Algebra Universalis, **11** (1980) 22–27 Birkhäuser Verlag, Basel

Congruence lattices of finite algebras and intervals in subgroup lattices of finite groups

PÉTER PÁL PÁLFY AND PAVEL PUDLÁK

Introduction

It is well-known that every algebraic lattice is isomorphic to the congruence lattice of an algebra. In this paper we are interested in the problem of characterizing the finite lattices, which are isomorphic to the congruence lattices of *finite* algebras. We are not able to settle the problem if every finite lattice is isomorphic to the congruence lattice of a finite algebra (cf. [1], Problem 13). Our main result shows that this problem is related to the problem to characterize intervals in subgroup lattices of finite groups. Namely, every finite lattice is isomorphic to the congruence lattice of a finite algebra if and only if every finite lattice is isomorphic to an interval in the subgroup lattice of a finite group.

Theorems

It is a trivial fact that, while representing lattices as congruence lattices of algebras, we can confine ourselves to unary algebras. By a unary algebra we shall mean a couple $\mathcal{A}=(A, F)$, where A is a set and F is a monoid of transformations of A. The congruence lattice of $\mathcal{A}$, i.e. the lattice of all congruence relations over $\mathcal{A}$, will be denoted by $\operatorname{Con}(\mathcal{A})$. Assuming that F is a monoid is no loss of generality, since, for any set F of transformations, $\operatorname{Con}(A, F)=\operatorname{Con}(A, F^*)$, where F^* is the monoid generated by F.

THEOREM 1. *Let L be a finite lattice and $\mathcal{A}=(A, F)$ a finite unary algebra of minimal cardinality for which* $\operatorname{Con}(\mathcal{A})\cong L$. *Then we have*

(i) *if L satisfies (A) below, every idempotent mapping in F is either the identity or a constant mapping;*

(ii) *if L satisfies (A) and (B) below, every element of F is either a permutation*

The work of the second author was supported in part by NSF Grant MCS 76-06447 A01.

Presented by G. Grätzer. Received June 29, 1978. Accepted for publication in final form November 2, 1978.

or a constant mapping;

(iii) *if L satisfies (A), (B) and (C) below, then $\mathcal{A}$ has no proper subalgebra.*

The conditions are

(A) *L is simple.*

(B) *For any nonzero element $x \in L$ there exist two elements $y_1, y_2 \in L$ such that $x \vee y_1 = x \vee y_2 = 1_L$ and $y_1 \wedge y_2 = 0_L$.*

(C) *$|L| \neq 2$ and, for any $x \in L$ not an atom and not 0_L, there exist at least 4 atoms less than x.*

We do not claim that the conditions (A), (B), (C) are the weakest such that Theorem 1 holds. The theorem serves us to prove our main result.

THEOREM 2. *The following statements are equivalent:*

(i) *Any finite lattice is isomorphic to the congruence lattice of a finite algebra.*

(ii) *Any finite lattice is isomorphic to an interval of the subgroup lattice of a finite group.*

Most investigations were concentrated on lattices of length 2. We shall denote by M_n the lattice of length two with n atoms. If $n = p^k + 1$ for p prime, then M_n is isomorphic to the congruence lattice of the two dimensional vector space over the finite field $GF(p^k)$. P. Goralčík pointed out that perhaps M_7 – the smallest among them which cannot be represented in the previous way – will be crucial for the problem of representability (see [1]).

If $n \geq 4$, then M_n satisfies the conditions (A), (B), (C), therefore, if it is representable as the congruence lattice of a finite algebra, then it is isomorphic to an interval $[H, G]$ of the subgroup lattice of a finite group G. Moreover, we can suppose that H contains no nontrivial normal subgroup of G, since otherwise we can factorize G by this normal subgroup and get an interval isomorphic to $[H, G]$ in the subgroup lattice of the factor group. The following theorem gives us important information about such representations.

THEOREM 3. *Let G be a finite group and $H < G$ such that the interval $[H, G]$ of the subgroup lattice of G is isomorphic to M_n, $n \geq 3$, and H contains no nontrivial normal subgroup of G. If G has a nontrivial abelian normal subgroup, then $n-1$, is a prime power.*

Thus for example M_7 cannot be an interval of the subgroup lattice of a finite solvable group. The case of non-solvable groups should be the topic of further investigations.

Proofs

LEMMA 1. *Let $\mathscr{A} = \langle A, F\rangle$ be a unary algebra where F is a monoid and let $e \in F$ be an idempotent operation. Let us define $\mathscr{B} = \langle B, G\rangle$ in the following way: $B = e(A)$, $G = \{ef \restriction_B \mid f \in F\}$. Finally let α:* Con $(\mathscr{A}) \to$ Con $(\mathscr{B})$ *be the restriction of congruences to the set B. Then α is a surjective homomorphism (even for arbitrary meets and joins).*

Proof of the Lemma. By the definition of $\mathscr{B}$, α obviously maps Con $(\mathscr{A})$ into Con $(\mathscr{B})$ and α is trivially $\wedge$-preserving. Now let $\theta, \Psi \in$ Con $(\mathscr{A})$ and let $a, b \in B$ for which $a \equiv b(\theta \vee \Psi)$. Then there exists a chain of elements $c_0 = a$, $c_1, \ldots, c_{n-1}$, $c_n = b \in A$ such that $c_{2i} \equiv c_{2i+1}(\theta)$ and $c_{2i+1} \equiv c_{2i+2}(\Psi)$ $(i = 0, 1, 2, \ldots)$. Now $e(c_0)$, $e(c_1), \ldots, e(c_n)$ is a chain of elements in $e(A) = B$ for which $e(c_{2i}) \equiv e(c_{2i+1})(\alpha(\theta))$ and $e(c_{2i+1}) \equiv e(c_{2i+2})(\alpha(\Psi))$ $(i = 0, 1, 2, \ldots)$. Since e is idempotent $e(c_0) = e(a) = a$ and $e(c_n) = e(b) = b$, so we have $a \equiv b(\alpha(\theta) \vee \alpha(\Psi))$ that is $\alpha(\theta \vee \Psi) \leqq \alpha(\theta) \vee \alpha(\Psi)$. However, the reverse inclusion trivially holds, so α is really $\vee$-preserving. Now let Φ be a congruence on $\mathscr{B}$. Let us denote by $\bar{\Phi}$ the congruence on $\mathscr{A}$ generated by Φ. We shall show that $\alpha(\bar{\Phi}) = \Phi$. To do this let $a, b \in B$ for which $a \equiv b(\bar{\Phi})$. By Mal'cev's lemma there exists a chain of elements $c_0 = a$, $c_1, \ldots, c_n = b \in A$ and exist operations $f_0, f_1, \ldots, f_{n-1} \in F$ and elements c'_0, $c'_1, \ldots, c'_{n-1}, c''_1, c''_2, \ldots, c''_n \in B$ satisfying $c'_1 \equiv c''_{i+1}(\Phi)$, $f_i(c'_i) = c_i$, $f_i(c''_{i+1}) = c_{i+1}$, $i = 0, 1, \ldots, n-1$. Again applying e we get a chain $e(c_0) = a$, $e(c_1), \ldots, e(c_n) = b \in B$ for which $e(c_i) = ef_i(c'_i) \equiv ef_i(c''_{i+1}) = e(c_{i+1})(\Phi)$, $i = 0, 1, \ldots, n-1$, therefore $\alpha(\bar{\Phi}) = \Phi$, indeed.

Proof of Theorem 1. (i) Let $\mathscr{A} = \langle A, F\rangle$ be a finite unary algebra of minimal cardinality with the congruence lattice $\mathscr{L}$ and let $\mathscr{L}$ be simple. If $e \in F$ is idempotent, then Lemma 1 can be applied. Since $\mathscr{L}$ is simple we obtain that either Con $(\mathscr{B}) \cong 1$ or Con $(\mathscr{B}) \cong L$. In the first case $|B| = 1$, so e is a constant. In the second case, from the minimality of $\mathscr{A}$, we infer that $\mathscr{B} = \mathscr{A}$, so e is the identity.

(ii) Let us denote by F_0 the set of all non-permutations from F. Define the congruence Φ in the following way: for $a, b \in A$ set $a \equiv b(\Phi)$ iff for all $f \in F_0$, $f(a) = f(b)$. Now Φ is clearly a congruence. First suppose that $\Phi = 0_{\mathscr{A}}$ – the identity equivalence. This means that for any two different elements $a, b \in A$ there exists an $f \in F_0$ for which $f(a) \neq f(b)$. Consider the set of all ordered pairs of different elements of A, then, from the finiteness of A, we obtain a sequence of pairs $(a_0, b_0), (a_1, b_1), \ldots, (a_n, b_n)$ and a sequence of operations $f_0, f_1, \ldots, f_n \in F_0$ for which $f_i(a_i) = a_{i+1}$, $f_i(b_i) = b_{i+1}$, $i = 0, 1, \ldots, n-1$, and $f_n(a_n) = a_0$, $f_n(b_n) = b_0$. Let $f = f_n f_{n-1} \cdots f_1 f_0$, then $f \in f_0$ and $f(a_0) = a_0$, $f(b_0) = b_0$, $a_0 \neq b_o$. Because of the finiteness of A, an appropriate power of f is idempotent. But f is a non-permutation having more than one fixed point which contradicts (i). So we have obtained that $\Phi = 0_{\mathscr{A}}$, thus the condition (B) yields two congruences $\theta_1, \theta_2 \in \mathrm{Con}\,(\mathscr{A})$ such that $\Phi \vee \theta_1 = \Phi \vee \theta_2 = 1_{\mathscr{A}} = A \times A$, $\theta_1 \wedge \theta_2 = 0_{\mathscr{A}}$. Let $a, b \in A$ be arbitrary elements. Then there exist chains $c_0 = a$, $c_1, \dots, c_{n-1}$, $c_n = b$ and $c'_0 = a$, $c'_1, \dots, c'_{n-1}$, $c'_{n-1} = b$ in A for which $c_{2i} \equiv c_{2i+1}(\Phi)$, $c_{2i+1} \equiv c_{2i+2}(\theta_1)$, $c'_{2i} \equiv c'_{2i+1}(\Phi)$, $c'_{2i+1} \equiv c'_{2i+2}(\theta_2)$, $i = 0, 1, 2, \dots$. Let us choose an arbitrary $f \in F_0$. Then we have $f(c_{2i}) = f(c_{2i+1})$, $f(c_{2i+1}) \equiv f(c_{2i+2})(\Phi)$, $f(c'_{2i}) = f(c'_{2i+1})$, $f(c'_{2i+1}) \equiv f(c'_{2i+2})(\theta_2)$, $i = 0, 1, 2, \dots$, thus $f(a) = f(c_0) \equiv f(c_n) = f(b)(\theta_j)$, $j = 1, 2$. Since $\theta_1 \wedge \theta_2 = 0_{\mathscr{A}}$ this means that $f(a) = f(b)$. This holds for any $a, b \in A$, $f \in F_0$, hence any element of F_0 is a constant, so we are done.

(iii) If we omit the constant operations, the congruence lattice will not change, so we may suppose that F is a permutation group on A. If $\mathscr{A} = \mathscr{A}_1 \cup \mathscr{A}_2$, $\mathscr{A}_1 \cap \mathscr{A}_2 = \phi$, $|\mathscr{A}_2| \geqq 2$, $|\mathscr{A}_2| \geqq 2$, is a decomposition of A into subalgebras, then let θ_j be an atom in $\mathrm{Con}\,(\mathscr{A}_j)$, $j = 1, 2$. Now, if we denote by $\bar{\theta}_j$ the smallest extension of θ_j to A, there are only two atoms in $\mathrm{Con}\,(\mathscr{A})$, namely $\bar{\theta}_1$ and $\bar{\theta}_2$, which are less than $\bar{\theta}_1 \vee \bar{\theta}_2$ contradicting the condition (C). Therefore $\mathscr{A}$ cannot be decomposed in the previous way. Since F is a permutation group, we can decompose $\mathscr{A}$ into a disjoint union of its minimal subalgebras. By the previous remark we can have only the following possibilities: I. $\mathscr{A} = \mathscr{A}_1 \cup \mathscr{A}_2 \cup \mathscr{A}_3$, $|\mathscr{A}_j| = 1$, $j = 1, 2, 3$; II. $\mathscr{A} = \mathscr{A}_1 \cup \mathscr{A}_2$, $|\mathscr{A}_j| = 1$, $j = 1, 2$; III. $\mathscr{A} = \mathscr{A}_1 \cup \mathscr{A}_2$, $|\mathscr{A}_1| > 1$, $\mathscr{A}_1$ has no proper subalgebra, $|\mathscr{A}_2| = 1$; IV. $\mathscr{A}$ has no proper subalgebra. In the cases I and II $\mathrm{Con}\,(\mathscr{A})$ is the partition lattice on three and two point sets respectively, but these lattices do not satisfy the condition (C). In the case III, $1_{\mathscr{A}}$ is a $\vee$-irreducible element, thus $\mathrm{Con}\,(\mathscr{A})$ does not satisfy the condition (B). Therefore $\mathscr{A}$ has no proper subalgebra as we claimed.

LEMMA 2. *Any finite lattice $\mathscr{L}$ can be embedded into a finite lattice $\mathscr{L}'$ as an interval $[u, 1_{\mathscr{L}'}]$ such that $\mathscr{L}'$ satisfies the conditions (A), (B) and (C).*

Proof. Given a lattice $\mathscr{L}$, the elements of $\mathscr{L}'$ will be the ones of $\mathscr{L}$, elements $t_i(z)$, where $z \in \mathscr{L}$, $i = 1, 2, 3, 4$, and $0_{\mathscr{L}'}$. For $x, y \in \mathscr{L}'$ let

$$x \leqq y \text{ iff} \begin{cases} x = y, \text{ or} \\ x = 0_{\mathscr{L}'}, \ y \text{ arbitrary, or} \\ x = t_i(z), \ y \in \mathscr{L}, \ z \leqq y \text{ in } \mathscr{L}, \text{ or} \\ x, y \in L, \ x \leqq y \text{ in } \mathscr{L}. \end{cases}$$

$\mathscr{L}'$ is clearly a lattice satisfying the property (C). In order to prove (B) let x be an arbitrary element, $x \neq 0_{\mathscr{L}'}$, and choose for y_1 and y_2 two elements from $\{t_i(1_{\mathscr{L}}) \mid i = 1, 2, 3\}$ such that x, y_1, y_2 will be different. Then obviously $x \vee y_1 = x \vee y_2 = 1_{\mathscr{L}'}$, $y_1 \wedge y_2 = 0_{\mathscr{L}'}$. The simplicity of $\mathscr{L}'$ (condition (A)) can be checked by routine computations.

LEMMA 3. *Let $\mathscr{A} = \langle A, G\rangle$ be a unary algebra, where G is a transitive group of operations. The* Con $(\mathscr{A})$ *is isomorphic to the interval* $[G_a, G]$ *of the subgroup lattice of G, where G_a denotes the subgroup of G consisting of all elements of G which fix the arbitrarily chosen element $a \in A$.*

Proof. For $\Psi \in \mathrm{Con}(\mathscr{A})$, let $G(\Psi) = \{g \in G \mid g(a) \equiv a(\Psi)\}$, and for H, $G_a \leqq H \leqq G$, let $b \equiv c(\theta(H))$ mean that there exist $g \in G$ and $h \in H$ such that $gh(a) = b$, $g(a) = c$. If $g_1, g_2 \in G(\Psi)$, then $g_1g_2^{-1}(a) \equiv g_1(a) \equiv a(\Psi)$, thus $G(\Psi)$ is a subgroup of G and clearly $G(\Psi) \geqq G_a$. It is also easy to see that $\theta(H)$ is a congruence on $\mathscr{A}$. The equality $G(\theta(H)) = H$ trivially follows from the definitions. On the other hand $b \equiv c(\theta(G(\Psi)))$ if and only if there exist $g, h \in G$ for which $h(a) \equiv a(\Psi)$ and $b = gh(a)$, $c = g(a)$. Since G is transitive, it is equivalent to $b \equiv c(\Psi)$. Therefore $\theta(G(\Psi)) = \Psi$. Finally $G(\theta) \leqq G(\Psi)$ iff $\theta \leqq \Psi$, so $\Psi \to G(\Psi)$ is an isomorphism between Con $(\mathscr{A})$ and $[G_a, G]$.

Proof of Theorem 2. (i) $\Rightarrow$ (ii). Let $\mathscr{L}$ be an arbitrary finite lattice. Let us embed it into a finite lattice $\mathscr{L}'$ as in Lemma 2. By (i) $\mathscr{L}'$ is isomorphic to Con $(\mathscr{A})$ for a finite algebra $\mathscr{A}$. Choose $\mathscr{A}$ to be a finite algebra of minimal cardinality with Con $(\mathscr{A}) \cong L'$. Con $(\mathscr{A})$ will not change if we consider only the unary polynomials of $\mathscr{A}$ as operations of a new algebra $\mathscr{A}'$ with the same universe as $\mathscr{A}$. Since (A), (B) and (C) hold for $\mathscr{L}'$, Theorem 1 forces that in $\mathscr{A}' = \langle A, G\rangle$ G is actually a transitive permutation group on A. Now by Lemma 3 $[G_a, G] \cong \mathrm{Con}(\mathscr{A}') = \mathrm{Con}(\mathscr{A}) \cong \mathscr{L}'$ for an arbitrary $a \in A$, and since $\mathscr{L}$ is an interval of $\mathscr{L}'$ we obtain that in fact $\mathscr{L}$ is isomorphic to an interval of the subgroup lattice of a finite group.

(ii) $\Rightarrow$ (i). Let $\mathscr{L}$ be a finite lattice and G a finite group, H a subgroup of G such that $[H, G] \cong \mathscr{L}$. We assume here that H contains no nontrivial normal subgroup of G. Consider the operation of G from the left on the set of the left cosets of G respective to H. Clearly it is a finite unary algebra with the transitive group of operations G, and the subgroup which fixes the coset H is H itself. Thus by Lemma 3 we are done.

Proof of Theorem 3. Let $[H, G] = \{H, K_1, K_2, \ldots, K_n, G\}$ and let A be a minimal nontrivial abelian normal subgroup of G. By the assumptions $A \nleqq H$, so either AH is a maximal subgroup in G or $AH = G$. In the latter case $A \cap K_1$ is a nontrivial abelian subgroup of G, and it is normal in K_1 and also in A, therefore in $AK_1 = G$. Since $(A \cap K_1)H \leqq K_1$, it contradicts to the minimality of A. Therefore AH is maximal in G, say $AH = K_1$. For $j = 2, \ldots, n$ we have $K_1K_j = AHK_j = AK_j = G$, from which $|G : K_j| = |K_1 : K_1 \cap K_j| = |K_1 : H| = |A : A \cap H|$, and $|G : K_j| = |A : A \cap K_j|$, hence $A \cap H = A \cap K_j$. Since $n \geqq 3$, $A \cap H$ is normal in $\langle K_2, K_3\rangle = G$, therefore by our assumptions $A \cap H = A \cap K_j = 1$, for $j = 2, \ldots, n$. Thus any of the subgroups K_j contains exactly one element from each coset of G respective to

A. Hence we have uniquely determined functions $\phi_j : K_2 \to A$ such that $K_j = \{x\phi_j(x) \mid x \in K_2\}$, $j = 2, \ldots, n$. Since $(x\phi_j(x))(y\phi_j(y)) = (xy)(\phi_j(xy))$, we have the following identity:

$$\phi_j(xy) = y^{-1}\phi_j(x)y\phi_j(y) \quad \text{for all} \quad x, y \in K_2, \quad j = 2, \ldots, n. \tag{1}$$

Moreover, since $H \leqq K_j$, we have

$$\phi_j(x) = 1 \quad \text{for all} \quad x \in H, \quad j = 2, \ldots, n. \tag{2}$$

Conversely, if we are given a function $\phi : K_2 \to A$ satisfying (1) and (2), then $B = \{x\phi(x) \mid x \in K_2\}$ is a subgroup of G such that $B \geqq H$, $AB = G$, $A \cap B = 1$, therefore B is one of the subgroups K_j, $j = 2, \ldots, n$. Henceforth the number of these subgroups, $n - 1$, is equal to the number of functions $\phi : K_2 \to A$ satisfying (1) and (2). If ϕ and ψ are such functions, then $\phi\psi$ defined by $\phi\psi(x) = \phi(x)\psi(x)$ also satisfies (1) and (2), since A is abelian. Moreover, A, being a minimal normal subgroup, is an elementary abelian p-group, therefore – as it can be easily verified – the functions ϕ_j, $j = 2, \ldots, n$ also form an elementary abelian p-group. Thus their number is a power of the prime p. So we are done.

Acknowledgement

The authors would like to thank Prof. Garrett Birkhoff for very useful suggestions concerning this paper.

REFERENCES

[1] P. GORALČÍK, Problem, Coll. Math. Soc. J. Bolyai 17, Contributions to Universal Algebra, p. 604.
[2] G. GRÄTZER, Universal Algebra, D. Van Nostrand Co., 1968.

Czechoslovak Academy of Sciences
Praha
Czechoslovakia

Hungarian Academy of Sciences
Budapest
Hungary