PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 125, Number 12, December 1997, Pages 3457–3463
S 0002-9939(97)04332-3

COMPUTING CONGRUENCE LATTICES OF FINITE LATTICES

RALPH FREESE

(Communicated by Lance W. Small)

Abstract. An inequality between the number of coverings in the ordered set J(**Con L**) of join irreducible congruences on a lattice **L** and the size of **L** is given. Using this inequality it is shown that this ordered set can be computed in time $O(n^2 \log_2 n)$, where $n = |L|$.

This paper is motivated by the problem of efficiently calculating and representing the congruence lattice **Con L** of a finite lattice **L**. Of course **Con L** can be exponential in the size of **L**; for example, when **L** is a chain of length n, **Con L** has 2^n elements. However, since **Con L** is a distributive lattice, it can be recovered easily from the ordered set of its join irreducible elements J(**Con L**). Indeed any finite distributive lattice **D** is isomorphic to the lattice of order ideals of J(**D**) and this lattice is in turn isomorphic to the lattice of all antichains of J(**D**), where the antichains are ordered by $A \ll B$, i.e., for each $a \in A$ there is a $b \in B$ with $a \le b$. If **P** is an ordered set of size n which has N order ideals, then there are straightforward algorithms to find the order ideals of **P** which run in time $O(nN)$; see, for example, [5]. In [10] Medina and Nourine give an algorithm which runs in time $O(dN)$, where d is the maximum number of covers of any element of **P**. Thus we will concentrate on the problem of efficiently finding J(**Con L**).

1. Preliminaries

Throughout this paper **L** denotes a finite lattice. J(**L**) denotes the set of nonzero join irreducible elements and M(**L**) the set of nonunit meet irreducible elements. These sets are ordered by the induced order from **L**. If $a \in \mathrm{J}(\mathbf{L})$, then it has a unique lower cover in **L** which we denote by a_*, and similarly if $q \in \mathrm{M}(\mathbf{L})$, then q^* is the unique upper cover of q. The cover relation is denote by $a \prec b$; $\mathrm{Cg}\,(x, y)$ is the smallest congruence identifying x and y. Throughout the paper we let

$$n = |L| \qquad m = |\,\mathrm{J}(\mathbf{Con\ L})|. \tag{1}$$

For an ordered set **P** we define

$$E_{\le} = \{\langle a, b\rangle : a \le b\}, \qquad e_{\le} = |E_{\le}|,$$
$$E_{\prec} = \{\langle a, b\rangle : a \prec b\}, \qquad e_{\prec} = |E_{\prec}|.$$

Received by the editors June 11, 1996.
1991 *Mathematics Subject Classification.* Primary 06B10, 06B05, 06B15.
Key words and phrases. Congruence lattice, algorithm.
This research was partially supported by NSF grant no. DMS–9500752.

For clarity we sometimes write $E_{\leq}(\mathbf{P})$, etc. Of course $\mathbf{P}$ is determined from its underlying set P and any 'edge' set E with

$$E_{\prec} \subseteq E \subseteq E_{\leq}. \tag{2}$$

The transitive, reflexive closure of any such E is $E_{\leq}$, and $E_{\prec}$ is the smallest set whose transitive, reflexive closure is $E_{\leq}$. $E_{\prec}$ is alternatively known as the *covering relation*, the *transitive reduct*, and the *Hasse diagram* of $\mathbf{P}$. We are most interested in the case $\mathbf{P} = \mathrm{J}(\mathbf{Con\ L})$ and in this paper $E_{\leq} = E_{\leq}(\mathrm{J}(\mathbf{Con\ L}))$, etc.

Chapter XI of [5] contains a discussion of algorithms for lattice theory including algorithms for calculating the congruence lattice of a finite lattice. It shows there is an algorithm which computes the set $\mathrm{J}(\mathbf{Con\ L})$ and an edge set E satisfying (2) in time $O(n^2)$. Of course $\mathbf{L}$ is simple exactly when $\mathrm{J}(\mathbf{Con\ L})$ has only one element, and it is subdirectly irreducible if it has only one minimal element. Since the minimal elements can be found quickly from any E satisfying (2), this gives $O(n^2)$ algorithms for testing the simplicity and subdirect irreducibility of $\mathbf{L}$. However, it does not give the full transitive, reflexive closure, $E_{\leq}$, which is needed for other purposes.

By Theorem 11.2 of [5] we can calculate $E_{\leq}$ from any E satisfying (2) (not just $E_{\prec}$) in time $O(m^2 + me_{\prec} + e_{\leq})$. It follows from part 3 of Lemma 1 below that $m \leq n$ and thus $E_{\leq}$ can be found in time $O(n^3)$. The main purpose of this paper is to improve this bound. We will show that $E_{\leq}$ can be found in time $O(n^2 \log_2 n)$.

In order to do this we explore the connection between $\mathbf{L}$ and $\mathrm{J}(\mathbf{Con\ L})$ more carefully. Namely, given a number $e_{\prec}$, we would like to know how small $\mathbf{L}$ can be with $e_{\prec} = e_{\prec}(\mathrm{J}(\mathbf{Con\ L}))$. In [8] and [9] Grätzer, Lakser, Rival, Schmidt, and Zaguia investigate the relation between m and n. As mentioned above, $m \leq n$. In [8] it is shown that for any ordered set $\mathbf{P}$ of size m there is a lattice $\mathbf{L}$ of size $O(m^2)$ with $\mathrm{J}(\mathbf{Con\ L}) \cong \mathbf{P}$. In [9] examples are given showing that no smaller power of m will work.

For our purposes we need a universal lower bound on the size of $\mathbf{L}$ in terms of $e_{\prec}$. What we show is that given an ordered set $\mathbf{P}$ with $e_{\prec}$ covers, any n-element lattice $\mathbf{L}$ with $\mathrm{J}(\mathbf{Con\ L}) \cong \mathbf{P}$ has

$$e_{\prec} \leq 2n \log_2 n.$$

We give examples showing that in a certain sense this is the best possible and we show how to derive the result of [9] as a corollary.

2. The inequality

We begin with some lemmas. The first is elementary and well known; the second is new; the third is from [9].

Lemma 1. *Let* $\mathbf{L}$ *be a finite lattice.*

1. *If* $a \prec b$ *in* $\mathbf{L}$*, then* $\mathrm{Cg}\,(a, b)$ *is join irreducible.*
2. *If* $\theta \in \mathrm{J}(\mathbf{Con\ L})$*, then there exist* $a \in \mathrm{J}(\mathbf{L})$ *and* $q \in \mathrm{M}(\mathbf{L})$ *with* $\theta = \mathrm{Cg}\,(a, a_*) = \mathrm{Cg}\,(q, q^*)$.
3. *The function* $a \mapsto \mathrm{Cg}\,(a, a_*)$ *maps* $\mathrm{J}(\mathbf{L})$ *onto* $\mathrm{J}(\mathbf{Con\ L})$.

Proof. The first statement follows easily from Dilworth's characterization of lattice congruences, Theorem 10.2 of [1], and does not require that $\mathbf{L}$ be finite. Again by Dilworth's theorem any (completely) join irreducible congruence θ has the form $\mathrm{Cg}\,(x, y)$ for some $x > y$. Since $\mathbf{L}$ is finite, there is a finite maximal chain from x

down to y, and since θ is join irreducible, one of the links of the chain must generate θ. So we may assume $x \succ y$ and if we choose q to be maximal above y but not x, then q is meet irreducible and $\theta = \mathrm{Cg}\,(q, q^*)$, as desired. The third statement follows from the second. □

Lemma 2. *Suppose $\theta \prec \phi$ in $\mathrm{J}(\mathbf{Con\,L})$. Then one of the following holds.*

1. *There is an $a \in \mathrm{J}(\mathbf{L})$ and $x \in L$ with $a \succ a_* > x$ such that $\mathrm{Cg}\,(a, a_*) = \theta$ and $\mathrm{Cg}\,(a_*, x) = \phi$.*
2. *There is a $q \in \mathrm{M}(\mathbf{L})$ and $x \in L$ with $q \prec q^* < x$ such that $\mathrm{Cg}\,(q, q^*) = \theta$ and $\mathrm{Cg}\,(q^*, x) = \phi$.*

Proof. For a, $b \in \mathrm{J}(\mathbf{L})$ and $q \in \mathrm{M}(\mathbf{L})$ we define two relations by

$$a \nearrow q \quad \text{if and only if} \quad a \leq q^* \text{ and } a \nleq q, \tag{3}$$

$$q \searrow b \quad \text{if and only if} \quad q \geq b_* \text{ and } q \ngeq b. \tag{4}$$

Note that $a \nearrow q$ if and only if $a \vee q = q^*$, and $q \searrow b$ if and only if $q \wedge b = b_*$. Define $\mathbf{G}(\mathbf{L}) = \langle V, \to \rangle$ to be the directed graph whose vertex set V is the disjoint union of (copies of) $\mathrm{J}(\mathbf{L})$ and $\mathrm{M}(\mathbf{L})$ and whose relation $\to$ is the union of $\nearrow$ and $\searrow$. Of course this graph determines a quasiorder. Let $\equiv$ be the equivalence relation for this quasiorder: $x \equiv y$ if and only if $x \to^* y$ and $y \to^* x$, where $\to^*$ represents a sequence, possibly of length 0, of edges. We let $\mathbf{G}(\mathbf{L})/{\equiv}$ denote the induced ordered set on the equivalence classes. By Lemma 11.11 of [5] $\mathbf{G}(\mathbf{L})/{\equiv}$ is isomorphic $\mathrm{J}(\mathbf{Con\,L})$.

Since $\phi \succ \theta$, there must be an edge of $\mathbf{G}(\mathbf{L})$ going from an element in the $\equiv$-class corresponding to θ to an element in the class corresponding to ϕ. Suppose this edge has the form (3). This situation is diagrammed in Figure 1.

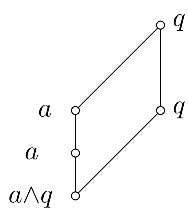

FIGURE 1

If $a \wedge q = a_*$, then we would have $\theta = \mathrm{Cg}\,(a, a_*) = \mathrm{Cg}\,(q, q^*) = \phi$, a contradiction. Thus $a \wedge q < a_*$ and the first statement of the lemma holds with $x = a \wedge q$. Of course if the the edge has the form (4), then the second statement of the lemma will hold. □

Lemma 3. *Let $\mathbf{L}$ be a lattice, let $A \subseteq L$, and let $b \in L$ be a lower bound of A in $\mathbf{L}$. Assume that $\mathrm{Cg}\,(b, a)$ is join irreducible and that $\mathrm{Cg}\,(b, a)$ and $\mathrm{Cg}\,(b, a')$ are incomparable for each $a \neq a'$ in A. Then A is join irredundant.*

Proof. This is proved in [9]. □

Theorem 4. *Let $\mathbf{L}$ be a finite lattice. Then*

$$e_{\prec}(\mathrm{J}(\mathbf{Con\,L})) \leq (|\,\mathrm{J}(\mathbf{L})| + |\,\mathrm{M}(\mathbf{L})|) \log_2 |L| \leq 2|L| \log_2 |L|.$$

Proof. Let $r = |\,\mathrm{J}(\mathbf{L})| + |\,\mathrm{M}(\mathbf{L})|$ and $e_\prec = e_\prec(\mathrm{J}(\mathbf{Con\ L}))$ and $t = \lceil e_\prec / r \rceil$. By Lemma 2, associated with each cover in $\mathrm{J}(\mathbf{Con\ L})$ is an element of L which is either join or meet irreducible. Hence there is either a join irreducible element a satisfying the first possible conclusion of that lemma or a meet irreducible one satisfying the second. Thus by duality we may assume that there is a meet irreducible element q and elements $x_1, \ldots, x_t$ with $q^* < x_i$ such that $\phi_i = \mathrm{Cg}\,(x_i, q^*)$ covers $\theta = \mathrm{Cg}\,(q, q^*)$. Thus $\phi_1, \ldots, \phi_t$ form an antichain. So by Lemma 3 $x_1, \ldots, x_t$ are join irredundant. Thus $2^t \leq |L|$ and so $e_\prec / r \leq \log_2 |L|$, and the theorem follows. □

Corollary 5. *If* $\mathbf{L}$ *is a lattice with* n *elements, then one can determine the ordered set* $\mathrm{J}(\mathbf{Con\,L})$ *and its order relation in time* $O(n^2 \log_2 n)$.

Proof. As we noted before we can find $\mathrm{J}(\mathbf{Con\ L})$ and its order relation in time $O(m^2 + me_\prec + e_\leq)$. Since $e_\prec \leq 2n \log_2 n$ and $m \leq n$, the result follows. □

Since the function $x/\log_2 x$ is increasing for $x \geq e$ (Euler's constant), we get the following corollary to Theorem 4.

Corollary 6. *Let* $\mathbf{L}$ *be a finite lattice and let* $e_\prec = e_\prec(\mathrm{J}(\mathbf{Con\,L}))$. *If* $e_\prec \geq 3$, *then*

$$|L| \geq \frac{e_\prec}{2 \log_2 e_\prec}.$$

3. Examples

In this section we give some examples showing that the inequality of Theorem 4 cannot be improved. We also show that this theorem easily gives the result of [9].

Example 7. Let r_1, r_2, and s be positive integers and let $\mathbf{K}_i = \mathbf{3} \times \mathbf{2}^{r_i - 1}$ for $i = 1$, 2. Of course $\mathbf{K}_1$ has a filter isomorphic to the three element chain $\mathbf{3}$ and $\mathbf{K}_2$ has an ideal isomorphic to $\mathbf{3}$. Using the gluing construction of Dilworth and Hall [3, 4], we can identify these two copies of $\mathbf{3}$ and use the natural order to obtain a lattice $\mathbf{K}$. Let x denote the middle element of this three element chain in $\mathbf{K}$. Replace x with $x_0 < x_1 < \cdots < x_s$ and order the resulting set by saying $z < x_i < y$ whenever $z < x < y$ in $\mathbf{K}$. Let $\mathbf{L}$ denote the resulting lattice. Note $\mathbf{L}$ is obtained from $\mathbf{K}$ by s applications of Alan Day's doubling construction [2]. The diagram of $\mathbf{L}$ is given in Figure 2 when $r_1 = r_2 = 3$ and $s = 3$.

$\mathbf{Con\ L}$ is the lattice obtained by placing the Boolean algebra $\mathbf{2}^r$ on top of the the Boolean algebra $\mathbf{2}^s$, where $r = r_1 + r_2$. $\mathrm{J}(\mathbf{Con\ L})$ is the complete bipartite ordered set with r top elements and s bottom elements. So

$$|L| = s + 3 \cdot 2^{r_1 - 1} + 3 \cdot 2^{r_2 - 1} - 3,$$
$$e_\prec(\mathrm{J}(\mathbf{Con\,L})) = rs,$$
$$|\,\mathrm{J}(\mathbf{L})| + |\,\mathrm{M}(\mathbf{L})| = 2r + 2s.$$

Let $e_\prec$ be an integer such that both $\log_2 e_\prec$ and $e_\prec / \log e_\prec$ are integers and let $r_1 = r_2 = \log_2 e_\prec$ (and so $r = 2 \log_2 e_\prec$) and $s = e_\prec / r$. (This means $e_\prec$ has the

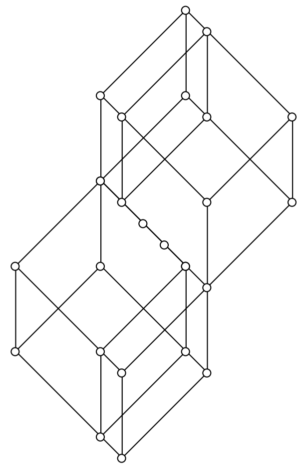

FIGURE 2. **L** when $r_1 = r_2 = 3$ and $s = 3$.

form 2^{2^k}.) Then we have by Theorem 4

$$1 \leq \frac{(2e_\prec/2\log_2 e_\prec + 4\log_2 e_\prec)\log_2(6\cdot 2^{\log_2 e_\prec - 1} - 3 + e_\prec/2\log_2 e_\prec)}{e_\prec}$$

$$\leq \frac{(2e_\prec/2\log_2 e_\prec + 4\log_2 e_\prec)\log_2(3e_\prec + e_\prec/2\log_2 e_\prec)}{e_\prec}.$$

But the latter expression tends to 1 as $e_\prec$ tends to ∞. It follows that Theorem 4 cannot be improved to state

$$e_\prec(\mathrm{J}(\mathbf{Con\ L})) \leq c(|\,\mathrm{J}(\mathbf{L})| + |\,\mathrm{M}(\mathbf{L})|)\log_2 |L|$$

for any $c < 1$.

If we take $r_1 = r_2 = \frac{1}{2}\log_2 e_\prec$, then $|L| = 6\cdot 2^{\frac{1}{2}\log_2 e_\prec - 1} + e_\prec/\log_2 e_\prec - 3 \leq 3\sqrt{e_\prec} + e_\prec/\log_2 e_\prec$. Thus $|L|/e_\prec \to 0$ for these lattices, showing that an inequality of the form $|L| \geq c\, e_\prec(\mathrm{J}(\mathbf{Con\ L}))$ cannot hold for any $c > 0$. Moreover, these parameters also show that

$$|\,\mathrm{J}(\mathbf{Con\ L})| \cdot e_\prec(\mathrm{J}(\mathbf{Con\ L})) \leq c \cdot |L|^2$$

fails for all c.

Finally, if m is even, let **P** be the height 1 ordered set with $m/2$ minimal elements, $m/2$ maximal elements, and each minimal element below each maximal element. Then $e_\prec = m^2/4$ and Corollary 6 shows that if **L** is a lattice with $\mathrm{J}(\mathbf{Con\ L}) \cong \mathbf{P}$, then

$$|L| \geq \frac{m^2}{16\log_2(m/2)}$$

and it follows that there is no α such that the class of all such **P**'s can be represented as $\mathrm{J}(\mathbf{Con\ L})$ with the size of **L** in $O(m^{2-\alpha})$, as was shown in [9].

4. Calculating the congruence lattice and an application

To actually compute **Con L** we form the graph $\mathbf{G}(\mathbf{L})$ and use Tarjan's linear time, depth first algorithm [11] to find the $\equiv$-classes and an edge set E satisfying

$E_{\prec} \subseteq E \subseteq E_{\leq}$. We then find the transitive, reflexive closure, $E_{\leq}$, of E. If there are k classes of $\equiv$, we represent congruences as bit vectors of length k. Of course the components of such a bit vector correspond to elements of $\mathrm{J}(\mathbf{Con\ L})$, since $\mathrm{J}(\mathbf{Con\ L}) \cong \mathbf{G}(\mathbf{L})/\equiv$. A congruence θ is represented by the vector which is 1 in those components corresponding to join irreducible congruences below θ. For each $a \in \mathrm{J}(\mathbf{L})$ we calculate the bit vector for $\mathrm{Cg}\,(a, a_*)$. (This is not just the vector with a 1 only in the component for $\mathrm{Cg}\,(a, a_*)$; in fact it is here that we need $E_{\leq}$.)

This representation is obviously compact. Meet and join are just the bitwise *and* and *or*. One can also decide if $x\ \theta\ y$ and compute $\mathbf{L}/\theta$ easily. For the latter we find

$$S_\theta = \{a \in \mathrm{J}(\mathbf{L}) : \langle a, a_* \rangle \notin \theta\}.$$

The join closure of this set is a join subsemilattice of $\mathbf{L}$ which is isomorphic to $\mathbf{L}/\theta$ under the induced order from $\mathbf{L}$. The details are given in [5].

W. Geyer [6, 7] conjectured that, if $\mathbf{L}$ is finite and a bounded homomorphic image of a free lattice, then $|L| \leq |\,\mathrm{Con}\ \mathbf{L}|$. He tested this conjecture on several examples and noted that when, in addition, $\mathbf{L}$ was subdirectly irreducible, equality held in all his examples. He asked me to use my computer program to try to find a counterexample. Associated with each completely join irreducible element of a free lattice is a finite, subdirectly irreducible lattice which is a bounded homomorphic image of a free lattice. Running the program on a wide selection of such elements produced a subdirectly irreducible lattice which is a bounded image of a free lattice with 53 elements whose congruence lattice had 52 elements. With this example in hand, it was not hard to construct a smaller example. An example with $|L| = 12$ and $|\mathrm{Con}\ \mathbf{L}| = 11$ is given in Figure 3.

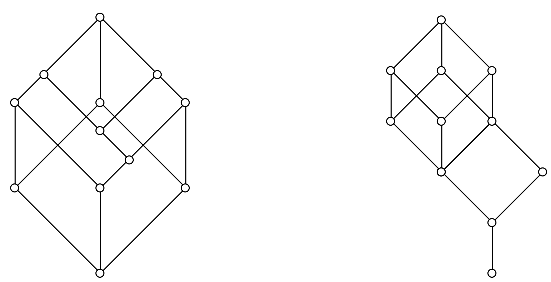

Figure 3. **L** and **Con L**.

References

[1] P. Crawley and R. P. Dilworth, *Algebraic Theory of Lattices*, Prentice-Hall, Englewood Cliffs, New Jersey, 1973.

[2] A. Day, *Doubling constructions in lattice theory*, Canad. J. Math. **44** (1992), 252–269. MR **93f:**06008

[3] R. P. Dilworth, *The arithmetical theory of Birkhoff lattices*, Duke Math. J. **8** (1941), 286–299. MR **3:**100a

[4] R. P. Dilworth and M. Hall, *The embedding theorem for modular lattices*, Ann. of Math. **45** (1944), 450–456. MR **6:**33c

[5] R. Freese, J. Ježek, and J. B. Nation, *Free Lattices*, Amer. Math. Soc., Providence, 1995, Mathematical Surveys and Monographs, vol. 42. MR **96c:**06013

[6] W. Geyer, *The class of lattices with* $|L| = |\mathrm{Con}(L)|$, General algebra and application, Heldermann, Berlin, 1993, pp. 86–88. MR **94c:**06012

[7] W. Geyer, *On Tamari lattices*, Discrete Math. **133** (1994), 99–122. MR **95m:**06021

[8] G. Grätzer, H. Lakser, and E. T. Schmidt, *Congruence lattices of small planar lattices*, Proc. Amer. Math. Soc. **123** (1995), 2619–2623. MR **95k:**06017a

[9] G. Grätzer, I. Rival, and N. Zaguia, *Small representations of finite distributive lattices as congruence lattices*, Proc. Amer. Math. Soc. **123** (1995), 1959–1961; Correction, Proc. Amer. Math. Soc., to appear. MR **95k:**06017b

[10] R. Medina and L. Nourine, *Algorithme efficace de génération des idéaux d'un ensemble ordonné*, C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), 1115–1120. MR **95i:**06006

[11] R. E. Tarjan, *Depth first searches and linear graph algorithms*, SIAM J. of Computing **1** (1972), 146–160. MR **46:**3313

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