Acta Sci. Math., 51 (1987), 153—162

Distributive congruence lattices of finite algebras

P. P. PÁLFY

To the memory of András Huhn

The most famous open problem in universal algebra is the representation of finite lattices as congruence lattices of finite algebras. The general question is very hard, and in essence it is a group theoretic problem (see [12], [10], [9]). Though, representing finite *distributive* lattices is an easy job. Perhaps the most standard way to do this is by starting with a boolean lattice B containing the given finite distributive lattice D and then adding the closure operation $f: B \to B$, defined by $f(x) = \bigwedge\{y \in D: y \geqq x\}$; it is easy to see that $\mathrm{Con}(B; \vee, \wedge, f) \cong D$. Another result which shows that it is extremely easy to find congruence representations for finite distributive lattices, due to QUACKENBUSH and WOLK [14], states that for any finite distributive sublattice D of $\mathrm{Eq}(A)$ — the lattice of equivalence relations over the set A — containing the equality and the total relation, some (unary) operations can be defined on A so that the congruences will be exactly the members of D. It was shown by P. PUDLÁK [13] that only the distributive finite lattices have this property, i.e. for any other finite lattice there is a representation by equivalences which is not the congruence lattice of any algebra defined on the given set.

In this paper we deal with the problem of representing *all* finite distributive lattices as congruence lattices of finite algebras belonging to some given class of algebras. For completeness we will cite some known results as well. The answer is positive for lattices (DILWORTH), groups (SILCOCK [18]), solvable groups (Theorem 2.2), modules (trivial, see Proposition 4.1), 2-unary algebras (Theorem 5.3), transitive permutation groups regarded as unary algebras (TŮMA [19], see also Proposition 5.5), algebras of any given type except the 1-unary (Corollary 6.1). There exist finite distributive lattices which are not representable as the congruence lattice of a finite ring (Proposition 3.1), of a 1-unary algebra (Corollary 5.2).

Received April 24, 1986.

Research supported by Hungarian National Foundation for Scientific Research grant No. 1813.

Throughout the paper D will stand for a finite distributive lattice with minimal element 0, J will denote the set of join-irreducible elements of D (0 is not regarded to belong to J), and $n=|J|$, the length of D.

1. Lattices. For lattices we only recall some well-known results. The most basic one is the following, which was first obtained by R. P. Dilworth (mentioned in [1] without proof), see also G. GRÄTZER and E. T. SCHMIDT [4].

1.1. Theorem. *Every finite distributive lattice is isomorphic to the congruence lattice of a finite lattice.*

The congruence lattice of a finite modular lattice is always boolean, but this is no longer true for *infinite* modular lattices. The following remarkable result is worth digressing from our topic of distributive congruence lattices of *finite* algebras.

1.2. Theorem (E. T. SCHMIDT [16]). *Every finite distributive lattice is isomorphic to the congruence lattice of a modular lattice.*

R. FREESE [3] proved that the lattices can be chosen to be finitely generated.

For more detailed discussion we refer the reader to E. T. SCHMIDT's lecture notes [17].

2. Groups. The question for groups was first dealt with by J. KUNTZMANN [8] in 1947, but his construction was not correct (see [15], p. 101). The solution came thirty years later:

2.1. Theorem (H. L. SILCOCK [18]). *Every finite distributive lattice is isomorphic to the congruence lattice (i.e. the lattice of normal subgroups) of a finite group.*

Silcock's construction is based on wreath products of nonabelian simple groups, but he also announced the solvable version of the result, see [18], p. 371. However, his construction of solvable groups with given distributive lattice of normal subgroups is rather complicated and has not been published. Since we deem our construction quite natural, we prove it here:

2.2. Theorem. *Every finite distributive lattice is isomorphic to the lattice of normal subgroups of a finite solvable group.*

Proof. All groups which will appear in the construction will have the property that in any chief series (i.e. maximal chain of normal subgroups) $1=N_0<N_1<\ldots$ $\ldots<N_{n-1}<N_n=G$ the chief factors N_{i+1}/N_i $(i=0, 1, \ldots, n-1)$ are elementary abelian p_i-groups for pairwise different prime numbers p_i (p_i will be called the *characteristic* of N_{i+1}/N_i). Then any chief series of G has this property by the Jordan—Hölder theorem. It implies that in any factor group G/N, no two minimal normal subgroups M_1/N and M_2/N can be isomorphic, as $N<M_1<M_1M_2$ is extendable

to a chief series of G. This property will enable us to make use of a theorem of R. KOCHENDÖRFFER [7], which ensures the existence of a faithful irreducible representation of G/N over the p-element field for any prime p not dividing the order of G/N. (This is in fact a strong sufficient condition derived from the necessary and sufficient condition given by Kochendörffer.) In other words this means that there exists an elementary abelian p-group A and a homomorphism $\varphi: G \to \mathrm{Aut}(A)$ with $\mathrm{Ker}\,\varphi = N$ such that there are no nontrivial subgroups of A invariant for the group of automorphisms $\varphi(G)$.

The construction will go by induction on the length of the finite distributive lattice D. Let a be an atom in D, $b = \bigvee\{x \in D: x \wedge a = 0\}$, then $a \wedge b = 0$. Let D_1 be the distributive lattice $\{x \in D: x \geqq a\}$. By the induction hypothesis, there exists a finite solvable group G with chief factors of different characteristics whose lattice of normal subgroups is isomorphic to D_1. Let B be the normal subgroup of G corresponding to $a \vee b \in D_1$. Choose a prime p not dividing the order of G. By the cited result of Kochendörffer, there exists a faithful irreducible representation of G/B over the p-element field, i.e. we have an elementary abelian p-group A and a homomorphism $\varphi: G \to \mathrm{Aut}(A)$ with $\mathrm{Ker}\,\varphi = B$ and $\varphi(G)$ acting irreducibly on A. Now form the semidirect product $\bar{G} = AG$ with respect to φ. Then the irreducibility of the representation φ implies that A is a minimal normal subgroup of $\bar{G}$, and by the choice of p, the characteristics of the factors in a chief series of $\bar{G}$ are also pairwise different.

Now let $N \lhd \bar{G}$. Since A is a minimal normal subgroup of $\bar{G}$, it follows that either $N \geqq A$ or $N \cap A = 1$. In the first case, $N = A(N \cap G)$ with $N \cap G \lhd G$. In the second, $N \leqq C_{\bar{G}}(A) = A \times B$, and as N contains no elements of orders divisible by p, we have $N \leqq B$. Conversely, if $N_1 \lhd G$, then $AN_1 \lhd \bar{G}$; if $N_1 \lhd G$ and $N_1 \leqq B$ then $N_1 \lhd \bar{G}$. Hence the lattice of normal subgroups of $\bar{G}$ is isomorphic to D.

The proof was based on an idea from the author's earlier work [11].

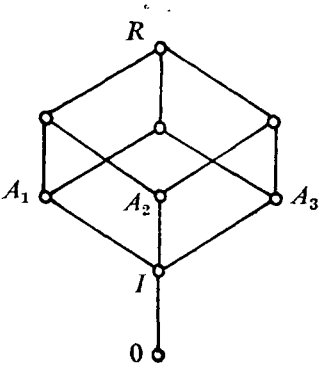
Solvability in Theorem 2.2 cannot be replaced by nilpotency:

2.3. Proposition. *If the lattice of normal subgroups of a finite nilpotent group G is distributive, then G is cyclic, and the lattice is a direct product of chains.*

Proof. Let $\Phi(G)$ denote the Frattini subgroup of G. Then $G/\Phi(G)$ is abelian, it is a direct product of some cyclic groups of prime orders. If two generators had the same prime order then the lattice of (normal) subgroups of $G/\Phi(G)$ would not be distributive. Hence $G/\Phi(G)$ is cyclic, therefore G is a cyclic group itself. Now the lattice of normal subgroups of G is isomorphic to the lattice of divisors of the order of G.

3. Rings. For rings the answer to our representation problem is negative:

3.1. Proposition. *No finite associative ring has congruence lattice (i.e. lattice of ideals) isomorphic to*



Before proving this proposition, let us note that the finiteness of the ring is a crucial requirement, since the following is true:

3.2. Theorem (K. H. Kim and F. W. Roush [6]). *Every finite distributive lattice is isomorphic to the lattice of ideals of some (regular) ring.*

Proof of Proposition 3.1. By way of contradiction assume that a finite ring R has the indicated lattice of ideals. Let I, A_1, A_2, A_3 be ideals of R as shown. We shall reach the final contradiction in several steps. The first observation is obvious:

1) $R/I=A_1/I\oplus A_2/I\oplus A_3/I$, the direct summands are simple rings, in particular any of them is either a ring with unit or a zeroring of prime order.

2) $I^2=0$.

Let $J(R)$ be the Jacobson radical of R. Since $R/J(R)$ is semisimple, its ideal lattice is boolean. Hence we have $J(R)\supseteq I$. So I is a nilpotent ideal, and by the minimality of I it follows that $I^2=0$.

3) If A_i/I is a ring with unit then there is an idempotent $e_i\in A_i$ for which e_i+I is the unit of A_i/I.

Let $a+I$ be the unit of A/I (for simplicity we leave out the index i in the proofs of steps 3, 4 and 5). Then $a^2=a+t$ for some $t\in I$. Now the required element is $e=a+t-2at$.

4) In the situation of step 3, either $e_iI=0$ or $e_ix=x$ for all $x\in I$.

We show that eI is an ideal of R. Obviously, $eIR\subseteq eI$. On the other hand, since e is central in R/I, $ReI\subseteq(eR+I)I\subseteq eI+0=eI$. If $eI\neq 0$ then $eI=I$ and by the finiteness of I the left multiplication by e induces a permutation on I. Since e is idempotent, it is the identical permutation.

5) In the situation of step 3, $e_iI=0$ and $Ie_i=0$ cannot hold simultaneously. Let $x\in A$ be an arbitrary element. Then $x-ex\in I$ and $Ie=0$ implies $(x-ex)e=0$. So $xe=exe$ and symmetrically $ex=exe$, therefore $xe=ex$ for all $x\in A$. Hence $eA=Ae$ is both right and left ideal of R. We have $eA\neq 0$, since $e=e^2\in eA$. However, $eA\cap I=0$, as for $ex\in eA\cap I$ it follows that $ex=e(ex)\in eI=0$. This contradiction proves that $eI=0=Ie$ is impossible.

6) If A_i/I and A_j/I are rings with unit $(i\neq j)$ then $e_iI=I$ and $e_jI=I$ cannot hold simultaneously.

Otherwise, by step 4 we would have $e_ix=x=e_jx$ for all $x\in I$, hence $e_i-e_j\in \mathrm{Ann}_l I$. This left annihilator is an ideal, but the least ideal of R containing e_i-e_j is A_i+A_j which contains e_i and e_j as well, a contradiction.

7) If A_i/I is a ring with unit and A_j/I is a zeroring then $e_iI=0$.

If not, then $e_ix=x$ for all $x\in I$ by step 4. In particular, $e_iI=e_iA_j=I$. Since A_j/I is a zeroring, $A_j^2\subseteq I$, $IA_j^2\subseteq I^2=0$ hence also $IA_j=0$. Define $B=\{y\in A_j: e_iy=0\}$. B is an ideal of R, since $RB\subseteq RA_j\subseteq A_j$, $e_iRB\subseteq(Re_i+I)B\subseteq Re_iB+IA_j=0$ and $BR\subseteq A_jR\subseteq A_j$, $e_iBR=0$. For the left multiplication by e_i, $\lambda: A_j\to A_j$, $\lambda(y)=e_iy$ we have $\lambda^2=\lambda$, hence $A_j=\mathrm{Ker}\,\lambda\oplus\mathrm{Im}\,\lambda=B\oplus I$. This is a contradiction.

8) A_i/I and A_j/I $(i\neq j)$ cannot be both zerorings.

Since R is directly indecomposable, its additive group is a p-group for some prime p. Hence A_i/I and A_j/I would be isomorphic zerorings and thus there would be another $p-1$ ideals between I and A_i+A_j.

9) Conclusion. We have already eliminated all possible cases. If all of A_1/I, A_2/I, A_3/I are rings with unit then step 6 implies that $e_iI=0$ for at least two indices i and symmetrically $Ie_j=0$ for at least two j's. Hence for some i we have $e_iI=0=Ie_i$ contrary to step 5. By step 8, there cannot be more than one zerorings among the direct summands. If A_i/I is a ring with unit and A_j/I is a zeroring, then step 7 gives that $e_iI=0$ and by symmetry $Ie_i=0$ as well, again a contradiction by step 5.

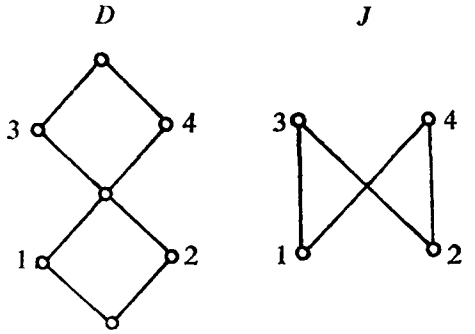
4. Modules. First we present a very elementary construction of a module with given finite distributive lattice of submodules. A similar result for modules over group algebras was obtained by S. M. Vovsi [20].

4.1. Proposition. *Every finite distributive lattice is isomorphic to the congruence lattice (i.e. lattice of submodules) of a finite module.*

Proof. Recall the definitions of n and J in the introduction. Let F be an arbitrary finite field, $M=F^n$, R the subspace of n by n matrices over F with row and column indices from J spanned by the elementary matrices e_{ij} for $i\leqq j$ in J (clearly, R is a ring), and let R act on M in the obvious way. We claim that the submodules of the R-module M are the F-subspaces spanned by the vectors e_i, $i\in I$, for a hereditary subset I of J. Indeed, let N be a submodule, $m\in N$, $m=\sum_{i\in J} f_ie_i$, $f_i\in F$,

then for $f_i \neq 0$ we get $e_i=(1/f_i)e_{ii}m \in N$. Hence N is spanned by some of the e_i's. Since $e_{ij} \in R$ for $i \leqq j$ (in J), it follows that $I=\{i \in J: e_i \in N\}$ is hereditary. The converse is obvious.

4.2. Example.



R

is the ring of all

matrices of the form

$$\begin{bmatrix} a_{11} & 0 & a_{13} & a_{14} \\ 0 & a_{22} & a_{23} & a_{24} \\ 0 & 0 & a_{33} & 0 \\ 0 & 0 & 0 & a_{44} \end{bmatrix} \quad (a_{ij} \in F)$$

Notice that the ring R depends on the lattice D. If we would like to have modules over the same ring we could take the direct sum of all these rings, or the free (non-commutative) ring with infinitely many generators. It would be desirable to choose a finite ring, however, it is not possible.

4.3. Proposition. *For any finite ring R, there exists a finite distributive lattice D (in fact a chain) such that no finite R-module has lattice of submodules isomorphic to D.*

Proof. Let $J(R)$ be the Jacobson radical of R. Since R is finite, $J(R)$ is nilpotent, i.e. $J(R)^r=0$ for some positive integer r, and $R/J(R)$ is semisimple. Suppose that the submodules of the R-module M form a chain $0=M_0<M_1<\ldots<M_{n-1}<M_n=M$. On one hand, $J(R)$ annihilates M_{i+1}/M_i $(i=0, 1, \ldots, n-1)$, since it is a minimal R-module; on the other hand, if M_j/M_i $(0 \leqq i<j \leqq n)$ is annihilated by $J(R)$ then it can be regarded as an $R/J(R)$-module, hence it is semisimple, which forces $j=i+1$. Thus we have $J(R) \cdot M_{i+1}=M_i$ $(i=0, 1, \ldots, n-1)$. Now it follows by induction that

$$J(R)^r \cdot M = \begin{cases} M_{n-r} & \text{if } n-r>0, \\ 0 & \text{otherwise.} \end{cases}$$

Since $J(R)^r=0$, we have $n-r \leqq 0$, $n \leqq r$. Hence no chain longer than r is representable as the congruence lattice (i.e. lattice of submodules) of an R-module.

5. Unary algebras. The 1-unary algebras with distributive congruence lattices have been determined by D. P. Egorova [2]. In order to formulate her result we need some notation. Let $(A; f)$ be a 1-unary algebra, for $a \in A$ we put $f^0(a)=a$,

$f^1(a)=f(a)$, $f^{i+1}(a)=f(f^i(a))$, $i=1, 2, \ldots$. On the set $\mathbf{Z}\cup\{\infty\}$ we define the operation f by $f(n)=n+1$ for $n\in\mathbf{Z}$ and $f(\infty)=\infty$. According to [2] the isomorphism types of 1-unary algebras with distributive congruence lattices are the following:

(1) $$\langle a \mid f^{t+r}(a) = f^t(a)\rangle, \quad t \geqq 0, r \geqq 1;$$

(2) $$\langle a, b \mid f^{t+r}(a) = f^t(a),\ f^s(b) = b\rangle,$$
$$t \geqq 0, \quad r \geqq 1, \quad s \geqq 1 \quad \text{and} \quad \text{g.c.d.}(r, s) = 1;$$

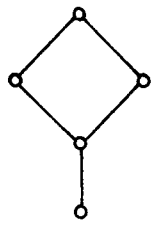
(3) four infinite algebras: $\mathbf{Z}\cup\{\infty\}$, $\mathbf{Z}$, $\mathbf{N}\cup\{\infty\}$, $\mathbf{N}$.

It is quite easy to determine their congruence lattices. Let $C(t)$ denote the chain of length t (i.e. having $t+1$ elements), $D(r)$ the lattice of divisors of r, and $L+1$ the lattice obtained from the lattice L by adding a new maximal element to it. Restricting our attention to finite algebras, we obtain that the congruence lattice in case (1) is isomorphic to $C(t)\times D(r)$, and in case (2) to $C(t)\times(D(rs)+1)$. Hence we have:

5.1. Proposition. *If the finite distributive lattice D is isomorphic to the congruence lattice of a finite 1-unary algebra, then either D is a direct product of chains or $D\cong C_0\times(C_1\times\ldots\times C_k+1)$ for some finite chains $C_0, C_1, \ldots, C_k$.*

Now it is easy to exhibit a finite distributive lattice which is not representable as the congruence lattice of a (finite) 1-unary algebra, cf. [5], p. 209, where this example is credited to J. Johnson and R. L. Seifert.

5.2. Corollary. *No finite 1-unary algebra has congruence lattice isomorphic to*



On the other hand, two unary operations already suffice.

5.3. Theorem. *Every finite distributive lattice is isomorphic to the congruence lattice of a finite 2-unary algebra.*

Proof. For the sake of simplicity suppose $J=\{1, 2, \ldots, n\}$, and let $J'=\{0, 1, \ldots, n\}$. Choose pairwise different primes $p_1, p_2, \ldots, p_n>n$, and let $p_0=1$. For the base set of the algebra we take $A=\{(j, k): j\in J',\ 0\leqq k\leqq p_j-1\}$, and we

define the two unary operations by

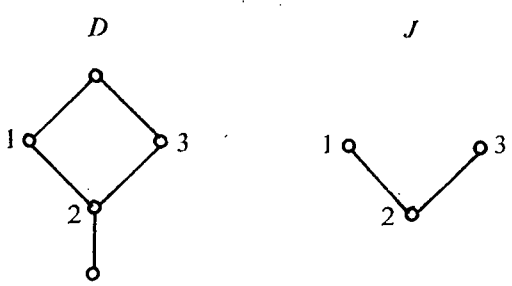
$$f((j,k)) = \begin{cases} (j,k+1) & \text{if } k \leqq p_j - 2 \\ (j,0) & \text{if } k = p_j - 1 \end{cases}$$

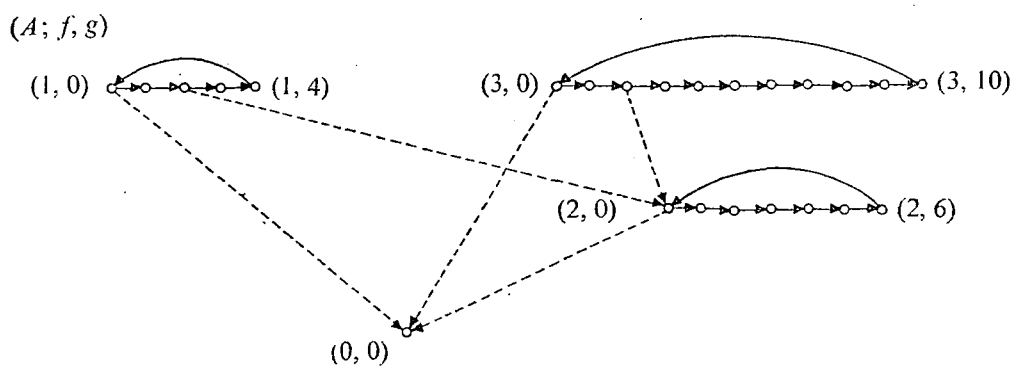
and

$$g((j,k)) = \begin{cases} (k,0) & \text{if } k = 0 \text{ or } k < j \text{ in } J \\ (j,k) & \text{otherwise.} \end{cases}$$

We claim that any nontrivial congruence of the algebra $(A; f, g)$ has one nontrivial class $\{(j,k): j \in I',\ 0 \leqq k \leqq p_j - 1\}$ where $I' = \{0\} \cup I$ for some hereditary subset I of J, the other classes are singletons. The proof of this statement is straightforward and left to the reader. Hence we see that $\mathrm{Con}(A; f, g) \cong D$.

5.4. Example.





Notation: $f \longrightarrow$, $g \dashrightarrow$ (fixed points are not denoted)

P. P. PÁLFY and P. PUDLÁK [12] showed that every finite lattice is representable as a 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. (In fact, the interval $[H, G]$ is isomorphic to the congruence lattice of the unary algebra on the set of

left cosets of the subgroup H in the group G, with the operations being the permutations defined by left multiplications by the elements of G.) For finite distributive lattices we construct suitable intervals by applying Silcock's theorem (see 2.1). J. TŮMA [19] has given another construction recently.

5.5. Proposition. *Every finite distributive lattice is isomorphic to the congruence lattice of a unary algebra where the operations form a transitive permutation group.*

Proof. Let G be a finite group with $\mathrm{Con}\, G \cong D$ (see Theorem 2.1). Take the diagonal subgroup $\Delta = \{(g, g): g \in G\}$ of $G \times G$. It is easy to prove that the subgroups K containing Δ have the form $K = \Delta \cdot (K_1 \times 1)$, where $K_1 \lhd G$, $K_1 \times 1 = K \cap (G \times 1)$. Hence the interval $[\Delta, G \times G] \cong \mathrm{Con}\, G \cong D$.

6. Type. In virtue of Corollary 5.2 not every finite distributive lattice is representable as the congruence lattice of a 1-unary algebra. However, if the type contains at least two operations then Theorem 5.3, while if it contains an operation which is at least binary then Theorem 2.1 is applicable. Hence we obtain:

6.1. Corollary. *Let us given any type except the 1-unary. Then every finite distributive lattice is isomorphic to the congruence lattice of a finite algebra of the given type.*

Acknowledgments. The author is indebted to E. T. Schmidt and E. Fried for helpful comments.

References

[1] G. Birkhoff, *Lattice theory*, Amer. Math. Soc. Colloq. vol. 25 (New York, 1948).
[2] D. P. Egorova, The congruence lattice of a unary algebra, in: *Uporjad. Množestva Rešetki*, vol. 5, Izd. Saratovsk. Univ. (Saratov, 1978); pp. 11—44. (Russian)
[3] R. Freese, Congruence lattices of finitely generated modular lattices, in: *Proc. Lattice Theory Conf.*, Univ. Ulm (Ulm, 1975); pp. 62—70.
[4] G. Grätzer and E. T. Schmidt, On congruence lattices of lattices, *Acta Math. Acad. Sci. Hungar.*, **13** (1962), 179—185.
[5] B. Jónsson, *Topics in universal algebra*, Lecture Notes in Math. 250, Springer (Berlin, 1972).
[6] K. H. Kim and F. W. Roush, Regular rings and distributive lattices, *Commun. Algebra*, **8** (1980), 1283—1290.
[7] R. Kochendörffer, Über treue irreduzible Darstellungen endlicher Gruppen, *Math. Nachr.*, **1** (1948), 25—39.
[8] J. Kuntzmann, Contribution a l'étude des chaines principales d'un groupe fini, *Bull. Sci. Math.* (2), **71** (1947), 155—164.
[9] R. McKenzie, Finite forbidden lattices, in: *Universal Algebra and Lattice Theory* (Proc. Conf. Puebla 1982), Lecture Notes in Math. 1004, Springer (Berlin, 1983); pp. 176—205.
[10] P. P. Pálfy, Unary polynomials in algebras. I, *Algebra Universalis*, **18** (1984), 262—273.

[11] P. P. PÁLFY, On partial ordering of chief factors in solvable groups, *Manuscripta Math.*, **55** (1986), 219—232.

[12] 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.

[13] P. PUDLÁK, Distributivity of strongly representable lattices, *Algebra Universalis*, **7** (1977), 85—92.

[14] R. QUACKENBUSH and B. WOLK, Strong representation of congruence lattices, *Algebra Universalis*, **1** (1971/72), 165—166.

[15] E. T. SCHMIDT, *Kongruenzrelationen algebraischer Strukturen*, VEB Deutscher Verlag d. Wiss. (Berlin, 1969).

[16] E. T. SCHMIDT, Every finite distributive lattice is the congruence lattice of some modular lattice, *Algebra Universalis*, **4** (1974), 49—57.

[17] E. T. SCHMIDT, *A survey on congruence lattice representations*, Teubner (Leipzig, 1982).

[18] H. L. SILCOCK, Generalized wreath products and the lattice of normal subgroups of a group, *Algebra Universalis*, **7** (1977), 361—372.

[19] J. TŮMA, Some finite congruence lattices. I, preprint, 1985.

[20] S. M. VOVSI, Lattices of invariant subspaces of group representations, *Algebra Universalis*, **12** (1981), 221—223.

MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
PF. 127
1364 BUDAPEST, HUNGARY