u,v\})| = 2$. By vertex transitivity there exists such a block B_y, B_z, B_u for each of y,z and u. But then two of them must have a point in common, hence be equal and then intersect $\{x,y,z,u\}$ in at least two elements.

So we can assume that $\{a,b\} \cap \{x,y,u,z\} = \emptyset$. If we now define a graph on the i and j block as vertices and we say that the i-block B and the j block C form an edge in this graph just when $|f(B) \cap C| = 2$, then this graph consists of a set of disjoint circles. Because of vertex transitivity, each of those circles contains the same **number** of i-blocks and j-blocks as any other such circle. This means that this number is either one or five. If the number is one, we get the desired result. If it is five, the diagram contains the following sub-diagram on 12 elements:



But this produces the following contradiction in the coloring of the blocks: Each of $\{x,y,u,v\}$ is a distinct j block different from those above, but there are only three j-blocks left. This establishes Lemma 5.2. □

LEMMA 5.3. To each color i with $i > 1$ there corresponds a color i^*, the dual of i, such that $(i^*)^* = i$ and if B is an i-block, then $f(B)$ is an i^* block.

PROOF. Because case 1 has been disposed of for every color $i > 1$, each 1 and i diagram looks like figure 5.2. If B is an i-block then by Lemma 5.2 there is a j such that $f(B)$ is a j-block. By vertex-transitivity then the same is true for every other i-block. Of course the color j is the dual of i.

Let us assume without loss of generality that $2^* = 3$, $4^* = 5$ and $6^* = 7$. Observe now that if (x,y) is 1 colored and (u,z) is 1 colored, and two elements from $\{x,y,u,z\}$ are i-colored then the other two are i^*-colored (Lemma 5.1). This means that for any two 1-colored edges $(x,f(x))$, $(y,f(y))$ exactly two of the dual pairs of colors are present on the edges between them. We will say that i is in $(x,f(x))$, $(y,f(y))$ if one of the four not 1-colored pairs of x, $f(x)$, y, $f(y)$ is i-colored and $i < i^*$. Each i-block produces six such pairs of 1-colored edges which contain i and no two i-blocks have such a pair in common, hence there are thirty 1-colored pairs which contain i. Because there are ten 1-colored edges, there are $\binom{10}{2} = 45$ pairs of 1-colored edges. Thirty of them contain i, so fifteen contain the other two dual pairs of colors only. We conclude that for any two dual pairs, there are fifteen pairs of 1-colored edges which contain them. On the other hand, each of the six pairs of 1-colored edges associated with any particular 2-block contains exactly one other pair, either a 4-5 or a 6-7 pair. Assume r of those six pairs include 4-5 and s include 6-7. Because of vertex-transitivity this distribution holds for every other 2-block. So $5r = 15 = 5s$ and $r = s = 3$. If $\{x,y,u,z\}$ is a 2-block, define a graph by stipulating that its vertex set is x,y,u,z and two vertices a,b are connected by an edge if $(a,f(a))$ and $(b,f(b))$ include the pair 3-4. This graph contains three edges and four vertices and must be regular because of vertex-transitivity. But no vertex-transitive graph with three edges on four points exists. This contradiction shows that 2 can not be realised either. This completes the proof of Theorem 5.0. □

6. CONCLUSION. If $\mathfrak{A}$ is a finite algebra with congruence lattice M_7 then $\langle A, \mathfrak{C}\mathrm{on}\,\mathfrak{A}\rangle$ is a FAR of M_7. By Theorems 3.2, 4.0 and 5.0 there are however no <u>complete</u> FAR's of M_7, thus $\langle A, \mathfrak{C}\mathrm{on}\,\mathfrak{A}\rangle$ is not complete. Hence for some pair $a,b \in A$ the edge (a,b) fails to belong to any atom and the principal congruence θ_{ab} is A^2. Since each of the other congruences is principal we have established:

THEOREM 6.0. *Every finite algebra with congruence lattice* M_7 *has principal congruences.*

Indeed, the vertex transitivity of IFAR's for M_n implies that $A^2 = \theta_{ab}$ for a great many pairs $a,b \in A$ in any FAR of M_7, and places thereby some serious constraints on the nature of any potential such representation.

**Added in proof: A recent private communication from P. Pálfy assures us that Walter Feit has exhibited a FAR for* M_7 *on a very large set.*

BIBLIOGRAPHY.

[1] Hall, M., "combinatorial Theory", Blaisdell Publishing Company (1967)

[2] Pálfy, P.P., "On Certain Congruence Lattices of Finite Unary Algebras", Commentationes Mathematicae Universitatis Carolinae, 19, 1 (1978), 89-94.

[3] Pálfy, P. and P. Pudlák, "Congruence Lattices of finite algebras and intervals in subgroup lattices of finite groups", Algebra Universalis, 11, (1980) 22-27.

[4] Power, J., "On the Problem of the Fifteen Schoolgirls", Quarterly Journal of Pure and Applied Math, Vol. 7-8 (1866) p. 236-251.

[5] Pudlák, P., "Distributivity of strongly representable lattices", Algebra Universalis, 7 (1977) 85-92.

[6] Pudlák, P., and J. Tuma, "Every finite lattice can be embedded in a finite partition lattice:, Algebra Universalis, 10 (1980) 74-95.

[7] Quackenbush, R. and B. Wolk, "Strong representation of congruence lattices", Algebra Universalis, 1 (1971) 165-166.

[8] Ray - Chaudhuri, D.K. and R.M. Wilson, "Solution of Kirkman's schoolgirl problem", Combinatorics, A.M.S. Proc. Symp. Pure Math 9 (1971) 187-203.

[9] Stone, M.G. and R.H. Weemark, "On representing M_n's by congruence Lattices of Finite Algebras". Manuscript submitted to Discrete Mathematics (Dec. 1980).

[10] Street, A.P., and W.D. Wallis, "Combinatorial Theory: An Introduction", Published by CBRC, Winnipeg (1977).

[11] Weedmark, R.H., "Finite Algebraic Partition Lattices", M.Sc. Thesis, University Of Calgary, 1980.

[12] Werner, H., "Which partition lattices are congruence lattices?", Coll. Math. Soc. J. Bolyai 14, Lattice Theory, Szeged (Hungary) (1974), 433-453.

NILPOTENCE IN PERMUTABLE VARIETIES

M.R. Vaughan-Lee

In this paper we show how a commutator calculus can be developed in any variety $\mathfrak{U}$ of unital algebras with permutable weakly regular congruences. (This class of algebras includes groups, rings, Lie rings, and loops.) We show how abelian algebras, centralizers, nilpotent algebras, and solvable algebras can be defined in this setting. We show that the abelian algebras in $\mathfrak{U}$ form a finitely based subvariety which is definitionally equivalent to a variety of modules. We also prove that if A is a finite nilpotent algebra in $\mathfrak{U}$, and if A is a direct product of algebras of prime power order, then A has a finite basis for its laws.

We show how the commutator of two congruences can be defined in this setting and confirm that the definitions we give for abelian algebras, centralizers, nilpotent algebras, and solvable algebras are equivalent in $\mathfrak{U}$ to the definitions given by Freese and McKenzie (1982) for modular varieties.

I am indebted to Ralph Freese for indicating how the results on nilpotent algebras can be extended to modular varieties. He showed me how in a modular variety solvable algebras have permutable congruences, and finite nilpotent algebras have regular congruences. The addition of extra constants to the language makes no difference to any of the proofs, though some of the theorems have to be restated slightly. For example the congruence class of 0 is no longer a subalgebra if there are extra constants. He has even shown how the existence of an equationally defined idempotent constant is unnecessary, but rather different arguments are needed without this assumption. The main result in this paper is Theorem 7.6, and this can be generalized as follows.

THEOREM. *Let $\mathfrak{U}$ be a variety of algebras with a finite set of finitary operations and an equationally defined idempotent constant. Suppose also that the algebras in $\mathfrak{U}$ have modular congruence lattices. If* A *is a finite nilpotent algebra in $\mathfrak{U}$, and if* A *is a direct product of algebras of prime power order, then* A *has a finite basis for its laws.*

This theorem generalizes well known results for groups and rings, and also provides new information about nilpotent loops. (Any finite nilpotent group or ring is a direct product of algebras of prime power order.)

We give an example of a nilpotent loop of order 12 which illustrates the difficulty of extending this theorem to arbitrary finite nilpotent algebras. We also give an example of a locally finite variety of loops of nilpotency class 3 which does not have the finite basis property. These loop examples grew out of many fruitful discussions I had with Trevor Evans at Emory University in 1977.

Several of the results obtained here are similar to results obtained by Gumm (1980) and Gumm (1982).

We will use upper case letters to denote sets and algebras, and lower case letters to denote elements and term functions. The letters $x,y,z,x_1,x_2,\ldots,y_1,y_2,\ldots,z_1,z_2,\ldots$ will be reserved for free generators in relatively free algebras. We will use the notation $\bar{x},\bar{a},\bar{b}$ to denote sequences of elements and if t is a term function we will sometimes denote

$$t(a_1,\ldots,a_m,b_1,\ldots,b_n)$$

by $t(\bar{a},\bar{b})$ and so on.

2. DEFINITIONS AND HIGMAN'S LEMMA. Let Ω be a finite set of finitary operations containing a single nullary operation (constant) 0. Let $\mathcal{U}$ be a variety of Ω-algebras with the property that if $A \in \mathcal{U}$ then

(1) A is unital, that is $\{0\}$ is a subalgebra of A,

(2) A has permutable congruences,

(3) A has weakly regular congruences, that is every congruence of A is determined by the congruence class of 0.

Condition (1) is equivalent to the condition that $f(0,0,\ldots,0) = 0$ is a law in $\mathcal{U}$ for all $f \in \Omega$.

Mal'cev (1954) showed that condition (2) is equivalent to the existence of a ternary term function p such that $p(x,y,y)=x$, $p(x,x,y)=y$ are laws in $\mathcal{U}$. In rings $p(x,y,z)=x-y+z$, and in groups $p(x,y,z)=xy^{-1}z$.

We will show that condition (3) is also a Mal'cev condition, but first we prove the following lemma.

LEMMA 2.1. *If* $A \in \mathcal{U}$ *and* $R \subset A^2$ *then the congruence of* A *generated by* R *consists of the set* S *of pairs*

$$(t(a_1,a_2,\ldots,a_n),t(b_1,b_2,\ldots,b_n))$$

where t *is a term function and* $(a_i,b_i) \in R$ *or* $a_i=b_i$ *for* $i=1,2,\ldots,n$.

Proof. S is certainly a subalgebra of A^2 containing R and contained in the congruence generated by R. Furthermore S is clearly reflexive, and so it suffices to show that S is symmetric and transitive. So let $(t(\bar{a}),t(\bar{b})) \in S$. Then

$$(t(\bar{b}),t(\bar{a})) = (p(t(\bar{a}),t(\bar{a}),t(\bar{b})),p(t(\bar{a}),t(\bar{b}),t(\bar{b})))$$

which is an element of S, and so S is symmetric. Suppose also that $(u(\bar{c}),u(\bar{d})) \in S$, where $t(\bar{b}) = u(\bar{c})$. Then

$$(t(\bar{a}),u(\bar{d})) = (p(t(\bar{a}),u(\bar{c}),u(\bar{c})),p(t(\bar{b}),u(\bar{c}),u(\bar{d})))$$

which is an element of S. It follows that S is transitive and this completes the proof of Lemma 2.1.

Now consider condition (3) again. Let A be the $\mathcal{U}$-free algebra generated by x and y, and let α be the endomorphism of A which maps x to x and maps y to x. Then α induces a congruence on A containing (x,y). If A satisfies (3) then this congruence is determined by the congruence class of 0 and so there are elements $q_1, q_2, \ldots, q_k \in A$ (with $q_i(x,x)=0$ for $i=1,2,\ldots,k$) such that (x,y) lies in the congruence generated by $(q_1,0),(q_2,0),\ldots,(q_k,0)$. Using the result above this implies that there is a term function r such that

$$(x,y) = (r(x,y,q_1,q_2,\ldots,q_k), r(x,y,0,0,\ldots,0)).$$

This proves the following lemma

LEMMA 2.2. *Condition (3) is equivalent to the existence of binary term functions* $q_1, q_2, \ldots, q_k$ *and a (k+2)-ary term function* r *such that*

$$q_i(x,x) = 0 \textit{ for } i=1,2,\ldots,k,$$
$$r(x,y,q_1(x,y),q_2(x,y),\ldots,q_k(x,y)) = x$$
$$r(x,y,0,0,\ldots,0) = y$$

are laws in $\mathcal{U}$.

We define commutators as follows. Let F be the $\mathcal{U}$-free algebra with basis x_1, $x_2, \ldots$. For each subset S of the positive integers we define an endomorphism δ_S of F by

$$x_i\delta_S = 0 \quad \text{if } i \in S,$$
$$x_i\delta_S = x_i \quad \text{if } i \notin S.$$

We also denote $\delta_{\{i\}}$ by δ_i. An element $w \in F$ is said to be a commutator if there is a finite set S of positive integers such that

(1) w is in the subalgebra of F generated by $\{x_i : i \in S\}$,

(2) $w\delta_i = 0$ for all $i \in S$.

We then say that w involves the variable x_i for all $i \in S$. In rings for example, x_3, x_1x_2, $x_1x_2x_3+2x_3x_1x_2x_2$ are commutators. In groups x_4^2, $[x_2,x_3]$, $[x_1,x_2,x_2]$ are commutators. In loops the associator $((x_1x_2)x_3)/(x_1(x_2x_3))$ is also a commutator. (Note that in groups and loops the idempotent element is usuallydenoted by 1 instead of 0.)

The following result provides an extremely powerful tool for calculating in varieties of $\mathcal{U}$-algebras. The result is well known in groups and rings, and I shall call it Higman's Lemma as that is what it is called in group theory after Higman (1959).

HIGMAN'S LEMMA. *If* u,v *are elements of* F *then there is a finite set* C *of commutators with the property that if* S *is any set of positive integers then*

(1) the law $u\delta_S = v\delta_S$ *implies the law* $c\delta_S = 0$ *for all* $c \in C$,

(2) $(u\delta_S, v\delta_S)$ *is contained in the congruence generated by* $\{(c\delta_S, 0) : c \in C\}$.

Proof. If $w \in F$ then we define $w\delta_i^* := p(w, w\delta_i, 0)$ and if $S = \{i,j,\dots,m\}$ is a finite set of positive integers with $i < j < \dots < m$ then we define

$$w\delta_S^* := w\delta_i^*\delta_j^*\dots\delta_m^*.$$

Now let C be the set of elements of the form $q_i(u,v)\delta_K\delta_L^*$, $i=1,2,\dots,k$, K,L disjoint sets of positive integers such that L is finite and $K \cup L = \{1,2,\dots\}$. We show that C satisfies the conditions of the lemma

It is easy to see that if S and T are any sets of positive integers then $\delta_S\delta_T = \delta_T\delta_S$ and hence that $\delta_S\delta_T^* = \delta_T^*\delta_S$. It is also easy to see that $\delta_T^*\delta_S = 0$ if $S \cap T$ is non-empty. Clearly $q_i(u,v)\delta_K\delta_L^*$ is contained in the subalgebra of F generated by $\{x_j : j \in L\}$ and, by the above remarks $q_i(u,v)\delta_K\delta_L^*\delta_j = 0$ if $j \in L$. So the elements of C are commutators. If S is any set of positive integers then the law $u\delta_S = v\delta_S$ implies the laws $q_i(u\delta_S, v\delta_S) = 0$ for $i=1,2,\dots,k$, and hence implies the laws $q_i(u\delta_S, v\delta_S)\delta_K\delta_L^* = 0$. Since $q_i(u\delta_S, v\delta_S)\delta_K\delta_L^* = q_i(u,v)\delta_K\delta_L^*\delta_S$ it follows that the law $u\delta_S = v\delta_S$ implies the laws $\{w\delta_S = 0 : w \in C\}$.

To show that $(u\delta_S, v\delta_S)$ is contained in the congruence generated by the elements $\{(w\delta_S, 0) : w \in C\}$ it is sufficient to show that the elements $(q_i(u,v)\delta_S, 0)$ lie in this congruence. To do this it is sufficient to show that if $u \in F$ then $(u,0)$ is contained in the congruence generated by the elements $(u\delta_K\delta_L^*, 0)$. Let u lie in the subalgebra generated by the elements $x_1, x_2, \dots, x_n$. Then $u\delta_K\delta_L^* = 0$ unless L is contained in $\{1,2,\dots,n\}$, and if $M = K \cap \{1,2,\dots,n\}$ then $u\delta_K = u\delta_M$. So it is sufficient to show that $(u,0)$ is contained in the congruence α generated by the elements $(u\delta_K\delta_L^*, 0)$, where $K \cup L = \{1,2,\dots,n\}$, $K \cap L = \emptyset$. We show by induction on r that α contains the elements $(u\delta_K\delta_L^*, 0)$ where $K \cup L = \{1,2,\dots,n-r\}$, $K \cap L = \emptyset$, for $r=0,1,\dots,n$. The case r=0 follows from the definition of α and the case r=n is what we want to prove. So suppose that the result is true for r, and let $K \cup L = \{1,2,\dots,n-r-1\}$, $K \cap L = \emptyset$. Then if $M = K \cup \{n-r\}$ and if $N = L \cup \{n-r\}$ we have $(u\delta_M\delta_L^*, 0) \in \alpha$, and $(u\delta_K\delta_N^*, 0) \in \alpha$. Now $u\delta_M\delta_L^* = u\delta_K\delta_{n-r}\delta_L^* = u\delta_K\delta_L^*\delta_{n-r}$ and $u\delta_K\delta_N^* = u\delta_K\delta_L^*\delta_{n-r}^* = p(u\delta_K\delta_L^*, u\delta_K\delta_L^*\delta_{n-r}, 0)$. So $(u\delta_K\delta_L^*\delta_{n-r}, 0) \in \alpha$ and $(p(u\delta_K\delta_L^*, u\delta_K\delta_L^*\delta_{n-r}, 0), 0) \in \alpha$ which implies that $(u\delta_K\delta_L^*, 0) \in \alpha$ as required.

This completes the proof of Higman's Lemma.

3. ABELIAN ALGEBRAS. An algebra $A \in \mathcal{U}$ is said to be abelian if w=0 is a law in A whenever w is a commutator involving at least two variables.

THEOREM 3. *The variety of abelian algebras in* $\mathcal{U}$ *is definitionally equivalent to a variety of modules.*

Proof. If A is an abelian algebra in $\mathcal{U}$ we define a binary operation + on A by

$$a+b := p(a,0,b),$$

and a unary operation − by

$$-a := p(0,a,0).$$

We show that these operations turn A into an abelian group (with additive identity 0). First, it follows immediately from the properties of the term function p that

$$a+0 = 0+a = a$$

for all $a \in A$. Next, consider the pair of words x_1+x_2, x_2+x_1. By Higman's Lemma there is a set C of commutators such that the law $(x_1+x_2)\delta_S = (x_2+x_1)\delta_S$ is equivalent to the set of laws $\{w\delta_S = 0 : w \in C\}$ for all subsets S of the positive integers. Taking $S = \{1\}$ we see that the law $x_2 = x_2$ is equivalent to the set of laws $\{w\delta_1 = 0\}$, and so w must involve x_1 for all $w \in C$. Similarly taking $S = \{2\}$ we see that w involves both x_1 and x_2, and so $w = 0$ is a law in A for all $w \in C$. This implies that $x_1+x_2 = x_2+x_1$ is a law in A. Similarly the law $(x_1+x_2)+x_3 = x_1+(x_2+x_3)$ is equivalent to a set of laws of the form $w = 0$ where w is a commutator involving x_1,x_2, and x_3. So + is associative on A. Finally a similar argument shows that the law $p(x_1,x_2,0) = x_1+(-x_2)$ holds in A, and so $x+(-x) = 0$ is a law in A. This shows that A is an abelian group under +.

Now let $f \in \Omega$ and apply Higman's Lemma to the law

$$f(x_1,x_2,\ldots,x_n) = f(x_1,0,\ldots,0)+f(0,x_2,0,\ldots,0)+\ldots+f(0,\ldots,0,x_n).$$

Let D be the set of commutators associated with this law and let $S = \{1,2,\ldots,i-1,i+1,\ldots,n\}$. Then the law

$$f(x_1,\ldots,x_n)\delta_S = (f(x_1,0,\ldots,0)+\ldots+f(0,\ldots,0,x_n))\delta_S$$

is trivial, and so $w\delta_S = 0$ for all $w \in D$. This means that each commutator in D must involve at least one of the variables $x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n$. Since this is true for all $i=1,2,\ldots,n$ it follows that each commutator in D involves at least two variables, and so if $w \in D$ the $w = 0$ is a law in A. So

$$f(x_1,\ldots,x_n) = f(x_1,0,\ldots,0)+\ldots+f(0,\ldots,0,x_n)$$

is a law in A. This means that every term function on A can be expressed as a composition of unary term functions and +. We turn the set R of unary term functions into a ring by setting

$$(f+g)(a) = f(a) + g(a),$$
$$(fg)(a) = f(g(a)).$$

All the ring axioms for R except for one of the distributive laws follow immediately from the fact that A is an abelian group under +. This distributive law follows easily from another application of Higman's Lemma. This completes the proof of Theorem 3.

Another characterization of Abelian algebras is obtained in Section 5.

4. NORMAL SUBALGEBRAS. If A is an algebras in $\mathcal{U}$, and if α is any congruence on A then the congruence class of 0 is a subalgebra of A. Subalgebras which arise in this way are called normal subalgebras. Because of the regularity of congruences of A there is an isomorphism between the lattice of congruences of A and the lattice of normal subalgebras. The following result characterizes normal subalgebras and follows immediately from Lemma 2.1.

LEMMA 4. *If* B *is a subalgebra of* A *then* B *is a normal subalgebra if and only if*

$$f(a_1,\ldots,a_m,b_1,\ldots,b_n) \in B$$

whenever $a_1,\dots,a_m \in A$ *and* $b_1,\dots,b_n \in B$ *and* f *is an* $(m+n)$*-ary term function such that* $f(a_1,\dots,a_m,0,\dots,0) = 0$.

5. CENTRALIZERS. If M is a normal subalgebra of an algebra $A \in \mathcal{U}$ we define the centralizer of M to be the set of elements $c \in A$ such that

$$w(a_1,a_2,\dots,a_n,c) = 0$$

whenever w is a commutator involving at least two variables and $a_1 \in M$, $a_2,\dots,a_n \in A$. In particular the centre of A is the set of elements $c \in A$ such that

$$w(a_1,a_2,\dots,a_n,c) = 0$$

for all $a_1,a_2,\dots,a_n \in A$, whenever w is a commutator involving at least two variables.

LEMMA 5.1. *If* M *is a normal subalgebra of* A *then the centralizer of* M *is also a normal subalgebra.*

Proof. Let C be the centralizer of M. First we show that C is a subalgebra of A. Let f be an m-ary operation in Ω and let $c_1,c_2,\dots,c_m \in C$. We need to show that $f(c_1,\dots,c_m)$ lies in C. So let w be a commutator involving $n+1$ variables where $n > 0$, let $a_1 \in M$, and let $a_2,\dots,a_n \in A$. By Higman's Lemma we see that the law

$$w(x_1,x_2,\dots,x_n,f(y_1,\dots,y_m)) = 0$$

is equivalent to a set of laws of the form $u = 0$ where u is a commutator involving $x_1,\dots,x_n$ and at least one of $y_1,y_2,\dots,y_m$. Furthermore

$$(w(x_1,\dots,x_n,f(y_1,\dots,y_m)),0)$$

is in the congruence generated by the elements $(u,0)$. If we substitute $a_1,\dots,a_n$, $c_1,\dots,c_m$ for $x_1,\dots,x_n,y_1,\dots,y_m$ then all the elements u take value 0, and so

$$w(a_1,\dots,a_n,f(c_1,\dots,c_m)) = 0.$$

This proves that C is a subalgebra. To show that C is a normal subalgebra it is sufficient by Lemma 4 to show that

$$w(a_1,\dots,a_n,t(c_1,\dots,c_m,\tilde{d})) = 0$$

whenever t is a term function such that $t(0,\dots,0,\tilde{d}) = 0$. We apply Higman's Lemma to the law

$$w(x_1,\dots,x_n,t(y_1,\dots,y_m,\tilde{z})) = w(x_1,\dots,x_n,t(0,\dots,0,\tilde{z})).$$

An argument similar to the one used to prove that C is a subalgebra shows that C is a normal subalgebra.

LEMMA 5.2. *The following conditions on an element* $c \in A$ *are equivalent*

(1) $c \in \zeta(A)$,

(2) $t(a_1,\dots,a_{i-1},a_i+d,a_{i+1},\dots,a_n) = t(a_1,\dots,a_i,\dots,a_n)+t(0,\dots,0,d,0,\dots,0)$ *for all term functions* t, *all* $a_1,\dots,a_n \in A$, *and all* d *in the subalgebra of* A *generated by* c.

(3) $f(a_1,\dots,a_{i-1},a_i+d,a_{i+1},\dots,a_n) = f(a_1,\dots,a_i,\dots,a_n)+f(0,\dots,0,d,0,\dots,0)$ *whenever* $f \in \Omega$, *or* $f = +$, *for all* $a_1,\dots,a_n \in A$ *and all* d *in the subalgebra of* A *generated by* c.

Proof. First we show that (1) implies (2). Let u be a unary term function, and consider the law

$$t(x_1,\ldots,x_{i-1},x_i+u(x_{n+1}),x_{i+1},\ldots,x_n) = t(x_1,\ldots,x_i,\ldots,x_n)+t(0,\ldots,0,u(x_{n+1}),0,\ldots,0).$$

By Higman's Lemma there is a set C of commutators each of which involves x_{n+1} and at least one of the variables $x_1,\ldots,x_n$, such that this law is equivalent to the set of laws $\{w = 0 : w \in C\}$. Furthermore

$$(t(x_1,\ldots,x_i+u(x_{n+1}),\ldots,x_n),t(x_1,\ldots,x_n)+t(0,\ldots,u(x_{n+1}),\ldots,0))$$

is in the congruence generated by the set $\{(w,0) : w \in C\}$. If $a_1,\ldots,a_n \in A$, $c \in \zeta(A)$, and we substitute $a_1,\ldots,a_n,c$ for $x_1,\ldots,x_n,x_{n+1}$ then the commutators in C all take value 0. Hence

$$(t(a_1,\ldots,a_i+u(c),\ldots,a_n),t(a_1,\ldots,a_n)+t(0,\ldots,u(c),\ldots 0))$$

is contained in the trivial congruence. This proves that (1) implies (2). Clearly (2) implies (3), and a straightforward induction shows that (3) implies (2). To show that (2) implies (1), let c satisfy (2), let w be a commutator involving n+1 variables where n > 0, and let $a_1,\ldots,a_n \in A$. Then

$$w(a_1,\ldots,a_n,c) = w(a_1,\ldots,a_n,0)+w(0,\ldots,0,c) = 0,$$

and so $c \in \zeta(A)$.

COROLLARY 5.3. *An algebra* $A \in \mathcal{U}$ *is abelian if*

$$f(a_1,\ldots,a_i+a,\ldots,a_n) = f(a_1,\ldots,a_n)+f(0,\ldots,a,\ldots,0)$$

for all $a,a_1,\ldots,a_n \in A$ *whenever* $f \in \Omega$ *or* $f = +$.

LEMMA 5.4. *If* T *is a transversal for* $\zeta(A)$ *in* A *then every element of* A *can be written uniquely in the form* $t+c$, $t \in T$, $c \in \zeta(A)$.

Proof. By a transversal we mean a set of representatives in A for the congruence classes of A under the congruence determined by the centre of A. Let α be this congruence. If $a \in A$ then $(a,t) \in \alpha$ for some $t \in T$. So by Lemma 2.1 there is a term function t and sequences $\tilde{b},\tilde{c}$ of elements of A and $\zeta(A)$ respectively such that

$$(a,t) = (t(\tilde{b},\tilde{c}),t(\tilde{b},0,\ldots,0)).$$

Now by Lemma 5.2,

$$t(\tilde{b},\tilde{c}) = t(\tilde{b},0,\ldots,0)+t(0,\ldots,0,\tilde{c}).$$

So $a = t+c$ where $c = t(0,\ldots,0,\tilde{c}) \in \zeta(A)$. To show that this representation is unique suppose that $t+c = u+d$, where $t,u \in T$ and $c,d \in \zeta(A)$. Now $t = t+c \bmod \alpha$ and $u=u+d \bmod \alpha$ and so this implies that $t=u$. So suppose that $t+c=t+d$. Then by Lemma 2.2, $q_i(t+c,t+d) = 0$ for $i=1,2,\ldots,k$. But since c and d are central

$$q_i(t+c,t+d) = q_i(t,t)+q_i(c,d) = q_i(c,d),$$

and so $q_i(c,d) = 0$ for $i=1,2,\ldots,k$. This implies that $c=d$.

6. THE COMMUTATOR OF TWO CONGRUENCES. If M,N are two normal subalgebras of an algebra $A \in \mathcal{U}$ then we define $[M,N]$ as the normal subalgebra generated by the set of elements of the form $w(a_1,a_2,\ldots,a_n)$ where w is a commutator involving at least two

variables and $a_1 \in M$, $a_2 \in N$. If M,N correspond to the congruences α,β respectively then we show that $[M,N]$ corresponds to the congruence $[\alpha,\beta]$ as defined by Smith (1976). By Proposition 4.4 of Freese and McKenzie (1982), $[\alpha,\beta]$ is the smallest congruence γ of A with the property that if t is any term function and if $\tilde{a},\tilde{a}',\tilde{b},\tilde{b}'$ are sequences of elements of A such that $\tilde{a}=\tilde{a}' \bmod \alpha$ and $\tilde{b}=\tilde{b}' \bmod \beta$ then $t(\tilde{a},\tilde{b}) = t(\tilde{a},\tilde{b}') \bmod \gamma$ if and only if $t(\tilde{a}',\tilde{b}) = t(\tilde{a}',\tilde{b}') \bmod \gamma$.

First we show that $[M,N] = \{0\} \bmod [\alpha,\beta]$. Let w be any commutator involving at least two variables and take $t=w$, $\tilde{a}=a_1 \in M$, $\tilde{a}'=0$, $\tilde{b}=(a_2,\ldots,a_n)$ with $a_2 \in N$, and $\tilde{b}'=(0,a_3,\ldots,a_n)$. Then $t(\tilde{a},\tilde{b}) = w(a_1,\ldots,a_n)$ which is a typical generator of $[M,N]$. It is easy to see that $t(\tilde{a}',\tilde{b}) = t(\tilde{a},\tilde{b}') = t(\tilde{a}',\tilde{b}') = 0$ and so $w(a_1,\ldots,a_n)=t(\tilde{a},\tilde{b})=0 \bmod [\alpha,\beta]$.

Conversely we show that if t is any term function and $\tilde{a}=\tilde{a}' \bmod \alpha$, $\tilde{b}=\tilde{b}' \bmod \beta$ then $t(\tilde{a},\tilde{b}) = t(\tilde{a},\tilde{b}') \bmod [M,N]$ if and only if $t(\tilde{a}',\tilde{b}) = t(\tilde{a}',\tilde{b}') \bmod [M,N]$. If a is a member of the sequence $\tilde{a}$, and if a' is the corresponding member of the sequence $\tilde{a}'$ then by Lemma we can find a term function v and sequences of elements $\tilde{d},\tilde{e}$ in M,A respectively such that $a=v(\tilde{d},\tilde{e})$, $a'=v(\tilde{0},\tilde{e})$. Similarly if b is a member of the sequence $\tilde{b}$ and if b' is the corresponding member of the sequence $\tilde{b}'$ then we can find a term function w and sequences of elements $\tilde{f},\tilde{g}$ in N,A respectively such that $b=w(\tilde{f},\tilde{g})$ and $b'=w(\tilde{0},\tilde{g})$. Combining these results we can find a term function u and sequences $\tilde{m},\tilde{n},\tilde{c}$ of elements in M,N,A respectively such that

$$\begin{aligned} t(\tilde{a},\tilde{b}) &= u(\tilde{m},\tilde{n},\tilde{c}), \\ t(\tilde{a},\tilde{b}') &= u(\tilde{m},\tilde{0},\tilde{c}), \\ t(\tilde{a}',\tilde{b}) &= u(\tilde{0},\tilde{n},\tilde{c}), \\ t(\tilde{a}',\tilde{b}') &= u(\tilde{0},\tilde{0},\tilde{c}). \end{aligned}$$

Consider the law

$$p(u(\tilde{0},\tilde{y},\tilde{z}),u(\tilde{0},\tilde{0},\tilde{z}),u(\tilde{x},\tilde{0},\tilde{z})) = u(\tilde{x},\tilde{y},\tilde{z}).$$

By Higman's Lemma this is equivalent to a set of laws of the form $w=0$ where w is a commutator involving at least one variable from the sequence $\tilde{x}$ and at least one variable from the sequence $\tilde{y}$. Furthermore

$$(p(u(\tilde{0},\tilde{y},\tilde{z}),u(\tilde{0},\tilde{0},\tilde{z}),u(\tilde{x},\tilde{0},\tilde{z})),u(\tilde{x},\tilde{y},\tilde{z}))$$

lies in the congruence generated by the elements $(w,0)$. If we substitute $\tilde{m},\tilde{n},\tilde{c}$ for $\tilde{x},\tilde{y},\tilde{z}$ respectively then each commutator w takes a value in $[M,N]$. So

$$p(u(\tilde{0},\tilde{n},\tilde{c}),u(\tilde{0},\tilde{0},\tilde{c}),u(\tilde{m},\tilde{0},\tilde{c})) = u(\tilde{m},\tilde{n},\tilde{c}) \bmod [M,N],$$

that is

$$p(t(\tilde{a}',\tilde{b}),t(\tilde{a}',\tilde{b}'),t(\tilde{a},\tilde{b}')) = t(\tilde{a},\tilde{b}) \bmod [M,N].$$

So if $t(\tilde{a}',\tilde{b}) = t(\tilde{a}',\tilde{b}') \bmod [M,N]$ then

$$\begin{aligned} t(\tilde{a},\tilde{b}) &= p(t(\tilde{a}',\tilde{b}),t(\tilde{a}',\tilde{b}'),t(\tilde{a},\tilde{b}')) \bmod [M,N] \\ &= p(t(\tilde{a}',\tilde{b}),t(\tilde{a}',\tilde{b}),t(\tilde{a},\tilde{b}')) \bmod [M,N] \\ &= t(\tilde{a},\tilde{b}'). \end{aligned}$$

Similarly

$$p(t(\tilde{a},\tilde{b}'),t(\tilde{a},\tilde{b}),t(\tilde{a}',\tilde{b})) = t(\tilde{a}',\tilde{b}') \bmod [M,N]$$

and this implies that if $t(\tilde{a},\tilde{b}) = t(\tilde{a},\tilde{b}') \bmod [M,N]$ then $t(\tilde{a}',\tilde{b}) = t(\tilde{a}',\tilde{b}') \bmod [M,N]$ This completes the proof that $[\alpha,\beta]$ is the congruence determined by $[M,N]$.

It follows immediately from this that the definitions of abelian algebras, centralizers, and centre given in this paper are equivalent to the definitions given for modular varieties in Freese and McKenzie.

If A is any algebra in $\mathcal{U}$ we define the lower central series $\gamma_i(A)$ inductively by setting $\gamma_1(A) = A$ and $\gamma_{i+1}(A) = [\gamma_i(A),A]$. A is nilpotent of class k if $\gamma_k(A)$ is non-zero and $\gamma_{k+1}(A) = \{0\}$. Note that if A is nilpotent of class k then $\gamma_k(A)$ is contained in the centre of A.

We define the derived series $A^{(i)}$ inductively by setting $A^{(0)} = A$, and defining $A^{(i+1)} = [A^{(i)},A^{(i)}]$. We say that A is solvable of derived length k if $A^{(k-1)}$ is non-zero and $A^{(k)} = \{0\}$.

7. NILPOTENT ALGEBRAS. If A is an algebra in $\mathcal{U}$ then we define the ascending central series $\zeta_r(A)$ by setting $\zeta_1(A) = \zeta(A)$ and setting $\zeta_{r+1}(A)$ equal to the inverse image in A of the centre of $A/\zeta_r(A)$. A is nilpotent if and only if some term of the ascending central series of A equals A.

LEMMA 7.1. *Let* A *be a nilpotent algebra in* $\mathcal{U}$ *and let* M *be a normal subalgebra of* A. *If* T *is a transversal for* M *in* A *then every element of* A *can be written uniquely in the form* t+m *for some* $t \in T$ *and some* $m \in M$.

Proof. We define a series $M = M_0 > M_1 > \dots > M_r = \{0\}$ of normal subalgebras inductively by setting $M_{i+1} = [M_i,A]$. (The series terminates since A is nilpotent.) We prove the lemma by induction on r. If r=1 then M is contained in the centre of A, and the proof is as in the proof of Lemma 5.4. By induction suppose that the lemma holds for the normal subalgebra M/M_{r-1} of A/M_{r-1}. The image of T in A/M_{r-1} is a transversal for M/M_{r-1}, and so by induction every element of A can be written in the form t+m mod M_{r-1} for some $t \in T$ and some $m \in M$. As in the proof of Lemma 5.4 this implies that every element of A can be written in the form (t+m)+c for some $t \in T$, $m \in M$, $c \in M_{r-1}$. Since $c \in M_{r-1}$ which is contained in the centre of A

$$(t+m)+c = t+(m+c) = t+d$$

where $d = m+c \in M$. The uniqueness of this representation follows by induction on r just as in the proof of Lemma 5.4.

Before stating the next lemma we introduce a left normed notation for repeated summation. As before we let $a+b := p(a,0,b)$ and we let

$$a_1+a_2+\dots+a_n = (\dots((a_1+a_2)+a_3)+\dots)+a_n.$$

LEMMA 7.2. *If* A *is a relatively free nilpotent algebra then the elements of* A *can all be written in the form* $c_1+c_2+\dots+c_m$ *where* $c_1,\dots,c_m$ *are commutators.*

Proof. The proof is by induction on the class of A. If A is abelian then every element of A can be written in the form

$$r_1(x_1)+r_2(x_2)+\ldots+r_m(x_m)$$

where $r_1, r_2, \ldots, r_m$ are unary term functions. This representation is of the required form. So suppose that A has class c (c>1) and that every element in the relatively free algebra $A/\gamma_c(A)$ can be written as a sum of commutators. Then by Lemma 7.1 every element of A can be written in the form $c_1+c_2+\ldots+c_m+d$ where $c_1,\ldots,c_m$ are commutators and where $d \in \gamma_c(A)$.

Now suppose that d lies in the subalgebra generated by the free generators x_1, $x_2,\ldots,x_n$ of A and consider the element

$$w := \Sigma\ (-1)^{|S|} d\delta_S$$

where the sum is taken over all subsets S of $\{1,2,\ldots,n\}$. All the elements $d\delta_S$ where $S \neq \emptyset$ lie in a subalgebra of A generated by a proper subset of $\{x_1,x_2,\ldots,x_n\}$ and by induction these elements can all be written as sums of commutators. If $S = \emptyset$ then $d\delta_S = d$ and so d-w can be written as a sum of commutators. (Note that the order and bracketing of this sum is irrelevant since all the summands are central.) It is easy to see that w is a commutator involving $x_1,x_2,\ldots,x_n$; in fact $w = d\delta_{\{1,2,\ldots,n\}}{}^*$. So $d = (d-w)+w$ is a sum of commutators, $d_1+d_2+\ldots+d_k$ say.

So every element of A can be written in the form

$$(c_1+\ldots+c_m)+(d_1+\ldots+d_k)$$

where $c_1,\ldots,c_m$ are commutators and where $d_1,\ldots d_k$ are commutators in the centre of A. But since $d_1,\ldots,d_k$ are central this sum equals

$$c_1+\ldots+c_m+d_1+\ldots+d_k$$

and this completes the proof of Lemma 7.2.

If A is an algebra in $\mathcal{U}$ and $a \in A$ then we define $\rho_a : A \to A$ by $x\rho_a = x+a$.

LEMMA 7.3. *If* A *is a finite nilpotent algebra and if* $a \in A$ *then* ρ_a *is a permutation of* A, *and the order of* ρ_a *divides the order of* A.

Proof. The proof is by induction on the class of A. The result is trivial if A is abelian, since then A is an abelian group under +. First we show that ρ_a is one-one. Suppose that $b+a = c+a$ for some $b,c \in A$. Then by induction, $b = c \bmod \zeta(A)$ and so by Lemma 5.4, $c = b+d$ for some $d \in \zeta(A)$. But then

$$b+a = c+a = (b+d)+a = (b+a)+d$$

(since d is central), and by Lemma 5.4 again this implies that $d = 0$, and hence that $b = c$. So ρ_a is one-one, and since A is finite this implies that ρ_a is a permutation of A. Now let $|A/\zeta(A)| = m$ and let $|\zeta(A)| = n$. Then $|A| = mn$ by Lemma 5.4. By induction if $c \in A$ then

$$c\rho_a{}^m = c \bmod \zeta(A)$$

and so

$$c\rho_a{}^m = c+d \quad \text{for some } d \in \zeta(A).$$

Now if $b \in A$ then

$$(b+d)\rho_a = (b+d)+a = (b+a)+d = b\rho_a+d$$

So

$$c\rho_a^{2m} = (c+d)\rho_a^{m} = c+d+d$$

and by repeated application of this argument

$$c\rho_a^{mn} = c + nd = c.$$

This proves that the order of ρ_a divides the order of A.

If A is a finite nilpotent algebra we let R(A) be the subgroup of the symmetric group on A generated by $\{\rho_a : a \in A\}$.

LEMMA 7.4. *If* A *is a finite nilpotent algebra then* R(A) *is a solvable group, and if* A *is of prime power order then* R(A) *is nilpotent.*

Proof. The proof is by induction on the class of A. If A is abelian then R(A) is isomorphic to A as an abelian group. So let A have class greater than 1, and let T be a transversal for the centre of A. Then by Lemma 5.4 every element of A can be written uniquely in the form t+c, $t \in T$, $c \in \zeta(A)$. As we saw in the proof of Lemma 7.3, if $a \in A$ then $(t+c)\rho_a = t\rho_a + c$ and it follows that if ρ is any element in R(A) then $(t+c)\rho = t\rho + c$. So there is a natural projection from R(A) to $R(A/\zeta(A))$ which maps ρ_a to $\rho_{(a+\zeta(A))}$. The kernel of this map is the set of elements in R(A) which map each element **t** of the transversal T to an element of the form t+c where $c \in \zeta(A)$. Clearly these elements all commute with each other and have orders dividing the order of $\zeta(A)$. So the kernel of the projection from R(A) to $R(A/\zeta(A))$ is an abelian subgroup of R(A) whose exponent divides the order of $\zeta(A)$. By induction $R(A/\zeta(A))$ is solvable and so R(A) is solvable. If A has prime power order then this argument also shows that R(A) has prime power order, and so R(A) is nilpotent.

This lemma points to a fundamental difference between nilpotent algebras of prime power order and nilpotent algebras which do not have prime power order. In Section 8 we give an example of a loop of order 12 which is nilpotent of class 2 but for which R(A) is not nilpotent.

THEOREM 7.5. *If* A *is a finite nilpotent algebra in* $\mathfrak{U}$ *and if* A *has prime power order then* A *has a finite basis for its laws. In addition there is an integer* M *such that if* w *is a commutator involving more than* M *variables then* w = 0 *is a law in* A.

Proof. The proof is by induction on the order of $A^{(1)}$. If $A^{(1)}$ has order 1 then A is abelian and the result is immediate since the variety generated by A is definitionally equivalent to a variety of modules generated by a finite module.

So suppose that A has order p^k (p a prime) and class c (c > 1). Let C be a minimal normal subalgebra contained in $\gamma_c(A)$. Then C is an elementary abelian p-group and by induction $A/C{\times}C$ is finitely based. In addition there is an integer K such that if w is a commutator involving more than K variables then $w=0$ is a law in $A/C{\times}C$. Let $w_1=0$, $w_2=0$, $\ldots$, $w_m=0$ be a basis for the laws of $A/C{\times}C$, where $w_1,w_2,\ldots,w_m$ are commutators. If $1 \leqslant i \leqslant m$ then any value of w_i in A must lie in C, and so must be central in A and of order p. The one variable laws of A follow from a finite set of one variable laws (since the free algebra of rank 1 in Var(A) is finite), and these laws imply that one generator algebras are finite. So, by Lemma 5.2, there is a finite set of laws which (together with the one variable laws) implies that values of $w_1,w_2,\ldots,w_m$ are central and of order p. There is no loss in generality in assuming that these are all laws in $\mathcal{U}$. So the $\mathcal{U}$-free algebra F with basis $x_1,x_2,\ldots$ is nilpotent of class c or c+1 and $w_1,w_2,\ldots,w_m$ all lie in the centre of F and all have order p. Now let $w \in F$ and suppose that $w=0$ is a law in $A/C{\times}C$. Then w is contained in the fully invariant normal subalgebra generated by $w_1,w_2,\ldots,w_m$. Since these generators all lie in the centre of F (which is a fully invariant subalgebra of F) and since it follows from Lemma 4 that any central subalgebra is normal this implies that $w = \Sigma\, r_j(v_j)$ where (for each j) r_j is a unary term function and v_j is of the form $w_i(a_1,a_2,\ldots,a_n)$ for some $a_1,a_2,\ldots,a_n \in F$. By Lemma 7.2, the elements $a_1,a_2,\ldots,a_n$ can all be written as sums of commutators. We will prove later that there is a finite set of laws of A which imply the following two technical results.

(1) If $u=0$, $v=0$ *are laws of* $A/C{\times}C$ *then* $u(a_1+v,a_2,\ldots,a_n) = u(a_1,a_2,\ldots,a_n)$ *for all* $a_1,a_2,\ldots,a_n \in F$.

(2) There is an integer N *such that if* $1 \leqslant i \leqslant m$ *then any image of* w_i *under an endomorphism of* F *can be written as a sum of elements of the form* $\pm\, w_i(a_1,\ldots,a_n)$ *where* $a_1,\ldots,a_n$ *are sums of at most* N *commutators.*

We assume that the finite set of laws which imply (1) and (2) is contained in the laws of $\mathcal{U}$. Let P be the maximum number of variables involved in any of the commutators $w_1,w_2,\ldots,w_m$ and let $M = PNK$. We show that if w is any commutator involving more than M variables then $w=0$. (This means that $w=0$ is a consequence of the finite set of laws of A which we have added to the laws of $\mathcal{U}$.) So let w be a commutator involving more than M variables. Then $w=0$ is a law in $A/C{\times}C$ (since $M \geqslant K$) and so by the remarks above w can be written as a sum of terms of the form $r(w_i(a_1,a_2,\ldots,a_n))$ where r is a unary term function and where $a_1,a_2,\ldots,a_n$ are sums of commutators. By (1) we may assume that no commutator in any of these sums involves more than K variables, and by (2) we can assume that these sums are all sums of at most N commutators. Since $n \leqslant P$ this means that w is a sum of terms each of which lies in an M generator subalgebra of F. Let

$$w = u_1+u_2+\ldots+u_r$$

where $u_1,u_2,\ldots,u_r$ are all central and each is contained in a subalgebra of F generated by at most M variables. Let w involve the variables x_i for $i \in S$. By hypothesis $|S| > M$, and so

$$w = w\delta_S{}^* = u_1\delta_S{}^* + u_2\delta_S{}^* + \ldots + u_r\delta_S{}^* = 0,$$

since $u\delta_S{}^* = 0$ whenever u is contained in a subalgebra which does not contain x_i for all $i \in S$. So if w is a commutator which involves more than M variables then $w=0$. By Higman's Lemma, the laws of A are equivalent to a set of laws of the form $w=0$, where w is a commutator. So the laws of A are equivalent to a set of M variable laws together with the finite set of laws which we have already added to the laws of $\mathcal{U}$. Hence the laws of A are finitely based, and, as shown above, if w is a commutator involving more than M variables then $w=0$ is a law in A.

We now prove (1). Let $u=0$, $v=0$ be laws of $A/C\times C$. Then v is contained in the centre of F and so

$$u(a_1+v, a_2, \ldots, a_n) = u(a_1, a_2, \ldots, a_n) + u(v, 0, \ldots, 0).$$

So it is sufficient to prove that there is a finite set of laws of A which imply that $u(v,0,\ldots,0)=0$. Any value of v in A lies in C, and $u=0$ is a law in C, and so $u(v,0,\ldots,0) = 0$ is a law in A. Since $u=0$, $v=0$ are laws in $A/C\times C$ both u and v can be written as sums of terms of the form $r(w)$ where r is a unary term function and w is the image of w_i for some i under some endomorphism of F. It follows that the law $u(v,0,\ldots,0) = 0$ is a consequence of the laws

$$w_i(0,\ldots,0,r(w_j),0,\ldots,0) = 0$$

where r is a unary term function and $1 \leqslant i,j \leqslant m$. (Note that these laws are all trivial except when w_i involves only one variable.) Now there are only finitely many unary term functions in Var(A), and so this proves (1).

Finally we prove (2). This is the key to the proof of Theorem 7.5 and it is at this point that we use the fact that that A is of prime power order. By Lemma 7.4, $R(A)$ is a finite p-group and this implies that the radical of the group ring $Z_pR(A)$ is nilpotent. For each $\rho \in R(A)$, $\rho-1$ is in the radical and so there is an integer N such that if $\rho_1, \rho_2, \ldots, \rho_N \in R(A)$ then $(\rho_1-1)(\rho_2-1)\ldots(\rho_N-1) = 0$. This product is a sum of terms of the form

$$\pm\ \rho_i\rho_j\ldots\rho_k$$

where the sum is taken over all subsets $\{i,j,\ldots,k\}$ of $\{1,2,\ldots,N\}$ with $i < j < \ldots < k$. If $a_1, a_2, \ldots, a_N$ are elements of A and we let $\rho_i = \rho_{a_i}$ for $i=1,2,\ldots,N$ then $\rho_i\rho_j\ldots\rho_k$ is the element of $R(A)$ which takes a to $a+a_i+a_j+\ldots+a_k$. In particular it takes 0 to $a_i+a_j+\ldots+a_k$. If $S = \{i,j,\ldots,k\}$ is a subset of $\{1,2,\ldots,N\}$ with $i < j < \ldots < k$ let $a_S = a_i+a_j+\ldots+a_k$ and let $\rho_S = \rho_i\rho_j\ldots\rho_k$. If $\rho \in R(A)$ then ρ can equal ρ_S for many different subsets S. But the fact that $(\rho_1-1)(\rho_2-1)\ldots(\rho_N-1) = 0$ implies that the number of even subsets S such that $\rho = \rho_S$ is equal (modulo p) to the number of odd subsets S such that $\rho = \rho_S$. This implies that if $a \in A$ then the number of even subsets S such that $a = a_S$ is equal modulo p to the number of odd subsets S such that $a = a_S$. So if w is an element of order p in the centre of F then

$$\Sigma\ (-1)^{|S|}w(a_S, b_2, \ldots, b_n) = 0$$

where the sum is taken over all subsets S of $\{1,2,\ldots,N\}$, and where $b_2,\ldots,b_n$ are any elements of A. This means that A satisfies the finite set of laws of the form

$$\Sigma\ (-1)^{|S|} w_i(x_1,\ldots,x_{j-1},y_S,x_{j+1},\ldots,x_n) = 0.$$

One term in this sum has $y_1+y_2+\ldots+y_N$ in the j-th place, and this law enables us to express this term as a sum of terms in which the j-th entry is a sum of fewer than N terms. This proves (2).

This completes the proof of Theorem 7.5.

THEOREM 7.6. *If* A *is a finite nilpotent algebra in* $\mathcal{U}$, *and if* A *is a direct product of algebras of prime power order, then* A *has a finite basis for its laws. In addition there is a finite integer* M *such that if* w *is a commutator involving more than* M *variables then* w=0 *is a law in* A.

Proof. Let $A = A_1 \times A_2 \times \ldots \times A_k$, where $A_1, A_2, \ldots, A_k$ have prime power order. Then, by Theorem 7.5, $A_1, A_2, \ldots, A_k$ have finite bases for their laws, and there is an integer M such that if w is a commutator involving more than M variables then w=0 is a law in A_i for i=1,2,...,k. It follows that w=0 is also a law in A. We prove that the laws of A are finitely based by induction on the order of $A^{(1)}$ as in the proof of Theorem 7.5. We let C be a minimal normal subalgebra of A contained in the centre of A. We let $w_1, w_2, \ldots, w_m$ be a set of commutators such that $w_1=0, w_2=0, \ldots, w_m=0$ is a basis for the laws of A/C×C. The proof uses (1) and (2) just as in the proof of Theorem 7.5, and (1) is proved as before. However (2) (with N=M) follows immediately from the fact that

$$\Sigma\ (-1)^{|S|} w_i(x_1,\ldots,x_{j-1},y_S,x_{j+1},\ldots,x_n)$$

(with the sum taken over all subsets S of {1,2,...,M+1}) is a commutator involving more than M variables.

8. EXAMPLES.

EXAMPLE 1. *There is a non-finitely based variety of loops which are nilpotent of class 3, which has the property that finitely generated loops in the variety have order* 2^k *for some* k.

We first let $\mathcal{L}$ be the variety of non-distributive rings determined by the laws

$(x+y)+z = x+(y+z)$,

$x+y = y+x$,

$x+0 = x$,

$x+x = 0$,

$(xy)z = 0$,

$x(yz) = 0$,

$x.0 = 0$,

$0.x = 0$,

$x(y + z(t+u)) = x(y + zt + zu)$,

$$x(y + (z+t)u) = x(y + zu + tu),$$
$$(x + y(z+t))u = (x + yz + yt)u,$$
$$(x + (y+z)t)u = (x + yt + zt)u.$$

It is easy to see that if $A \in \mathcal{C}$ and if $a,b,c \in A$ then

$$(a+b)c - ac - bc \quad \text{and} \quad a(b+c) - ab - ac$$

lie in the centre of A, and that $A/\zeta(A)$ is an associative distributive ring satisfying the law $xyz = 0$. In our notation this implies that $A/\zeta(A)$ is nilpotent of class 2, and hence that A is nilpotent of class 3. Rings in $\mathcal{C}$ are elementary abelian two-groups under addition, and it is easy to see that $\mathcal{C}$ is locally finite. We show that the subvariety of $\mathcal{C}$ determined by the laws $(x_1{}^2 + x_2{}^2 + \ldots + x_n{}^2)^2 = 0$ for $n=1,2,\ldots$ is not finitely based by constructing (for any N) a ring $A \in \mathcal{C}$ which satisfies these laws for $n \leq N$ but does not satisfy these laws for all n.

A is constructed as follows. A is generated by $a_1, a_2, \ldots$. As an elementary abelian 2-group under addition A has a basis consisting of the generators $a_1, a_2, \ldots$, the products a_ia_j for all positive i,j, and one extra basis element c in the centre of A. We also let $d = a_1{}^2 + a_2{}^2 + \ldots + a_n{}^2$ where n is some integer to be determined later. We define the product of two elements in the span of $a_1, a_2, \ldots$ by linearity. We denote general elements in the span of $a_1, a_2, \ldots$ by a,a', general elements in the span of the products a_ia_j by b,b', and general elements in the span of c by e,e'. Thus every element of A can be written uniquely in the form a+b+e. Finally we define the product of two elements of A by the rule

$$(a+b+e).(a'+b'+e') = aa' \quad \text{unless } b = b' = d,$$
$$(a+d+e).(a'+d+e') = aa' + c.$$

(Remember that the product aa' is defined by linearity.) It is straightforward to verify that A is a ring in $\mathcal{C}$. In fact A/<c> is an associative distributive ring satisfying the law $xyz = 0$. If we choose n so that d cannot be expressed as a sum of N squares then A satisfies the law $(x_1{}^2+x_2{}^2+\ldots+x_N{}^2)^2 = 0$, but A does not satisfy the law $(x_1{}^2+x_2{}^2+\ldots+x_n{}^2)^2 = 0$. This proves that the subvariety of $\mathcal{C}$ determined by all these laws is not finitely based

We define derived binary operators $*, /, \backslash$ in $\mathcal{C}$ by

$$x*y := x + y + xy$$
$$x/y := x + y + (x+y+xy+yy)y,$$
$$x\backslash y := x + y + x(x+y+xx+xy).$$

It is straightforward to verify that these operations turn any ring in $\mathcal{C}$ into a loop (with 0 as identity). This loop will also be nilpotent of class 3 as a loop. Since $x*x = xx = x^2$ and since $x*(y^2) = x + y^2$ it follows that $(x_1{}^2+x_2{}^2+\ldots+x_n{}^2)^2$ can be expressed as a word in $x_1, x_2, \ldots, x_n$ using only the loop operation $*$. It follows that the laws $(x_1{}^2+x_2{}^2+\ldots+x_n{}^2)^2 = 0$ determine a non-finitely based subvariety of the variety of loops which are nilpotent of class 3 and satisfy the law $(x*x)*(x*x) = 0$. This law together with the nilpotency condition imply that finitely generated loops in this variety have order 2^k for some k.

EXAMPLE 2. *Let* A *be the loop of order 12 with the following multiplication table.*

	1	a	a^2	a^3	c	ac	a^2c	a^3c	c^2	ac^2	a^2c^2	a^3c^2
1	1	a	a^2	a^3	c	ac	a^2c	a^3c	c^2	ac^2	a^2c^2	a^3c^2
a	a	a^2	a^3	c	ac	a^2c	a^3c	c^2	ac^2	a^2c^2	a^3c^2	1
a^2	a^2	a^3	1	a	a^2c	a^3c	c	ac	a^2c^2	a^3c^2	c^2	ac^2
a^3	a^3	c	a	a^2	a^3c	c^2	ac	a^2c	a^3c^2	1	ac^2	a^2c^2
c	c	ac	a^2c	a^3c	c^2	ac^2	a^2c^2	a^3c^2	1	a	a^2	a^3
ac	ac	a^2c	a^3c	c^2	ac^2	a^2c^2	a^3c^2	1	a	a^2	a^3	c
a^2c	a^2c	a^3c	c	ac	a^2c^2	a^3c^2	c^2	ac^2	a^2	a^3	1	a
a^3c	a^3c	c^2	ac	a^2c	a^3c^2	1	ac^2	a^2c^2	a^3	c	a	a^2
c^2	c^2	ac^2	a^2c^2	a^3c^2	1	a	a^2	a^3	c	ac	a^2c	a^3c
ac^2	ac^2	a^2c^2	a^3c^2	1	a	a^2	a^3	c	ac	a^2c	a^3c	c^2
a^2c^2	a^2c^2	a^3c^2	c^2	ac^2	a^2	a^3	1	a	a^2c	a^3c	c	ac
a^3c^2	a^3c^2	1	ac^2	a^2c^2	a^3	c	a	a^2	a^3c	c^2	ac	a^2c

Note that A is commutative. The centre of A is $\{1,c,c^2\}$ which is a cyclic group of order 3, and $A/\zeta(A)$ is a cyclic group of order 4. So A is nilpotent of class 2. A is not associative since if we set $(x,y,z) = ((xy)z)/(x(yz))$ then $(a^2,a,a) = c$. Let $w_n := ((\ldots(x_1{}^2x_2{}^2)x_3{}^2)\ldots)x_n{}^2$ and let

$$w := (w_n,x_{n+1},x_{n+2})^{\delta}\{1,2,\ldots,n\}^*.$$

Then w is a commutator involving $x_1,x_2,\ldots,x_{n+2}$ but $w = 1$ is not a law in A, as can be seen by substituting a for x_i for $i=1,2,\ldots,n+2$. So although A is a finite nilpotent loop, there is no integer M such that if w is a commutator involving more than M variables then $w=1$ is a law in A. It follows that Theorem 7.6 cannot be extended to arbitrary finite nilpotent algebras. It is also straightforward to verify that R(A) (as defined in Section 7) is not nilpotent.

REFERENCES

H.P. Gumm (1980), "An easy way to the commutator in modular varieties", Arch. der Math. 34, 220-228.

H.P. Gumm (1982), "Geometrical methods in congruence modular algebras", to appear, Memoirs A.M.S.

R.S. Freese and R.N. McKenzie (1982), "The commutator, an overview".

Graham Higman (1959), "Some remarks on varieties of groups", Quart. J. Math. Oxford (2) 10, 165-178.

A.I. Mal'cev (1954), "On the general theory of algebraic systems", Mat. Sb. (77), 35, 3-20.

J.D.H. Smith (1976), "Mal'cev Varieties", Springer Lecture Notes 554, Berlin.