Algebra Universalis, **34** (1995) 4–23

ALAN DAY'S EARLY WORK: CONGRUENCE IDENTITIES

Ralph Freese

November 20, 1997

In Memory of Alan Day

The death of R. Alan Day on November 26, 1990 was a great loss to the community of lattice theorists and universal algebraists. Alan was a hard working, hard playing man whose enthusiasm for mathematics and life will be greatly missed by all of us.

This paper concentrates on congruence identities, i.e., lattice equations satisfied by the congruence lattices of all the algebras in a variety. Although this area represents only a small part of Alan's mathematical work, this is a subject in which Alan was greatly interested and to which he made profound contributions. This paper surveys the struggles Alan and others of us made to understand this area. It also gives some of the recent results, including some of Alan's, and lists several open problems.

Day's Master's Thesis

In what is without a doubt the most quoted master's thesis in our field, Alan Day gave a Maltsev condition for a variety of algebras to have modular congruence lattices. This result was published in the Canadian Mathematical Bulletin [2]. It is the starting point of almost all work on varieties with modular congruence lattices (modular varieties) including the commutator theory, see [14].

Maltsev showed in [27] that a variety of algebras has permutable congruence lattices if and only if there is a term p in the language of the variety such that

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

Pixley showed that a variety is arithmetic (both permutable and distributive) if and only if there is a term p as above which, in addition, satisfies $p(x, y, x) = x$, [35]. Jónsson [22] showed that a variety has distributive congruences if and only if there is an n and 3–ary terms $d_0, \dots, d_n$ such that

(1) $d_0(x, y, z) = x$ and $d_n(x, y, z) = z$.
(2) $d_i(x, y, x) = x$, for $0 \le i \le n$.
(3) $d_i(x, x, y) = d_{i+1}(x, x, y)$, for all even $i < n$.
(4) $d_i(x, y, y) = d_{i+1}(x, y, y)$, for all odd $i < n$.

This research was partially supported by NSF grant no. DMS–9204481. The author would like to thank the referee for several helpful suggestions.

Day's Maltsev condition has the same flavor.

Theorem 1 (A. Day [2]). *A variety $\mathcal{K}$ is congruence modular, i.e., its members all have modular congruence lattices, if and only if for some n there are 4–ary terms $m_0, \dots, m_n$ such that $\mathcal{K}$ satisfies*

(1) $m_0(x, y, z, u) = x$ *and* $m_n(x, y, z, u) = u$.
(2) $m_i(x, y, y, x) = x$, *for* $0 \le i \le n$.
(3) $m_i(x, x, y, y) = m_{i+1}(x, x, y, y)$, *for all even* $i < n$.
(4) $m_i(x, y, y, z) = m_{i+1}(x, y, y, z)$, *for all odd* $i < n$.

Day's and Jónsson's conditions are now known as *Maltsev conditions.* Maltsev's original condition and Pixley's condition are known as *strong Maltsev conditions.* If C_n, $n \in \omega$, are Maltsev conditions such that C_n implies C_m for $n \ge m$, then the infinite conjunction of the C_n's is a *weak Maltsev condition.* See Taylor [38] for a more rigorous development of these concepts.

Day also obtained some interesting relationships between these concepts. Let us call a variety *n–modular* if Theorem 1 holds for this n. Define n–distributive similarly. Day showed that if a variety is 2–modular, it is permutable. He also showed that if a variety is n–distributive, it is $2n-1$–modular.[1]

At first blush it might appear that Day's result would be a straightforward generalization of Jónsson's. When the result first appeared, J. B. Nation and I were both graduate students at Caltech, and Nation lectured on it at our seminar. He explained that it was not an easy generalization of Jónsson's result. In the next few years this became particularly clear. One would suspect that, in light of Jónsson and Day's theorems, there would be a Maltsev condition corresponding to every lattice equation. Pixley [36] and Wille [39] showed that there is a weak Maltsev condition for each equation, but for several years it was not known if any nontrivial equation outside of distributivity and modularity had a Maltsev condition. We will say more about this problem later.

An important corollary of Alan's development of Theorem 1 is that, if the sublattice generated by

$$\theta = \mathrm{Cg}\,(a, b) \qquad \phi = \mathrm{Cg}\,(\langle a, b\rangle, \langle c, d\rangle) \qquad \psi = \mathrm{Cg}\,(\langle a, c\rangle, \langle b, d\rangle) \tag{1}$$

in $\mathbf{Con}\ \mathbf{F}_{\mathcal{K}}(a, b, c, d)$ is modular, then $\mathcal{K}$ has modular congruences. Clearly $\phi \le \theta \vee \psi$, and so the sublattice generated by ϕ, θ, and ψ is a homomorphic image of the lattice diagrammed in Figure 1.

Corollary 2. *Let θ, ϕ, and ψ be the congruences on $\mathbf{F}_{\mathcal{K}}(a, b, c, d)$ defined in* (1) *above. Then $\mathcal{K}$ is congruence modular if and only if $\theta \vee (\psi \wedge \phi) = \phi$, which is equivalent to*

$$\langle c, d\rangle \in \theta \vee (\psi \wedge \phi)$$

[1] It always seemed odd to me that 2–modularity implies permutability, but 2-distributivity does not. However, if one interchanges 'even' and 'odd' in Jónsson's condition for distributivity above, as is done in [30], the resulting condition still is equivalent to distributivity, and now 2–distributivity does imply permutability; in fact it gives a Pixley term. Under Jónsson's scheme, 2–distributivity is equivalent to having a ternary majority term. These facts show that the least n such that a variety is n–distributive is not a very good invariant.

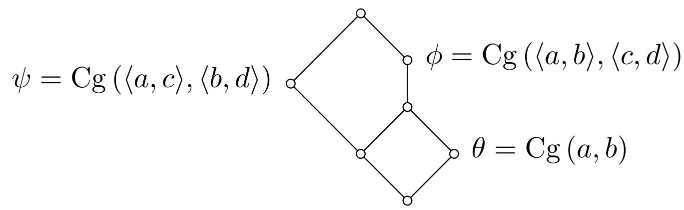


FIGURE 1

Of course, this result has the corollary that if $\mathbf{Con}\,\mathbf{F}_{\mathcal{K}}(4)$ is modular then $\mathcal{K}$ is congruence modular. This is not true if 4 is changed to 3. Indeed, the 3–generated free algebra in the variety of all sets is the 3 element set and its congruence lattice is just $\mathbf{M}_3$ (but of course the variety of all sets is not congruence modular).

It is not hard to see that both ϕ and ψ are the kernels of homomorphisms of $\mathbf{F}_{\mathcal{K}}(4)$ onto $\mathbf{F}_{\mathcal{K}}(2)$. Since the copy of $\mathbf{N}_5$ of Figure 1 lies in the filter above $\phi \wedge \psi$, this $\mathbf{N}_5$ lies in the congruence lattice of a subdirect product of two copies of $\mathbf{F}_{\mathcal{K}}(2)$. Thus we obtain the following corollary.

Corollary 3. *A variety $\mathcal{K}$ is congruence modular if and only if the variety generated by $\mathbf{F}_{\mathcal{K}}(2)$ is.*

The next corollary follows from Corollary 2 by considering the algebra $\mathbf{A} = \mathbf{F}_{\mathcal{K}}(a, b, c, d)/(\psi \wedge \phi)$.

Corollary 4. *A variety $\mathcal{K}$ is not congruence modular if and only if there is an algebra $\mathbf{A} \in \mathcal{K}$ generated by elements a, b, c, and d such that the sublattice of* **Con A** *generated by $\theta = \mathrm{Cg}\,(a, b)$, $\phi = \mathrm{Cg}\,(\langle a, b\rangle, \langle c, d\rangle)$, and $\psi = \mathrm{Cg}\,(\langle a, c\rangle, \langle b, d\rangle)$ is isomorphic to $\mathbf{N}_5$ and $\psi \wedge \phi = 0$.*

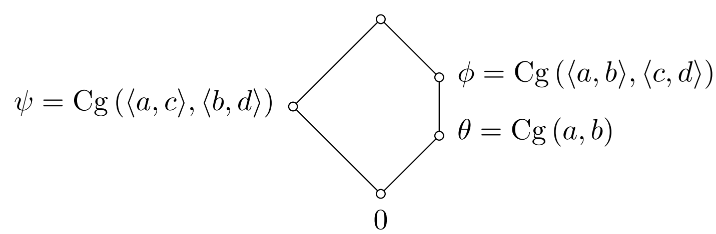


FIGURE 2

Congruence Identities

Nation, inspired by Day's work, proved the following remarkable result in his thesis. McKenzie described this as "a dramatic development in an area which seemed thoroughly cultivated and not very promising of new results," [29].

Theorem 5 (Nation [33])**.** *There is a lattice equation not implying modularity, such that whenever all of the congruence lattices of a variety $\mathcal{K}$ satisfy this equation, $\mathcal{K}$ is congruence modular.*

Nation proved his result for a certain class of lattice equations defined syntactically. His proof was also syntactic: in proving that congruence–ϵ implies congruence modularity, he used the weak Maltsev condition for ϵ to derive Day's Maltsev condition. (A variety is congruence–ϵ if its congruence lattices satisfy ϵ.) Nation's result prompted McKenzie to conjecture in [29]

- *If the congruences of a variety satisfy a nontrivial lattice equation, the variety must be congruence modular.*

The fact that this had been verified for unary algebras by Nation in [32] and for semigroups by Nation and myself in [15] was part of McKenzie's motivation for the conjecture.

Alan was so intrigued by Nation's result that he invited J. B. to Lakehead to discuss it. There they started a lifelong friendship by going to the NorShore Bar in Lakehead and drinking it out of five brands of beer. On that trip Nation explained his techniques in detail to Alan.

A *congruence variety* is a variety of lattices $\mathcal{V}$ which is generated by the congruence lattices of some variety of algebras $\mathcal{K}$. We let $\mathbf{Con}\ \mathcal{K}$ denote the congruence variety associated with $\mathcal{K}$. McKenzie's conjecture states that the only nonmodular congruence variety is the variety of all lattices. For several years Alan and others worked intensely on this conjecture and certain related problems:

- *Is there an effective method to decide which lattice equations imply congruence modularity?*
- *Is there a unique smallest nonmodular congruence variety?*
- *Are there any congruence varieties other than the two trivial varieties, distributive lattices, and the congruence variety associated with the variety of groups?*
- *Do congruence varieties form a sublattice of the lattice of all lattice varieties?*

In Day's first paper on congruence varieties [3] he showed that the equation

$$(x \vee (y \wedge z)) \wedge (z \vee (x \wedge y)) = (z \wedge (x \vee (y \wedge z))) \vee (x \wedge (z \vee (x \wedge y))) \tag{2}$$

implies congruence modularity. Lattices satisfying this equation are called p–modular. This equation is weaker than modularity, so, for congruence varieties, the two are equivalent. E. Gedeonová had shown in [17] that (2) has a Maltsev condition associated with it, seemingly answering the question on the existence of Maltsev conditions for lattice equations raised above. But Alan's result showed that p–modularity is really the same as modularity, and thus *his* Maltsev condition could be used to define the class of varieties with p–modular congruences.

In [4] and [6],[2] Day extended Nation's Theorem by giving more examples of lattice equations which imply congruence modularity. His proofs, like Nation's,

[2] This paper, as well as some of Alan's other papers and some papers of other authors, thanks Croy Pitzer. The story behind Croy Pitzer was related to me by Bill Lampe. At the International Congress at Vancouver in 1974, he and Alan and Al Stralka were having a picnic lunch, where Stralka told them that while in Pennsylvania he listened to a disc jockey named Alan Day. One day this disc jockey admitted that his name was not Alan Day but Croy Pitzer. This is how Alan got the nickname Croy Pitzer.

involved a subtle manipulation of terms, and, when asked by a colleague about how he found one particularly hard proof, he replied "Simple. I came to work each day, wrote down the equations, and tried to manipulate them. After two years of doing this every day, I found the proof."

The second of these papers was particularly nice. In order to state this result we need certain concepts from lattice theory. If $a \succ b$ (a covers b) in a lattice $\mathbf{L}$, then, by Dilworth's characterization of lattice congruences [10], there is a unique maximal congruence $\psi(a,b) \in \mathrm{Con}\ \mathbf{L}$ not containing the pair $\langle a,b\rangle$. Naturally, $\mathbf{L}/\psi(a,b)$ is subdirectly irreducible. In the case when $\mathbf{L}$ is a free lattice, $\mathbf{L}/\psi(a,b)$ is finite and is called a *splitting lattice*. Every lattice variety either satisfies the equation $a \approx b$ identically or contains $\mathbf{L}/\psi(a,b)$. The equation $a \approx b$ is known as a *splitting equation*. These concepts were invented by McKenzie in [28] and are extremely important in lattice theory. One of Alan's most important results is the following theorem, which shows that there are many splitting equations.

Theorem 6 (A. Day [5]). *Finitely generated free lattices are weakly atomic. Consequently, the variety generated by all splitting lattices is the variety of all lattices.*

The equivalence of the two statements was proved by McKenzie in [28]. Day proved this result using his doubling construction. In this construction one starts with an interval $\mathbf{I}$ in a lattice $\mathbf{L}$ and replaces $\mathbf{I}$ with $\mathbf{I} \times \mathbf{2}$ and uses the (more or less) obvious order, see [7].

In [6], Alan showed that if one took a finite distributive lattice $\mathbf{D}$, doubled a single element p, then, if the resulting lattice (which we denote by $\mathbf{D}[p]$) is subdirectly irreducible, it is a splitting lattice. For example, if we take the lattice $\mathbf{3} \times \mathbf{3}$ and double the very middle element we get the lattice diagrammed in Figure 3.

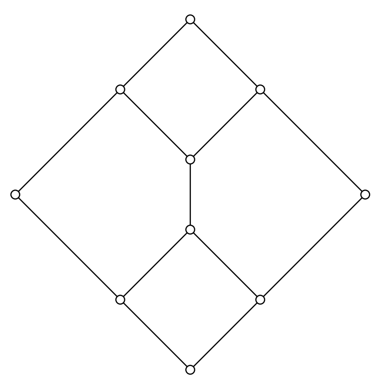


FIGURE 3

The splitting equation for this lattice is the equation for p–modularity given in (2). Alan proved that any splitting equation obtained from a distributive lattice in this way implied congruence modularity. What made this result so attractive is that it had all other known results as a consequence. This included Nation's original theorem, the theorems of Jónsson in [23], the work of Mederly [31], as well as all of Alan's own results. Nation and I used Alan's result to show that all 3–3 lattice equations (the depth of both sides is at most 3) imply congruence modularity [16].

This theorem of Alan's began to give some semblance of order to the results in this area, as the following semantic formulation of it shows.

Theorem 7. *Any nonmodular congruence variety must contain the variety* $\mathcal{D}_1$ *generated by the lattices* $\mathbf{D}[p]$ *where* $\mathbf{D}$ *is a distributive lattice and* $p \in D$.

Another reason why this result is attractive is that $\mathcal{D}_1$ has a very nice characterization. In [25], Jónsson and Rival showed that there are exactly 16 covers of the variety generated by $\mathbf{N}_5$. (These varieties had been discovered by McKenzie in [28].) In the notation of [25], these varieties are $\boldsymbol{V}(\mathbf{N}_5) \vee \boldsymbol{V}(\mathbf{M}_3)$ and $\boldsymbol{V}(\mathbf{L}_1), \dots, \boldsymbol{V}(\mathbf{L}_{15})$. $\mathbf{L}_{15}$ is the lattice diagrammed in Figure 3. $\mathbf{L}_{14}$ is the lattice diagrammed in Figure 4 and $\mathbf{L}_{13}$ is the dual of $\mathbf{L}_{14}$. In proving their result on covers of $\boldsymbol{V}(\mathbf{N}_5)$, Jónsson and Rival prove the following theorem.

Theorem 8. *Every variety is either contained in* $\mathcal{D}_1$ *or contains* $\mathbf{M}_3$*, or one of* $\mathbf{L}_1, \dots, \mathbf{L}_{12}$.

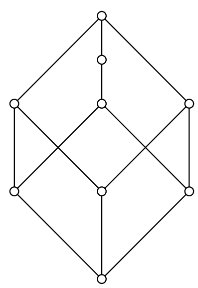


FIGURE 4

$\mathbf{L}_{14}$

A more semantic approach. My own work in this area is more model theoretical in nature. By Theorem 5, if the congruence variety associated with a variety $\mathcal{K}$ contains $\mathbf{N}_5$, it must contain larger subdirectly irreducible lattices. For a semantic proof, suppose $\mathbf{A} \in \mathcal{K}$ has a sublattice as diagrammed in Figure 5.

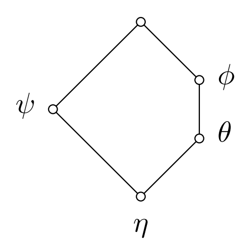


FIGURE 5

The congruence θ is (the universe of) a subalgebra of $\mathbf{A} \times \mathbf{A}$. We denote this subalgebra by $\mathbf{A}(\theta)$. For an arbitrary congruence $\rho \in \mathrm{Con}\ \mathbf{A}$ and for $i = 0, 1$, let ρ_i

be the congruence on $\mathbf{A}(\theta)$ which identifies $\langle x_0, x_1\rangle$ with $\langle y_0, y_1\rangle$ provided $x_i \ \rho \ y_i$. By calculating with elements of $\mathbf{A}$, it is easy to see that if $\rho \geq \theta$ then $\rho_0 = \rho_1$ and

$$\eta_0 \vee \eta_1 = \theta_0 = \theta_1 \tag{3}$$

Indeed, if $\langle x_0, x_1\rangle \ \theta_0 \ \langle y_0, y_1\rangle$, then all four elements are in the same θ–class and hence $\langle x_0, x_1\rangle \ \eta_0 \ \langle x_0, y_1\rangle \ \eta_1 \ \langle y_0, y_1\rangle$. A similar agument shows that $\eta_0 \vee (\psi_0 \wedge \psi_1) = \psi_0$. The first projection defines a homomorphism of $\mathbf{A}(\theta)$ onto $\mathbf{A}$. By the usual correspondence theorem, Theorem 4.12 of [30], the filter of the congruence lattice of $\mathbf{A}(\theta)$ above η_0 is isomorphic to **Con A**. In particular, $\phi_0 \wedge \psi_0 = \eta_0$, and from this it follows that $\psi_0 \wedge \eta_1 = \psi_0 \wedge \phi_1 \wedge \eta_1 = \psi_0 \wedge \phi_0 \wedge \eta_1 \leq \eta_0$. Similarly, $\psi_1 \wedge \eta_0 \leq \eta_1$. Using these facts it is straightforward to see that the sublattice generated by θ_0, ϕ_0, ψ_0, and ψ_1 is the lattice diagrammed in Figure 6. Thus we have shown that every nonmodular congruence variety must contain $\mathbf{L}_{14}$.

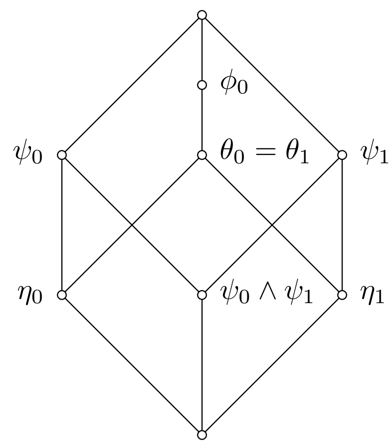


FIGURE 6

Using similar techniques, Jónsson and I proved the following theorem, [13].

Theorem 9. *If a variety $\mathcal{K}$ is congruence modular, then its congruence lattices satisfy the Arguesian equation.*

The Arguesian equation is an equation strictly stronger than the modular law which reflects Desargues Law of geometry. The only projective geometries that fail it are planes and any plane that can be embedded into a high dimensional space satisfies this law. The proof of Theorem 9 uses the construction above to effectively embed the congruence lattice into a larger lattice so that the proof from projective geometry can be imitated.

It had been known that if $\mathbf{A}$ has permutable congruences, then **Con A** is Arguesian [21]. Thus the classical algebraic systems (groups, rings, modules) have Arguesian congruence lattices. But not all congruence modular varieties have permutable congruence, eg., lattices.

Using the above semantic approach, it is not hard to classify the minimal modular, nondistributive congruence varieties, [12].

Theorem 10. *The minimal modular, nondistributive congruence varieties are the congruence varieties associated with the varieties $\mathcal{K}_p$ of all vector spaces over the prime field of characteristic p, where p is a prime or* 0.

This theorem has a corollary that the set of congruence varieties is not a sublattice of the lattice of all lattice varieties (since $\mathbf{M}_3 \in \mathcal{K}_p \cap \mathcal{K}_{p'}$ but the smallest congruence variety contained in $\mathcal{K}_p \cap \mathcal{K}_{p'}$ is $\mathcal{D}$), answering one of the questions raised by McKenzie in [29]. On the other hand, the join of two congruence varieties is a congruence variety.

Polin's Variety

Work on McKenzie's conjecture and on minimal nonmodular congruence varieties continued for the next few years until, in 1976, Alan visited Prague briefly. There he met with Pavel Goralčík who had just seen Polin in Russia. Polin had just found a variety $\mathcal{P}$ whose congruences were nonmodular but still satisfy a nontrivial identity, refuting McKenzie's conjecture. Alan scribbled down what Goralčík said on a sheet of paper. When he returned to Canada, he wrote this up into a set of notes which he distributived to the people most interested in congruence varieties. Since he had only an outline of Polin's proof, he had to reconstruct most of it himself. Consequently, his proof was different from Polin's in [37]. Alan's proof developed the arithmetic of $\mathcal{P}$ much more thoroughly than Polin's did.

When I received his notes, I studied them intensely. Alan and I then developed the arithmetic of the congruence lattices of the members of $\mathcal{P}$, found the subdirectly irreducible algebras of $\mathcal{P}$, and the free algebras, $\mathbf{F}_{\mathcal{P}}(n)$. Armed with this, we hoped to solve the problem of finding the minimal nonmodular congruence varieties. In particular we wanted to know if the congruence variety associated with Polin's variety was the unique minimal nonmodular congruence variety. Of course by Theorem 7, if $\mathbf{Con}\ \mathcal{P} \subseteq \mathcal{D}_1$, then they would be equal and this would be the unique minimal nonmodular congruence variety. By Theorem 8, this would be true if none of the lattices $\mathbf{L}_1, \ldots, \mathbf{L}_{12}$, and $\mathbf{M}_3$ is contained in $\boldsymbol{V}(\mathbf{Con}\ \mathcal{P})$.

Now we had already been able to show that $\mathbf{Con}\ \mathcal{P}$ is semidistributive, and thus $\mathbf{M}_3$ and $\mathbf{L}_1, \ldots, \mathbf{L}_5$ are not in $\boldsymbol{V}(\mathbf{Con}\ \mathcal{P})$, since these lattices are not semidistributive. The remaining lattices are splitting lattices, and so each has a splitting equation. If we could prove that each of these 7 equations holds in $\mathbf{Con}\ \mathcal{P}$, then we would have the result we wanted. Six of the 7 equation held, but the seventh failed. Thus $\mathbf{Con}\ \mathcal{P}$ just barely missed being inside $\mathcal{D}_1$.

Despite this setback, we pressed on in our study of Polin's variety, and eventually were able to prove the theorem we wanted.

Theorem 11 (A. Day and R. Freese [9]). *The congruence variety generated by* $\mathbf{Con}\ \mathcal{P}$ *is the unique minimal nonmodular congruence variety. In other words, if* $\mathcal{K}$ *is a variety with nonmodular congruence lattices, then the congruence variety associated with* $\mathcal{K}$ *contains* $\mathbf{Con}\ \mathcal{P}$.

This theorem has many important consequences, including a recursive procedure for deciding if a lattice equation implies congruence modularity. Before giving some of these consequences, we will discuss some of the ideas of the proof.

First we describe the members of $\mathcal{P}$. Let $\mathbf{A}$ be a Boolean algebra. For each $a \in A$, let $\mathbf{S}(a)$ be a Boolean algebra and, for each pair $a \geq b$, let ξ_b^a be a homomorphism from $\mathbf{S}(a)$ into $\mathbf{S}(b)$ satisfying

(1) ξ_a^a is the identity map.
(2) If $a \geq b \geq c$, then $\xi_c^a = \xi_c^b \circ \xi_b^a$.

Let

$$P = \bigcup_{a \in A} \{a\} \times \mathrm{S}(a)$$

and define a binary, two unary, and two constant operations on P by

$$\begin{aligned} \langle a, s\rangle \cdot \langle b, t\rangle &= \langle a \cdot b,\, \xi_{ab}^a(s) \cdot \xi_{ab}^b(t)\rangle \\ \langle a, s\rangle' &= \langle a, s'\rangle && \text{(internal complement)} \\ \langle a, s\rangle^+ &= \langle a', 1\rangle && \text{(external complement)} \\ 1 &= \langle 1, 1\rangle \\ 0 &= \langle 0, 0\rangle \end{aligned}$$

where $x \cdot y$ is the meet in both coordinates. On the resulting algebra $\mathbf{P}$, the binary operation $\cdot$ makes P into a semilattice with 0 and 1. We call the Boolean algebra $\mathbf{A}$ associated with $\mathbf{P}$ the *external Boolean algebra*.

The proof of Theorem 11 involves several steps:

(1) Describe the congruence lattices of members of $\mathcal{P}$ and find the subdirectly irreducible members of $\mathcal{P}$.
(2) Find the n–generated free algebra $\mathbf{F}_{\mathcal{P}}(n)$ in $\mathcal{P}$ and its congruence lattice, $\mathbf{L}_n = \mathbf{Con}\ \mathbf{F}_{\mathcal{P}}(n)$. We show that $\mathbf{L}_n$ is subdirectly irreducible and is in fact a splitting lattice.
(3) Describe the splitting equation, ζ_n, of $\mathbf{L}_n$.

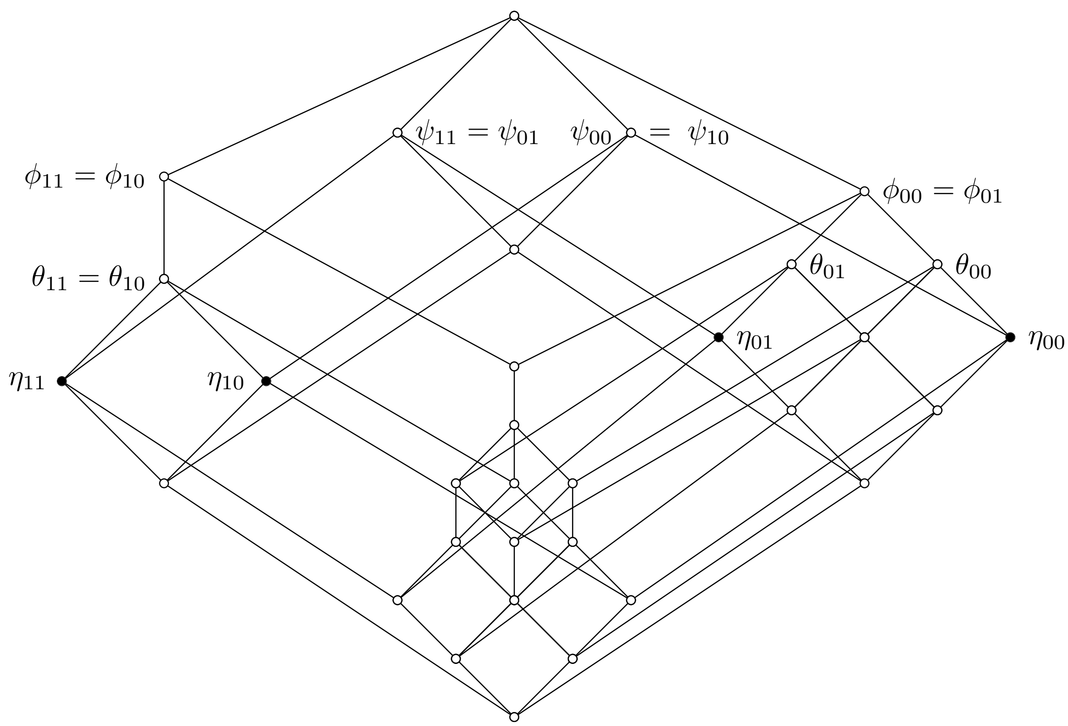
Now if a variety $\mathcal{K}$ is not congruence modular, then, by Corollary 4, it has an algebra $\mathbf{A}$ whose congruence lattice contains the sublattice isomorphic to $\mathbf{N}_5$ represented in Figure 2.

(4) Using a modification of the semantic technique outlined above, construct a subdirect power $\mathbf{B}$ of $\mathbf{A}$ such that $\mathbf{Con}\ \mathbf{B}$ fails ζ_n.

This does it: by (4), $\mathbf{L}_n$ is in the congruence variety associated with $\mathcal{K}$. It is not hard to show that, in general, the congruence variety associated with a variety $\mathcal{K}'$ is generated by the congruence lattices of the finitely generated free algebras of $\mathcal{K}'$, and from this it follows that $\mathbf{Con}\ \mathcal{P}$ is contained in the congruence variety associated with $\mathcal{K}$.

These steps above are not easy. What really made (4) possible is that $\mathbf{L}_1 = \mathbf{Con}\ \mathbf{F}_{\mathcal{P}}(n)$ was small enough to draw, but large enough so that one could see, from a proof that it is in every nonmodular congruence variety, how to prove that $\mathbf{L}_n$ is in every nonmodular congruence variety. A description of $\mathbf{F}_{\mathcal{P}}(n)$ is not difficult: its external Boolean algebra is the free Boolean algebra on n generators and, for each a in the external Boolean algebra, $\mathbf{S}(a)$ is the free Boolean algebra on k generators, where k is the number of generators above a. The maps between the $\mathbf{S}(a)$'s are the natural embeddings. Thus the external Boolean algebra of $\mathbf{F}_{\mathcal{P}}(0)$ is $\mathbf{2}$ and $\mathbf{S}(0) = \mathbf{S}(1) = \mathbf{2}$. Its congruence lattice is $\mathbf{N}_5$.[3]

The external Boolean algebra for $\mathbf{F}_{\mathcal{P}}(1)$ is $\mathbf{F}_{\mathcal{B}}(1) \cong \mathbf{2} \times \mathbf{2}$. Let $\{x, x', 0, 1\}$ be the universe of this Boolean algebra. Then $\mathbf{S}(1) = \mathbf{S}(x') = \mathbf{2}$ and $\mathbf{S}(x) = \mathbf{S}(0) = \mathbf{2} \times \mathbf{2}$. The congruence lattice of this algebra is diagrammed in Figure 7.



Con $\mathbf{F}_{\mathcal{P}}(1)$
FIGURE 7

In the semantic approach outlined above, we took an algebra $\mathbf{A}$ whose congruence lattice contained a pentagon labelled as in Figure 5 and formed the algebra $\mathbf{A}(\theta)$. The congruence lattice of this algebra contained two copies of $\mathbf{N}_5$ whose bottoms joined to θ. Using the Correspondence Theorem and the fact that $\eta_0 \vee \eta_1 = \theta_0 = \theta_1$, one could exactly determine the sublattice generated by these pentagons. If one tries a similar approach with $\mathbf{A}(\phi)$ or $\mathbf{A}(\psi)$, the sublattice generated by the two

[3]The variety $\mathcal{P}$ is important as an example in other aspects of algebra as well. It is generated by $\mathbf{F}_{\mathcal{P}}(1)$, which is the direct product of two 2 element algebras, both polynomially equivalent to the two element Boolean algebra. Thus $\mathcal{P}$ is the join of two congruence distributive, permutable varieties, but is nonmodular. Also $\mathcal{P}$ is residually large. Hence *the join of two congruence distributive varieties need not be congruence distributive* and *the join of two residually small varieties can be residually large*. This contrasts the situation for congruence modular varieties: *the join of two congruence distributive subvarieties of a congruence modular variety is congruence distributive* [18] and *the join of two residually small subvarieties of a congruence modular variety is residually small* (see Theorem 11.1 of [14]).

K. Kearnes and M. Valeriote have used a modification of $\mathcal{P}$ and the description of its congruences in [9] to answer some questions raised by Hobby and McKenzie in their book [19] on tame congruence theory.

pentagons is no longer uniquely determined. This limited the usefulness of this approach. However, in proving Theorem 11, one does not need to show $\mathbf{L}_n$ is a sublattice of some algebra constructed from $\mathbf{A}$, but only that some such algebra fails ζ_n. This is the same as constructing an algebra $\mathbf{B}$ from $\mathbf{A}$ and finding congruences on $\mathbf{B}$ such that the sublattice generated by these congruences has $\mathbf{L}_n$ as a homomorphic image.

How is this $\mathbf{B}$ constructed? Looking at Figure 7, we see that there are four filters of $\mathbf{Con}\ \mathbf{F}_{\mathcal{P}}(1)$ isomorphic to $\mathbf{N}_5$. Their least elements are indicated with solid points and labelled η_{ij} for $i, j < 2$. Of the $\binom{4}{2}$ pairs, two join to a ψ, one joins to a θ, one to a ϕ, and the two other pairs join to 1. This suggests letting $\mathbf{B}$ be the subalgebra of $\mathbf{A}^4$ which consists of all 2 by 2 matrices $\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$ whose elements satisfy the relations indicated in Figure 8.

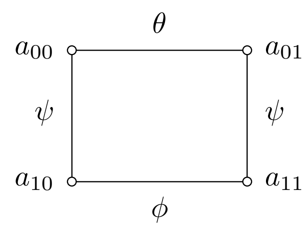


FIGURE 8

In general, to build an algebra from $\mathbf{A}$ whose congruence lattice fails ζ_n, we take all matrices (a_{fg}), where f, $g : \{0, 1, \ldots, n-1\} \to \{0, 1\}$, such that each column lies in a single ψ–class, each row lies in a single ϕ–class, and, if g and h agree on the support of f, then $a_{fg}\ \theta\ a_{fh}$.

The proof is inductive: ζ_n is defined inductively and the proof uses several inductive intermediate results. The proof when $n = 1$ is not hard, but unfortunately ζ_1 is a little too long to write out. But we can illustrate the argument by showing that the filter $1/(\eta_{00} \wedge \eta_{10})$ of $\mathbf{L}_1$ is contained in every nonmodular congruence variety. Let $\mathbf{L}$ denote this lattice; it is diagrammed in Figure 9. It is subdirectly irreducible with critical quotient r/s. If f is the homomorphism of $\mathbf{FL}(x, y_0, y_1, z_0, z_1)$ onto $\mathbf{L}$ indicated by the labelling of Figure 9, then the largest inverse image of s under f is

$$\alpha(s) = [(y_0 \vee z_0) \wedge (z_1 \vee (x \wedge (y_1 \vee z_1)))] \vee [(y_1 \vee z_1) \wedge (z_0 \vee (x \wedge (y_0 \vee z_0)))]$$

and the least preimage of r is

$$\begin{aligned} \beta(r) = [&(x \wedge y_0 \wedge z_0) \vee (y_0 \wedge ((x \wedge y_1 \wedge z_1) \vee (y_0 \wedge z_0 \wedge y_1 \wedge z_1)))] \\ &\wedge [(x \wedge y_1 \wedge z_1) \vee (y_1 \wedge ((x \wedge y_0 \wedge z_0) \vee (y_0 \wedge z_0 \wedge y_1 \wedge z_1)))]. \end{aligned}$$

The splitting equation for $\mathbf{L}$ is

$$\beta(r) \leq \alpha(s). \tag{4}$$

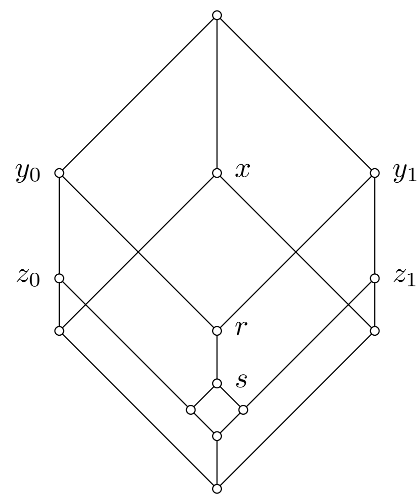


FIGURE 9

Now let **A** be an algebra containing elements a, b, c, and d whose congruence lattice contains the pentagon of Figure 2. Let $\mathbf{C} = \mathbf{A}(\psi)$. As before, if $\delta \in \mathrm{Con}\ \mathbf{A}$, $\delta_i \in \mathrm{Con}\ \mathbf{C}$, $i = 0$, 1, is defined by $\langle a_0, a_1\rangle\ \delta_i\ \langle b_0, b_1\rangle$ if $a_i\ \delta\ b_i$. Note $\psi_0 = \psi_1$; we denote this congruence again by ψ. Let $\eta_i = \psi \wedge \phi_i$ (so $\langle a_0, a_1\rangle\ \eta_i\ \langle b_0, b_1\rangle$ if and only if $a_i = b_i$). We will show that (4) fails in **Con C** under the interpretation $x \mapsto \psi$, $y_i \mapsto \phi_i$, and $z_i \mapsto \theta_i$, by showing that $\langle\langle c, c\rangle, \langle d, d\rangle\rangle$ is in the left side but not in the right.

The first meetand of the interpretation of $\beta(r)$ simplifies to

$$\eta_0 \vee (\phi_0 \wedge (\eta_1 \vee (\theta_0 \wedge \theta_1))).$$

We calculate

$$\langle c, a\rangle\ \eta_1\ \langle a, a\rangle\ \theta_0 \wedge \theta_1\ \langle b, b\rangle\ \eta_1\ \langle d, b\rangle$$

and hence, since $c\ \phi\ d$,

$$\langle c, c\rangle\ \eta_0\ \langle c, a\rangle\ \phi_0 \wedge (\eta_1 \vee (\theta_0 \wedge \theta_1))\ \langle d, b\rangle\ \eta_0 \langle d, d\rangle.$$

Thus $\langle\langle c, c\rangle, \langle d, d\rangle\rangle$ is in the first meetand of $\beta(r)$ and by symmetry it is in the second and hence in $\beta(r)$.

Under our interpretation $\alpha(s)$ simplifies to $(\phi_0 \wedge \theta_1) \vee (\phi_1 \wedge \theta_0)$. Suppose that $\langle\langle c, c\rangle, \langle d, d\rangle\rangle$ is in this congruence. Then there are elements $\langle a_0^i, a_1^i\rangle \in C$, $i = 0, \ldots, n$ with $\langle a_0^0, a_1^0\rangle = \langle c, c\rangle$ and $\langle a_0^n, a_1^n\rangle = \langle d, d\rangle$ such that the relations indicated in Figure 10 hold.

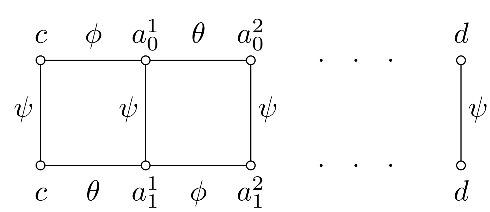


FIGURE 10

Since $\theta \le \phi$, we have that $\langle a_0^1, a_1^1\rangle \in \phi \wedge \psi = 0$. Thus $a_0^1 = a_1^1$. Continuing this argument, we see that $a_0^i = a_1^i$, for each i. But then

$$c\;\theta\; a_1^1 = a_0^1\;\theta\; a_0^2 = a_1^2\;\theta\;\cdots\; d$$

showing $c\,\theta\, d$. But this implies that $\theta = \phi$, a contradiction.

Theorem 11 has some important consequences. It follows immediately from this theorem that a lattice equation ϵ will imply congruence modularity if and only if ϵ fails in **Con** $\mathcal{P}$. This will happen if and only if ϵ fails in **Con** $\mathbf{F}_{\mathcal{P}}(n)$, i.e., ϵ implies ζ_n for some n. Using the fact that $\mathcal{P}$ has 4–permutable congruences (Theorem 7.6 of [9]), one can effectively find such an n; in fact, n can be taken as a linear function of the size of ϵ. Thus we have the following theorem of [1].

Theorem 12. *One can effectively decide if a lattice equation implies congruence modularity. One can also effectively decide if a lattice equation implies congruence distributivity.*

This puts a nice close on the problem of which equations imply congruence modularity. It is also shown in [9] that **Con** $\mathcal{P}$ is not self-dual. This is the first known congruence variety which is not self-dual. This paper also proves a strong compactness result for equations implying congruence modularity: if Σ is a set of lattice equations which imply congruence modularity, then, for some $\epsilon \in \Sigma$, ϵ implies congruence modularity.

More Recent Results

After completing [9], Bjarni Jónsson and J. B. Nation accused Alan and I of killing the subject of congruence varieties, since this paper answered most of the questions we had been interested in. And in fact the subject was dormant for several years. However, the subject is coming back to life because of some important recent developments. There are also some very interesting unsolved problems.

One problem that is still open:

- *Is there a unique largest modular congruence variety?*

Of course one candidate is the congruence variety determined by the variety of groups. This raises another interesting question:

- *Is the congruence variety associated with the variety of groups the same as the one associated with the variety of abelian groups?*

At first glance this would seem unlikely—the variety of groups is a much richer and more diverse class of algebras. However, if $\mathbf{A} \supseteq \mathbf{B}$ are normal subgroups of a group $\mathbf{G}$ such that the interval $\mathbf{A}/\mathbf{B}$ in the lattice of normal subgroups contains $\mathbf{M}_3$ as a sublattice with least element $\mathbf{B}$ and greatest element $\mathbf{A}$, then the quotient group $\mathbf{A}/\mathbf{B}$ is abelian. This is sometimes called Remak's Principle. Thus the modular, nondistributive parts of the congruence lattice of $\mathbf{G}$ correspond to abelian sections of the group. This gives credence to the idea that abelian groups and groups might have the same congruence variety and suggests that, if this is not the case, finding a counter example would be difficult and that one should look at nilpotent groups since, by the remark above, the nonabelian chief factors only contribute a subdirect factor isomorphic to the two element lattice to the normal subgroup lattice.

Up until recently, the only known modular, nondistributive congruence varieties were those associated with varieties of modules. It was conceivable that these were the only ones. These congruence varieties are well understood; they have been completely classified by G. Hutchinson and G. Czédli in [20]. Alan Day and Emil Kiss proved an important result in this direction. They showed that if $\mathcal{K}$ is a residually finite variety which is (contains only finite subdirectly irreducible algebras), congruence modular, but is not congruence distributive, then $\mathbf{Con}\,\mathcal{K}$ is the same as the congruence variety of the variety of modules over the ring, $\mathbf{R}(\mathcal{K})$, associated with $\mathcal{K}$. (This ring is defined in [14]; the exact definition is not important for the present discussion.) In particular, the next theorem follows from the result of Day and Kiss [8].

Theorem 13. *If $\mathcal{K}$ is a residually finite, congruence modular variety then* $\mathbf{Con}\,\mathcal{K}$ *is contained* $\mathbf{Con}\,\mathcal{A}$*, where $\mathcal{A}$ is the variety of abelian groups.*

Despite this, the above problem does have a negative solution, as was recently shown in an important result of P. P. Palfy and C. Szabó, [34].

Theorem 14. *There is a lattice equation which holds in* $\mathbf{Con}\,\mathcal{A}$ *but not in* $\mathbf{Con}\,\mathcal{G}$*, where $\mathcal{G}$ is the variety of groups.*

The next logical question is:

- *Is the congruence variety associated with groups the same as the one associated with loops? with quasigroups?*

The best result along these lines is the result of D. Hobby and R. McKenzie, [19]. The full problem remains open.

Theorem 15. *If $\mathcal{K}$ is a locally finite, congruence modular variety, then* $\mathbf{Con}\,\mathcal{K}$ *is contained in the congruence variety associated with the variety of loops.*

Tame congruence theory sheds more light on the congruence varieties associated with locally finite varieties. The next theorem, of Hobby and McKenzie, is from [19]. The definition of the type set of a variety is given there.

Theorem 16. *Let $\mathcal{K}$ is a locally finite variety. Then the following hold.*

(1) *If $\mathcal{K}$ satisfies a nontrivial congruence identity, then* $\operatorname{typ}(\mathcal{K}) \subseteq \{\mathbf{2},\mathbf{3},\mathbf{4}\}$.
(2) *If* $\operatorname{typ}(\mathcal{K}) \subseteq \{\mathbf{2},\mathbf{3}\}$*, then $\mathcal{K}$ satisfies a nontrivial congruence identity.*
(3) *If $\mathcal{K}$ is residually small and* $\operatorname{typ}(\mathcal{K}) \subseteq \{\mathbf{2},\mathbf{3},\mathbf{4}\}$*, then $\mathcal{K}$ is congruence modular.*

Combining the last part of this with the Day-Kiss result, the following theorem obtains.

Theorem 17. *Let $\mathcal{K}$ is a locally finite, residually small variety. If $\mathcal{K}$ satisfies a nontrivial congruence identity, then the congruence variety of $\mathcal{K}$ is the same as that of the variety of modules over* $\mathbf{R}(\mathcal{K})$*. In particular,* $\mathbf{Con}\,\mathcal{K}$ *is contained* $\mathbf{Con}\,\mathcal{A}$*, where $\mathcal{A}$ is the variety of abelian groups.*

In [26], Paolo Lipparini was able to remove the local finiteness hypothesis from part (2) of Theorem 16 and used this to prove the following theorem.

Theorem 18. *Every congruence n–permutable variety satisfies a nontrivial congruence identity.*

Finite basis results. Of course the varieties of distributive lattices and of modular lattices are defined by single equations, and thus are finitely based. The variety of distributive lattices is a congruence variety, but, by Theorem 9, the variety of modular lattices is not. This raises the question: which congruence varieties are finitely based? Surprisingly, no modular congruence variety is, [11].

Theorem 19. *No modular, nondistributive congruence variety is finitely based.*

The situation for nonmodular congruence varieties is open at this time.

Maltsev conditions. We end this paper with the same subject as we started with. There has not been much progress on Maltsev conditions for lattice equations. We already mentioned the result of Pixley and Wille that, for every lattice equation ϵ, congruence–ϵ is definable by a weak Maltsev condition. But no equation is known to only have a weak Maltsev condition associated with it. Using the commutator theory, it is possible to show that there are infinitely many lattice equations ϵ such that congruence–ϵ is defined by a Maltsev condition and for each pair of these equations, there is a congruence variety where one holds and the other fails. This is presented in Chapter XIII of [14]. Obviously a great deal of work remains to be done. It really is a shame that we won't have Alan to help in this endeavor. His contributions to our areas of mathematics will not soon be forgotten.

References

1. G. Czédli and R. Freese, *On congruence distributivity and modularity*, Algebra Universalis **17** (1983), 216–219.
2. A. Day, *A characterization of modularity for congruence lattices of algebras*, Canad. Math. Bull. **12** (1969), 167–173.
3. A. Day, *p–modularity implies modularity in equational classes*, Algebra Universalis **3** (1973), 398–399.
4. A. Day, *Lattice conditions implying congruence modularity*, Algebra Universalis **6** (1976), 291–301.
5. A. Day, *Splitting lattices generate all lattices*, Algebra Universalis **7** (1977), 163–170.
6. A. Day, *Splitting lattices and congruence-modularity*, Contributions to universal algebra, Proceedings of the Colloquium held in Szeged, 1975. Colloq. Math. Soc. János Bolyai, vol. 17, North Holland Publishing Co., Amsterdam, 1977, pp. 57–71.
7. A. Day, *Doubling constructions in lattice theory*, Canad. J. Math. **44** (1992), 252–269.
8. A. Day and E. Kiss, *Frames and rings in congruence modular varieties*, J. Algebra **109** (1987), 479–507.
9. A. Day and R. Freese, *A characterization of identities implying congruence modularity,* I, Canad. J. Math. **32** (1980), 1140–1167.
10. R. P. Dilworth, *The structure of relatively complemented lattices*, Ann. of Math. **51** (1950), 348–359.
11. R. Freese, *Finitely based modular congruence varieties are distributive*, Algebra Universalis (to appear).
12. R. Freese, C. Herrmann and A. P. Huhn, *On some identities valid in modular congruence varieties*, Algebra Universalis **12** (1981), 322–334.
13. R. Freese and B. Jónsson, *Congruence modularity implies the Arguesian identity*, Algebra Universalis **6** (1976), 225–228.
14. Ralph Freese and Ralph McKenzie, *Commutator Theory for Congruence Modular Varieties*, London Math. Soc. Lecture Note Series vol. **125**, Cambridge University Press, Cambridge, 1987.

15. R. Freese and J. B. Nation, *Congruence lattices of semilattices*, Pacific J. Math. **49** (1973), 51–58.
16. R. Freese and J. B. Nation, *3-3 lattice inclusions imply congruence modularity*, Algebra Universalis **7** (1977), 191–194.
17. E. Gedeonová, *A characterization of p-modularity for congruence lattices of algebras*, Acta. Fac. Rerum Natur. Univ. Comenian. Math. Publ. **28** (1972), 99–106.
18. J. Hagemann and C. Herrmann, *A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity*, Arch. Math. (Basel) **32** (1979), 234–245.
19. D. Hobby and R. McKenzie, *The Structure of Finite Algebras (tame congruence theory)*, Contemporary Mathematics, vol. 76, American Mathematical Society, Providence, RI, 1988.
20. G. Hutchinson and G. Czédli, *A test for identities satisfied in lattices of submodules*, Algebra Universalis **8** (1978), 269–309.
21. B. Jónsson, *Modular lattices and Desargues theorem*, Math. Scand. **2** (1954), 295–314.
22. B. Jónsson, *Algebras whose congruence lattices are distributive*, Math. Scand. **21** (1967), 110–121.
23. B. Jónsson, *Identities in congruence varieties*, Lattice theory (Proc. Colloq., Szeged,1974), Colloq. Math. Soc. János Bolyai, vol. 14, 1976, pp. 195–205.
24. B. Jónsson, *Congruence Varieties*, Algebra Universalis **10** (1980), 355–394.
25. B. Jónsson and I. Rival, *Lattice varieties covering the smallest non-modular variety*, Pacific J. Math. **82** (1979), 463–478.
26. Paolo Lipparini, *n–permutable varieties satisfy nontrivial congruence identities*, preprint.
27. A.I. Maltsev, *On the general theory of algebraic systems*, (Russian), Mat. Sbornik **77** (1954), 3–20.
28. R. McKenzie, *Equational bases and non-modular lattice varieties*, Trans. Amer. Math. Soc. **174** (1972), 1–43.
29. R. McKenzie, *Some unsolved problems between lattice theory and equational logic*, In Proc. Univ. Houston Lattice Theory Conf., 1973, pp. 563–573.
30. Ralph McKenzie, George McNulty and Walter Taylor, *Algebras, Lattices, Varieties,* Volume I, Wadsworth and Brooks/Cole, Monterey, California, 1987.
31. P. Mederly, *Three Mal'cev type theorems and their applications*, Math. Časopis Sloven. Akad. Vied. **25** (1975), 83–95.
32. J. B. Nation, *Congruence lattices of relatively free unary algebras*, Algebra Universalis **4** (1974), 132.
33. J. B. Nation, *Varieties whose congruences satisfy certain lattice identities*, Algebra Universalis **4** (1974), 78–88.
34. P. P. Pálfy and C. Szabó, *An identity for subgroup lattices of abelian groups*, Algebra Universalis (to appear).
35. A. F. Pixley, *Distributivity and permutability of congruence relations in equational classes of algebras*, Proc. Amer. Math. Soc. **14** (1963), 105–109.
36. A. F. Pixley, *Local Malcev conditions*, Canad. Math. Bull. **15** (1972), 559–568.
37. S. V. Polin, *Identities in congruence lattices of universal algebras*, Mat. Zametki **22** (1977), 443–451; English transl. in Mathematical Notes **22** (1977), 737–742.
38. W. Taylor, *Characterizing Mal'cev conditions*, Algebra Universalis **3** (1973), 351–397.
39. R. Wille, *Kongruenzklassengeometrien*, Lecture Notes in Mathematics, vol. **113**, Springer-Verlag, New York, 1970.

University of Hawaii, Honolulu, HI 96822
E-mail address: ralph@math.hawaii.edu