CONGRUENCE LATTICES OF FINITE CHAINS WITH ENDOMORPHISMS

Jaroslav Ježek, Václav Slavík, Praha

(Received November 19, 1999)

Abstract. Characterization of congruence lattices of finite chains with either one or two endomorphisms is given.

Keywords: chain, congruence lattice

MSC 2000: 06B10

1. Introduction

The aim of this paper is to prove that every finite distributive lattice is isomorphic to the congruence lattice of a finite chain with two endomorphisms (these are algebras with one binary and two unary operations), and to characterize those finite lattices that are isomorphic to the congruence lattice of a finite chain with one endomorphism (not every finite distributive lattice can be represented in this way). Moreover, we prove general results on congruence lattices of chains with an arbitrary set of endomorphisms. Some of these general results were obtained in cooperation with R. Wille.

The techniques used are those of universal algebra, as explained in [2], and those of context theory; see [3] and [4]. By a context we mean a triple (A,B,I) where A,B are sets and $I \subseteq A\times B$. For a subset S of A, the extent of S is the subset $\{b\in B\colon\ (a,b)\in I \text{ for all } a\in S\}$ of B. Similarly, for a subset T of B, the intent of T is the subset $\{a\in A\colon\ (a,b)\in I \text{ for all } b\in T\}$ of A. We obtain a Galois correspondence between subsets of A and subsets of B. By a concept of (A,B,I) we mean a pair

While working on this paper the first author was partially supported by the Grant Agency of the Charles University (grant GAUK 15/1997) and the second author was partially supported by the Grant Agency of the Czech Republic, (grant GAČR 201/99/0263).

(S, T) such that T is the extent of S and S is the intent of T. For a given context, the lattice of concepts is isomorphic to the lattice of intents and antiisomorphic to the lattice of extents.

2. Finite chains with arbitrary sets of endomorphisms

Given a finite ordered set $A = (A, \leqslant)$, we denote by $A + 0$ and $A + 1$ the ordered sets obtained from A by adding a new least element and a new greatest element, respectively. The order relation of both $A+0$ and $A+1$ will be denoted by the same symbol $\leqslant$ as that of A, and the added elements by 0 and 1 if there is no confusion. If A is a chain then both $A+0$ and $A+1$ are chains, too; in this case we will denote the predecessor and the cover of an element $a \in A$ by $a - 1$ and $a + 1$, respectively.

Let a finite chain $A = (A, \leqslant)$ be given. The set of endomorphisms of $A + 0$ (i.e., isotone mappings of $A + 0$ into itself) will be denoted by $E(A, \leqslant)$, or simply by E. Let us define a context $(E, A \times A, I)$ by

$$(f, (a, b)) \in I \quad \text{iff either } f(a-1),\ f(a) \leqslant b - 1 \text{ or } f(a-1),\ f(a) \geqslant b.$$

Notice that

$$(f, (a, b)) \notin I \quad \text{iff} \quad f(a-1) \leqslant b - 1 < b \leqslant f(a).$$

Theorem 1. *Let a finite chain $A = (A, \leqslant)$ be given. All subsets of $A \times A$ are intents of the context $(E, A \times A, I)$. On the other hand, a subset F of E is an extent iff it satisfies the following condition: if $f \in E$ is an endomorphism such that, for any $a, b \in A$, $f(a-1) \leqslant b-1 < b \leqslant f(a)$ implies the existence of a $g \in F$ with $g(a-1) \leqslant b-1 < b \leqslant g(a)$, then $f \in F$.*

Proof. Denote the intent corresponding to a subset F of E by F' and the extent corresponding to a set $R \subseteq A \times A$ by R'. Let $R \subseteq A \times A$. In order to prove that R is an intent, we need to prove that if $(a, b) \in R''$ then $(a, b) \in R$. Define an endomorphism f by $f(x) = b - 1$ for $x \leqslant a - 1$ and $f(x) = b$ for $x \geqslant a$. If $(a, b) \notin R$ then it is easy to see that $f \in R'$; indeed, if $(c, d) \in R$ then $(c, d) \neq (a, b)$ and so either $f(c-1), f(c) \leqslant d-1$ or $f(c-1), f(c) \geqslant d$; but then $(a, b) \in R''$ yields $(f, (a, b)) \in I$, a contradiction. The condition in the last assertion is a reformulation of $F'' \subseteq F$. $\square$

A subset F of E is said to be rich if it is an extent of the investigated context, i.e., if it satisfies the condition formulated in Theorem 1. We get that the lattice of rich subsets of E is antiisomorphic to the Boolean lattice of all subsets of $A \times A$. However, we shall be more interested in certain lattices that are subsets of these two lattices.

By a submonoid of E we mean a subset containing the identity and closed under superposition.

Theorem 2. *Let A be a finite chain. If F is a submonoid of E and R is the corresponding intent of the context $(E, A\times A, I)$ then $(A\times A)\setminus R$ is a quasiorder on A. If $R\subseteq A\times A$ is a complement of a quasiorder on A then the corresponding intent is a rich submonoid. Consequently, if (F,R) is a concept then F is a rich submonoid iff $(A\times A)\setminus R$ is a quasiorder on A.*

Proof. Let F be a submonoid and $R=\{(a,b)\colon \forall f\in F\ (f,(a,b))\in I\}$. We have $(a,b)\in(A\times A)\setminus R$ iff there exists an $f\in F$ with $f(a-1)\leqslant b-1<b\leqslant f(a)$. The reflexivity of $(A\times A)\setminus R$ is a consequence of $\mathrm{id}_A\in F$, while the transitivity follows from F being closed under superposition.

Now let $R=(A\times A)\setminus\sqsubseteq$ for a quasiorder $\sqsubseteq$ on A and

$$\begin{aligned} F&=\{f\in E\colon \forall(a,b)\in R(f,(a,b))\in I\}\\ &=\{f\in E\colon \forall a,b\in A\ (f(a-1)\leqslant b-1<b\leqslant f(a)\to a\sqsubseteq b)\}.\end{aligned}$$

Easily, $\mathrm{id}_A\in F$. If $f,g\in F$ and $gf(a-1)\leqslant b-1<b\leqslant gf(a)$ then there exists an element c with $f(a-1)\leqslant c-1<c\leqslant f(a)$ and $g(c-1)\leqslant b-1<b\leqslant g(c)$; we get $a\sqsubseteq c$ and $c\sqsubseteq b$ and hence $a\sqsubseteq b$. □

Theorem 3. *Let A be a finite chain. Then there exists an isomorphism of the lattice of rich submonoids of E onto the lattice of quasiorders on A. If F is a submonoid of E then the quasiorder $\sqsubseteq$ corresponding to the rich submonoid generated by F can be defined as follows:*

$$a\sqsubseteq b \text{ iff there exists an } f\in F \text{ with } f(a-1)\leqslant b-1<b\leqslant f(a).$$

If $\sqsubseteq$ is a quasiorder on A then the corresponding rich submonoid F can be defined by

$$f\in F \text{ iff } f(a-1)\leqslant b-1<b\leqslant f(a) \text{ implies } a\sqsubseteq b \text{ for any } a,b\in A.$$

Proof. It is a consequence of Theorem 2. □

We are interested in the congruence lattices of $(A+0,\leqslant,F)$ for various subsets F of E. By a congruence of $(A+0,\leqslant)$ we mean a congruence of the corresponding lattice, or an equivalence all the blocks of which are intervals; a congruence of $(A+0,\leqslant,F)$ must preserve, moreover, all the unary operations from F.

By an order filter of a quasiordered set $(A,\sqsubseteq)$ we mean a subset $S\subseteq A$ such that $a\sqsubseteq b$ and $a\in S$ imply $b\in S$. Order ideals are defined dually.

Theorem 4. *Let $A = (A, \leqslant)$ be a finite chain, F be a subset of E and $\sqsubseteq$ be the quasiorder on A corresponding (under the isomorphism described in Theorem 3) to the rich submonoid generated by F; put $A_0 = A + 0$. The congruence lattice of $(A + 0, \leqslant, F)$ is isomorphic to the lattice of order filters of $(A, \sqsubseteq)$.*

P r o o f. We can assume that F is a submonoid. Define a context $(A_0 \times A_0, A, I_F)$ as follows: $((x, y), a) \in I_F$ iff

$$\text{for any } f \in F, \text{ either } f(x),\ f(y) \leqslant a - 1 \text{ or } f(x),\ f(y) \geqslant a.$$

Clearly, $a \sqsubseteq b$ is equivalent with $((a-1, a), b) \notin I_F$. For $S \subseteq A_0 \times A_0$ put $S^{\#} = \{a \in A\colon\ \forall (x, y) \in S\ \ ((x, y), a) \in I_F\}$. For $T \subseteq A$ put $T^{\#} = \{(x, y) \in A_0 \times A_0\colon\ \forall a \in T\ \ ((x, y), a) \in I_F\}$.

It is easy to see that $T^{\#}$ is a congruence of $(A_0, \leqslant, F)$ for any $T \subseteq A$. If S is a congruence of $(A_0, \leqslant, F)$ then

$$S^{\#} = \{a \in A\colon\ \forall (x, y) \in S\ x, y \leqslant a - 1 \text{ or } x, y \geqslant a\}$$

and one can easily prove $S^{\#\#} = S$.

Let us prove that if S is a congruence of $(A_0, \leqslant, F)$ then $S^{\#}$ is an order ideal of $(A, \sqsubseteq)$. For this we need to show that if $((x, y), a) \in I_F$ and $b \sqsubseteq a$ then $((x, y), b) \in I_F$; it is sufficient to consider the case $x \leqslant y$. As $b \sqsubseteq a$, there exists an $f \in F$ with $f(b-1) \leqslant a - 1 < a \leqslant f(b)$. If $((x, y), b) \notin I_F$ then $g(x-1) \leqslant b - 1 < b \leqslant g(y)$ for some $g \in F$; but then $fg(x) \leqslant f(b-1) \leqslant a - 1 < a \leqslant f(b) \leqslant fg(y)$ and we get a contradiction with $fg \in F$ and $((x, y), a) \in I_F$.

Let us prove $T^{\#\#} = T$ for any order ideal T of $(A, \sqsubseteq)$. We need to prove that if $a \in T^{\#\#}$ then $a \in T$. If $a \in T^{\#\#}$ then $(a-1, a) \notin T^{\#}$ (since otherwise we would have $((a-1, a), a) \in I_F$, which is impossible) and so there exist an element $b \in T$ and an endomorphism $f \in F$ with $f(a-1) \leqslant b - 1 < b \leqslant f(a)$, i.e., $a \sqsubseteq b$; but then $a \in T$.

These observations show that the concept lattice of $(A_0 \times A_0, A, I_F)$ is isomorphic to the congruence lattice of $(A_0, \leqslant, F)$ and at the same time antiisomorphic to the lattice of order ideals of $(A, \sqsubseteq)$; consequently, it is isomorphic to the lattice of order filters of $(A, \sqsubseteq)$. $\square$

Theorem 5. *Every finite distributive lattice is isomorphic to the congruence lattice of a finite chain with two endomorphisms.*

Proof. As follows from Birkhoff [1], every finite distributive lattice is isomorphic to the lattice of order filters of a finite ordered set $(A, \sqsubseteq)$. Denote by n the cardinality of A and take an ordering $a_1, \dots, a_n$ of the elements of A. For any nonnegative integer i put $a_i = a_{p(i)}$ where $p(i)$ is the number in $\{1, \dots, n\}$ which is congruent with i modulo n.

Consider the decomposition of the set of positive integers into the segments $S_k = \{k+1, \dots, k+n\}$ $(k = 0, 1, 2, \dots)$. We will call a segment S_k regular if either $k = 0$ or $k = n^j + n^{j-1} + \dots + n + j + 2$ for some $j \geqslant 0$; all the other segments will be called singular. So, the first segment S_0 is regular, then comes one singular segment, the next one is regular, the next n ones are singular, the next one is regular, the next n^2 segments are singular, and so on.

By induction let us define a positive integer $q(i)$ for any positive integer i in the following way. If i belongs to a regular segment S then put $q(i) = i + c$ where c is the least positive multiple of n such that $S + c$ is again regular. Now, let i belong to a singular segment S. Denote by R_0 the last regular segment preceding S and by R_1 and R_2 the next two regular segments. There exists an $m \geqslant 1$ such that there are exactly n^m elements in the singular segments between R_0 and R_1 and at the same time there are exactly n^m singular segments between R_1 and R_2. If i stands as the j-th among the n^m elements, we will define $q(i)$ to be an element of the j-th singular segment T between R_1 and R_2. Which element? There are n elements to choose from. Well, first of all we demand $q(i)$ to be such that $a_{q(i)} \sqsubseteq a_i$; this can be always accomplished by taking $q(i)$ to be the element of T with $a_q(i) = a_i$; but we will prefer to take, whenever possible, an element giving us a new pair $(a_{q(i)}, a_i)$ in the following sense. If there exists an element $a \in A$ such that $a \sqsubseteq a_i$ and $(a, a_i) \neq (a_{q(j)}, a_j)$ for any $j < i$, take one such element a and define $q(i)$ to be the element of T with $a_{q(i)} = a$; only if such an element does not exist, let $q(i)$ be the element of T with $a_{q(i)} = a_i$.

Clearly, q is an increasing mapping with the property $q(i) > i$ for all i. Since $q(i)$ was defined in such a way that $a_{q(i)} \sqsubseteq a_i$ is a new relation whenever possible, a positive integer must exist starting from which all the finitely many pairs $(a, b) \in A \times A$ with $a \sqsubseteq b$ were already exhausted as the new ones. So, there exists a regular segment H such that for any $(a, b) \in A \times A$ with $a \sqsubseteq b$ there is an i with $q(i) < h$ for $h \in H$ and $(a, b) = (a_{q(i)}, a_i)$. Denote by s the largest element of H and by C the chain $\{1, 2, \dots, s\}$ (with respect to the usual ordering of natural numbers); we have $C + 0 = \{0, 1, \dots, s\}$.

Define two endomorphisms f, g of $C + 0$ as follows: $f(x) = x + n$ for $x \leqslant s - n$; $f(x) = s$ for $x > s - n$; $g(x) = 0$ for $x < q(1)$ (i.e., for $x \leqslant 2n$); if $x \geqslant q(1)$ then put $g(x) = i$ where i is the integer with $q(i) \leqslant x < q(i + 1)$.

Denote by F the submonoid generated by f, g and by $\sqsubseteq'$ the quasiorder on C corresponding to F under the isomorphism described in Theorem 3. Put

$$R_f = \{(a, b) \in C \times C\colon\ f(a - 1) \leqslant b - 1 < b \leqslant f(a)\},$$
$$R_g = \{(a, b) \in C \times C\colon\ g(a - 1) \leqslant b - 1 < b \leqslant g(a)\}.$$

It is clear that $\sqsubseteq'$ is just the reflexive and transitive closure of $R_f \cup R_g$.

If $a \in C$ is such that $a + n \in C$ then it is clear that $(a, a + n) \in R_f$. If S and $S + c$ are two neighboring regular segments both contained in C then clearly $(a, a - c) \in R_g$ for any $a \in S + c$. From these two observations and from the fact that the segments $\{1, \ldots, n\}$ and $\{s - n + 1, \ldots, s\}$ are both regular it follows that whenever $i, j \in C$ and $i \equiv j \bmod n$ then $i \sqsubseteq' j$ and $j \sqsubseteq' i$. Clearly, $(i, j) \in R_g$ implies $a_i \sqsubseteq a_j$; and it now follows from the choice of the segment H that whenever $a \sqsubseteq b$ then there exist $i, j \in C$ with $a = a_i$, $b = a_j$ and $(i, j) \in R_g$. We get $i \sqsubseteq' j$ iff $a_i \sqsubseteq a_j$. But then, the lattice of order filters of $(C, \sqsubseteq')$ is isomorphic to the lattice of order filters of $(A, \sqsubseteq)$. By Theorem 4, the congruence lattice of $(C + 0, \leqslant, f, g)$ is isomorphic to the lattice of order filters of $(C, \sqsubseteq')$. □

4. One endomorphism

By a forest we will mean an ordered set, any principal ideal of which is a chain.

Theorem 6. *The following three conditions are equivalent for a finite lattice L:*

1. *L is isomorphic to the congruence lattice of an at least two-element finite chain with one endomorphism;*
2. *L is isomorphic to the lattice of order filters of a finite forest;*
3. *L belongs to the smallest class $\mathbf{L}$ of finite lattices closed under isomorphic images, containing the two-element lattice and such that whenever $L_1, L_2 \in \mathbf{L}$ then $L_1 \times L_2 \in \mathbf{L}$ and $L_1 + 1 \in \mathbf{L}$.*

Proof. (1) implies (2). Let $A = (A, \leqslant)$ be a finite chain, f be an endomorphism of $A + 0$ and F be the submonoid generated by f (so that $F = \{f^k\colon\ k \geqslant 0\}$). By Theorem 3 there is a quasiorder $\sqsubseteq$ on A corresponding to F and we need only to prove that $(A, \sqsubseteq)$ is a forest. Define a relation R by $(a, b) \in R$ iff $a \neq b$ and $f(a-1) \leqslant b-1 < b \leqslant f(a)$. Then $a \sqsubseteq b$ iff there exists a sequence $a = a_0, a_1, \ldots, a_k = b$ ($k \geqslant 0$)

such that $(a_0, a_1) \in R, \dots, (a_{k-1}, a_k) \in R$; it is easy to see that in the case $a_0 < a_1$ we have $a_0 < a_1 < a_2 < \dots$, while in the case $a_0 > a_1$ we have $a_0 > a_1 > a_2 > \dots$. It follows that $\sqsubseteq$ is an order. It is a forest order, since $(a, c) \in R$ and $(b, c) \in R$ clearly imply $a = b$.

(2) implies (1). Let $(A, \sqsubseteq)$ be a forest. Then A can be decomposed into the disjoint union of its maximal subtrees $T_1, \dots, T_n$ (i.e., principal filters generated by the minimal elements of $(A, \sqsubseteq)$). We can define a linear ordering $\leqslant$ on A in such a way that all the components $T_1, \dots, T_n$ become segments and for any two elements a, b of a component T_i we have $a < b$ whenever either the principal ideal of T_i generated by a has smaller cardinality than the one generated by b or the two cardinalities (the heights of a and b) are the same and the predecessor of a (with respect to $\sqsubseteq$) is less (with respect to $<$) than the predecessor of b. For $a \in A$ denote by S_a the set of the elements covering a in $(A, \sqsubseteq)$; then S_a is a segment in $(A, \leqslant)$. Define an endomorphism f of $(A + 0, \leqslant)$ as follows: $f(0) = 0$; if $a \in A$ and S_a is nonempty, let $f(a)$ be the largest (with respect to $\leqslant$) element of S_a; if S_a is empty, put $f(a) = f(a - 1)$ (where $a - 1$ is the element covered by a in $(A + 0, \leqslant)$; so, this definition is inductive). For any $a \in A$ it is easy to see that the set of the elements b satisfying $f(a - 1) \leqslant b - 1 < b \leqslant f(a)$ coincides with the set of the covers of a in $(A, \sqsubseteq)$. From this it follows that $\sqsubseteq$ coincides with the quasiorder corresponding to the rich submonoid generated by f; by Theorem 3, the congruence lattice of $(A+0, \leqslant, f)$ is isomorphic to the lattice of order filters of $(A, \sqsubseteq)$.

The equivalence of (2) with (3) is a consequence of the following three simple observations:

(i) The lattice of order filters of the one-element forest is the two-element lattice.

(ii) If A is a forest with the least element 0 and $A \neq \{0\}$ then the lattice of order filters of A is isomorphic to $L + 1$ where L is the lattice of order filters of the forest $A \setminus \{0\}$.

(iii) If A is a forest which can be decomposed into the disjoint union of two proper nonempty order filters A_1 and A_2 then the lattice of order filters of A is isomorphic to the product of the lattice of order filters of A_1 and the lattice of order filters of A_2. $\square$

References

[1] *G. Birkhoff*: Rings of sets. Duke Math. J. *3* (1937), 443–454.

[2] *R. McKenzie, G. McNulty, W. Taylor*: Algebras, Lattices, Varieties, Volume I. Wadsworth&Brooks/Cole, Monterey, CA, 1987.

[3] *R. Wille*: Restructuring lattice theory: an approach based on hierarchies of concepts. Ordered Sets (I. Rival, ed.). Reidel, Dordrecht, 1982, pp. 445–470.

[4] *R. Wille*: Finite distributive lattices as concept lattices. THD-Preprint Nr. 860, 1984.

Authors' addresses: *Jaroslav Ježek*, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Republic, e-mail: `jezek@karlin.mff.cuni.cz`, *Václav Slavík*, Czech Agricultural University, Kamýcká 129, 165 21 Praha 6-Suchdol, Czech Republic, e-mail: `slavik@tf.czu.cz`.