Algebra Universalis, **17** (1983) 216–219

0002–5240/83/020216–04$01.50+0.20/0

Mailbox

On congruence distributivity and modularity*

GÁBOR CZÉDLI and RALPH FREESE

Let ε be a lattice equation. We say ε implies congruence modularity if whenever $\mathcal{K}$ is a variety of algebras all of whose congruence lattices satisfy ε then all of these lattices are modular. The definition of ε implies congruence distributivity is similar. In this note we prove that the class of lattice equations which imply congruence modularity and the class of equations which imply congruence distributivity are both recursive. Although the proof we give is short it depends on results from [5] [6] and [9].

This subject began with J. B. Nation who showed that there are lattice equations strictly weaker than the modular law, which nevertheless imply congruence modularity. This theorem said that any ε of a certain syntactical form implied congruence modularity [13]. In a series of subsequent papers this theorem was extended to show other (but still rather special) syntactical forms imply congruence modularity [2, 3, 4, 8, 11]. Analogous results are known for congruence distributivity [11, 13]. In this light the results of this note are somewhat surprising.

In an important development, Polin constructed a variety of algebras, here denoted $\mathcal{P}$ which did not have modular congruences but did satisfy a nontrivial lattice identity. In [5] Alan Day and the second author showed that Con ($\mathcal{P}$) was the unique minimal nonmodular congruence variety. (A *congruence variety* is a variety of lattices generated by the congruence lattices of a variety of algebras $\mathcal{K}$ and is denoted Con ($\mathcal{K}$).) With this it was not hard to obtain a characterization of lattice equations which imply congruence modularity. We will show here that this characterization can be made effective.

In [5] the arithmetic of $\mathcal{P}$ and Con ($\mathcal{P}$) was worked out in detail. Let L_n be the

Presented by B. Jónsson. Received July 19, 1982. Accepted for publication in final form September 16, 1982.

* This research was partially supported by the National Science and Engineering Research Council of Canada, Operating Grant A8190, and the National Science Foundation, Grant No. MCS-8002311.

congruence lattice of the free, n-generated algebra in $\mathcal{P}$. Then L_n is a finite subdirectly irreducible splitting lattice (Theorem 4.9 of [5]). L_n is a splitting lattice means there is a lattice equation ζ_n such that every lattice variety either satisfies ζ_n or contains L_n, but not both.

Since Con $(\mathcal{P})$ is the unique minimal nonmodular congruence variety, ε will imply congruence modularity if and only if Con $(\mathcal{P})$ fails ε. The key to effectively deciding if Con $(\mathcal{P})$ fails ε is that $\mathcal{P}$ has 4-permutable congruences (see Theorem 7.6 of [5]). For t a lattice term define t^4 inductively: $x^4 = x$ if x is a variable, $(t_1 \wedge t_2)^4 = t_1^4 \wedge t_2^4$, and $(t_1 \vee t_2)^4 = t_1^4 \circ t_2^4 \circ t_1^4 \circ t_2^4$, where $\circ$ is the symbol for relational product. The above theorem says that for any congruences $z_1, \ldots, z_k$ on an algebra in $\mathcal{P}$ $t(z_1, \ldots, z_k) = t^4(z_1, \ldots, z_k)$.

Now we may assume ε has the form $u(x_1, \ldots, x_k) \leq v(x_1, \ldots, x_k)$. Then Con $(\mathcal{P})$ satisfies ε if and only if $u^4 \leq v^4$ holds for congruences of members of $\mathcal{P}$. Thus if Con $(\mathcal{P})$ fails ε then for some $A \in \mathcal{P}$ and congruences $z_1, \ldots, z_k$ there are elements $a_1, a_2 \in A$ with $(a_1, a_2) \in u^4(z_1, \ldots, z_k)$ but $(a_1, a_2) \notin v^4(z_1, \ldots, z_k)$. Now if $u = u_1 \wedge u_2$ then $(a_1, a_2) \in u_1$ and u_2. If $u = u_1 \vee u_2$ then $u^4 = u_1^4 \circ u_2^4 \circ u_1^4 \circ u_1^4$. Hence there are elements $a_3, a_4, a_5 \in A$ with (a_1, a_3) and (a_4, a_5) in u_1^4, and (a_3, a_4) and (a_5, a_2) in u_2^4. If we continue this process until we reach the z_i's we obtain a finite set $\{a_1, a_2, \ldots, a_m\}$ of elements of A, and associated with each z_i is a partition φ_i of $\{a_1, \ldots, a_m\}$ with $\varphi_i \subseteq z_i$. It is not hard to show, using the natural homomorphism from $F_{\mathcal{P}}(a_1, \ldots, a_m)$ into A, that $u^4 \leq v^4$ fails in Con $(F_{\mathcal{P}}(m))$. These arguments, which go back to Malcév, have been developed into an algorithm (described below) by Wille [15]. A detailed description of this algorithm, together with several examples is given in [9] (see Theorem 1 of [9]).

Notice that m is 2 more than the number of $\circ$ symbols in u^4. Also note that the partition φ_i on $\{a_1, \ldots, a_m\}$ can be calculated formally from u and does not depend on A. Thus from $u(x_1, \ldots, x_k)$ alone we can effectively determine m and the partitions $\varphi_1, \ldots, \varphi_k$ of $\{a_1, \ldots, a_m\}$. Let θ_i be the congruence on $F_{\mathcal{P}}(a_1, \ldots, a_m)$ generate by φ_i and if ε is $u(x_1, \ldots, x_k) \leq v(x_1, \ldots, x_k)$ let $m(\varepsilon)$ be two plus the number of $\circ$ symbols in u^4. Then we have the following theorem (conditions (3) and (4) are equivalent by the definition of splitting lattices).

THEOREM. *Let ε be a lattice equation. Then the following are equivalent:*

(1) *ε implies congruence modularity*
(2) Con $(\mathcal{P})$ *does not satisfy ε*
(3) *for some n, ε implies ζ_n*
(4) *for some n, L_n fails ε*
(5) *$L_{m(\varepsilon)}$ fails ε*
(6) *$(a_1, a_2) \notin v(\theta_1, \ldots, \theta_k)$ in $F_{\mathcal{P}}(a_1, \ldots, a_{m(\varepsilon)})$*

Since $\mathscr{P}$ is generated by a single four element algebra L_n can effectively be found. Thus we have the following corollary:

COROLLARY. *One can recursively decide if a lattice equation ε implies congruence modularity.*

The L_n's grow too fast for (5) to be practical. However, since the arithmetic of $\mathrm{Con}(\mathscr{P})$ is well-developed, condition (6) is practical. A related, but slightly different technique for verifying equations valid in $\mathrm{Con}(\mathscr{P})$, is given in §7 of [5].

For the distributive case we need the second author's list of the minimal modular, nondistributive congruence varieties. For p a prime or 0 let $\mathscr{V}_p$ be the congruence variety associated with the variety of all vector spaces over F_p, the field with p elements ($F_0 = Q$). Then if $\mathscr{V}$ is a modular, nondistributive congruence variety, $\mathscr{V}_p \subseteq \mathscr{V}$ for some p ([6], [7]). Thus if ε implies congruence modularity, it will imply congruence distributivity if and only if it fails in every $\mathscr{V}_p$.

Now George Hutchinson and the first author have shown that associated with any lattice equation ε are two natural numbers $m_\varepsilon \geq 0$, $n_\varepsilon \geq 1$ (and these can be effectively found from ε) such that $\mathscr{V}_p$ will satisfy ε if and only if there is an $x \in F_p$ such that $m_\varepsilon x = n_\varepsilon$ ([9], Theorems 2 and 3). If $m_\varepsilon \neq 0$ and then clearly this condition will be true in Q. If $m_\varepsilon = 0$ and $n_\varepsilon \neq 1$ then this condition will be true in F_p for any p dividing n_ε. Thus ε will fail to hold in every $\mathscr{V}_p$ if and only if $m_\varepsilon = 0$ and $n_\varepsilon = 1$. Thus to test if ε implies congruence distributivity one first tests if it implies congruence modularity. If it does then one evaluates m_ε, n_ε. If $m_\varepsilon = 0$ and $n_\varepsilon = 1$, ε implies congruence distributity; otherwise it does not.

COROLLARY. *Once can recursively decide if a lattice equation ε implies congruence distributivity.*

Acknowledgment

The authors are indebted to Alan Day for several helpful discussions and for providing the first author with financial support and excellent ambiance at Lakehead University.

REFERENCES

[1] P. CRAWLEY and R. P. DILWORTH, *Algebraic Theory of Lattices*, Prentice-Hall, Englewood Cliffs, N.J., 1973.

[2] A. DAY, *p-modularity implies modularity in equational classes*, Algebra Universalis *3* (1973), 398–399.
[3] A. DAY, *Lattice conditions implying congruence modularity*, Algebra Universalis *6* (1976), 291–302.
[4] A. DAY, *Splitting lattices and congruence modularity*, Colloq. Math. Soc. János Bolyai 17. Contributions to Universal Algebra, Szeged (1975), 57–71.
[5] A. DAY and R. FREESE, *A characterization of identities implying congruence modularity I*, Can. J. Math., *32* (1980), 1140–1167.
[6] R. FREESE, *Minimal modular congruence varieties*, Amer. Math. Soc. Notices *23* (1976).
[7] R. FREESE, C. HERRMANN, and A. HUHN, *On some identities valid in modular congruence varieties*, Algebra Universalis *12* (1981), 322–334.
[8] R. FREESE and J. B. NATION, 3-3 *lattice inclusions imply congruence modularity*, Algebra Universalis 7 (1977), 191–194.
[9] G. HUTCHINSON and G. CZÉDLI, *A test for identities satisfied in lattices of submodules*, Algebra Universalis *8* (1978) 269–309.
[10] B. JÓNSSON, *Varieties of algebras and their congruence varieties*, Proceedings of the International Congress of Mathematicians, Vancouver (1974), 315–320.
[11] B. JÓNSSON, *Identities in congruence varieties*, Colloq. Math. Soc. János Bolyai 14. Lattice Theory, Szeged, 1974, 195–205.
[12] P. MEDERLY, *Three Mal'cev type theorems and their applications*, Math. Casopis Sloven. Akad. Vied. 25 (1975), 83–95.
[13] J. B. NATION, *Varieties whose congruences satisfy certain lattice identities*, Algebra Universalis *4* (1974), 78–88.
[14] S. V. POLIN, *On identities in congruence lattices of universal algebras*, Mat. Zametki *22* (1977), 443–451. Translated in Mathematical Notes.
[15] R. WILLE, *Kongruenzklassengeometrien*, Springer Verlag Lecture Notes in Math. 113, Berlin, (1970).

University of Hawaii
Honolulu, Hawaii
U.S.A.