Representing Finite Lattices as Congruence Lattices of Finite Algebras

William DeMeo, Ralph Freese, and Peter Jipsen

Abstract. This article describes various methods for representing a finite lattice as the congruence lattice of a finite algebra or for proving that such a representation exists. Using these methods, we show that with one possible exception every lattice with at most seven elements is isomorphic to the congruence lattice of a finite algebra.

1. Introduction

sec:intro

TODO: Expand the introduction.

1.1. Notation. Throughout this paper, we use $\mathscr{L}$ to denote the class of finite lattices that are isomorphic to congruence lattices of finite algebras. We call the lattices that belong to $\mathscr{L}$ *representable* lattices.

Let L be a lattice and suppose α and β belong to L. We denote by $[\![\alpha, \beta]\!]$ the sublattice of L consisting of all elements in L that lie above α and below β. That is, $[\![\alpha, \beta]\!] = \{\theta \in L \mid \alpha \leqslant \theta \text{ and } \theta \leqslant \beta\}$. (If $\alpha \nleqslant \beta$, then $[\![\alpha, \beta]\!] = \emptyset$.)

For a lattice (or, more generally, a partially ordered set) L, the *dual* of L, denoted L', is the lattice (poset) with the inverse order. That is, $x \leqslant y$ holds in L if and only if $y \leqslant x$ holds in L'. The dual of L can be depicted by flipping the Hasse diagram for L upside down. In a broader sense, two lattices (posets) are also said to be duals if they are dually isomorphic. Although we often denote the dual of L by L', on some occasions it is more convenient to use an operator notation, such as ∂L, to denote the dual of L.

2. Closure properties of the class of representable lattices

sec:clos-prop-class

This section describes some *closure properties* of the class $\mathscr{L}$. By closure properties, we mean the following: if O is an operation that can be applied to a lattice or collection of lattices, we say that $\mathscr{L}$ is *closed under* O provided $\mathsf{O}(\mathscr{K}) \subseteq \mathscr{L}$ for all $\mathscr{K} \subseteq \mathscr{L}$. For example, if $\mathsf{S}(\mathscr{K})$ is all sublattices of lattices in $\mathscr{K}$, it is unknown whether $\mathscr{L}$ is closed under S. If this were known to

be true, then the *finite lattice representation problem* would be solved. The congruence lattice of the algebra consisting of a set X with no operations is the lattice of all equivalence relations on X, which we denote by $\operatorname{Eq} X$. By a celebrated theorem of Pudlák and Tůma [13], for every finite lattice L there is a finite set X such that $L \leqslant \operatorname{Eq} X$. Therefore, $\mathscr{L}$ would contain all finite lattices if it were closed under S.

The following is a list of operations under which $\mathscr{L}$ is known to be closed, along with the names of those who first (or independently) proved them. We discuss some of these results in greater detail later in this section. The class $\mathscr{L}$ of lattices isomorphic to congruence lattices of finite algebras is closed under the following operations:

<div style="border:1px solid;display:inline-block;padding:2px">item:1</div>

(1) lattice duals (Hans Kurzweil [6] and Raimund Netter [10], 1986),
(2) interval sublattices (follows from (1)),
(3) direct products (Jiří Tůma [17], 1986),
(4) ordinal sums (Ralph McKenzie [8], 1984; John Snow [16], 2000),
(5) parallel sums (John Snow [16], 2000),
(6) certain sublattices of lattices in $\mathscr{L}$ – namely, those which are obtained as a union of a filter and an ideal of a lattice in $\mathscr{L}$ (John Snow [16], 2000).
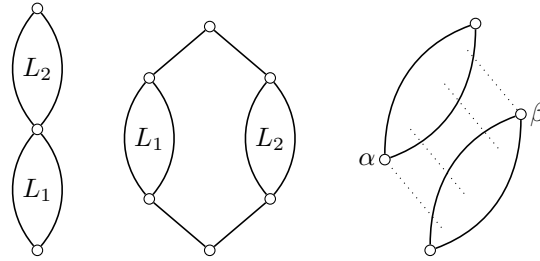

FIGURE 1. The adjoined ordinal sum (left) and parallel sum (middle) of the lattices L_1 and L_2; a union of an order filter $\alpha^\uparrow$ and order ideal $\beta^\downarrow$ (right).

<div style="border:1px solid;display:inline-block;padding:2px">fig:ord_par_fil-uni</div>

Remarks.

a. The first item in the list above says that if L is representable then so is the dual of L. It follows from this that every interval sublattice of a representable lattice is also representable. Indeed, suppose L is representable, say, $L \cong \bar{L} = \operatorname{Con} \mathbf{A}$. Let $[\![\alpha, \beta]\!]$ be an interval sublattice of L, and $[\![\bar{\alpha}, \bar{\beta}]\!]$ the corresponding interval of $\bar{L}$. For ease of notation, let's rename $\bar{\alpha}$ and $\bar{\beta}$, dropping the bars. Thus $[\![\alpha, \beta]\!]$ is the interval of interest and we assume $[\![\alpha, \beta]\!] \leqslant \operatorname{Con} \mathbf{A}$. The filter $\alpha^\uparrow = [\![\alpha, 1_A]\!]$ is isomorphic to $\operatorname{Con}(\mathbf{A}/\alpha)$, hence representable, so by (1) the dual $\partial(\alpha^\uparrow) = [\![1'_A, \alpha']\!]$ is also representable. (Here x' denotes the image of x under dualization.) Another quotient (this

time by β') gives a representation of the interval $[\![\beta', \alpha']\!]$ above β' in $\partial(\alpha^\uparrow)$. Since $[\![\beta', \alpha']\!]$ is the dual of $[\![\alpha, \beta]\!]$, we apply (1) once more to obtain the desired representation of $[\![\alpha, \beta]\!]$. Thus (2) follows from (1).

b. By the ordinal sum of two lattices L_1, L_2, we mean the lattice on the left of Figure 1. By the parallel sum of two lattices L_1, L_2, we mean the lattice in the middle of Figure 1.

c. Item (6) above is a very useful result which we will discuss further in Section 2.2 below, where we present a short proof of this fact.

d. Whether the class $\mathscr{L}$ is closed under homomorphic images seems to be an open question.

2.1. Lattice duals: the theorem of Kurzweil and Netter. As mentioned above, the class $\mathscr{L}$ – the lattices isomorphic to congruence lattices of finite algebras – is closed under dualization. That is, if L is representable, then so is the dual of L. This was proved in 1986 by Raimund Netter [10], generalizing the idea of his advisor, Hans Kurzweil [6]. Though Kurzweil's article did appear, it is unclear whether Netter's article was ever published. In this section we present a proof of their result. The argument requires a fair bit of machinery, but it is a nice idea and well worth the effort.[1]

If G is a group and X a set, then the set $\{f \mid X \to G\}$ of functions from X into G is denoted by G^X. This is a group with binary operation $(f, g) \mapsto f \cdot g$, where, for each $x \in X$, $(f \cdot g)(x) = f(x)g(x)$ is simply multiplication in the group G. The identity of the group G^X is of course the constant map $f(x) = 1_G$ for all $x \in X$.

Let X be a finite totally ordered set, with order relation $\leqslant$, and consider the set X^X of functions mapping X into itself. The subset of X^X consisting of functions that are idempotent and satisfy $f(x) \leqslant x$ for all $x \in X$ will be denoted by $\mathcal{ID}(X)$. That is,

$$\mathcal{ID}(X) = \{f \in X^X \mid f^2 = f \text{ and } \forall x \ f(x) \leqslant x\}.$$

Define the binary relation $\sqsubseteq$ on the set $\mathcal{ID}(X)$ by

$$f \sqsubseteq g \quad \Leftrightarrow \quad \ker f \leqslant \ker g, \tag{2.1}$$

where $\ker f = \{(x, y) \in X^2 \mid f(x) = f(y)\}$. It is easy to see that $f \sqsubseteq g$ holds if and only if $gf = g$, and that $\sqsubseteq$ is a partial ordering of $\mathcal{ID}(X)$. In fact, under this ordering, $\mathcal{ID}(X)$ is a lattice which is isomorphic to $\mathbf{Eq}(X)$. The lattice isomorphism is the map $\Theta : \mathrm{Eq}\, X \to \mathcal{ID}(X)$ given by $\Theta(\alpha) = f_\alpha$, where $f_\alpha(x) = \min\{y \in X \mid x \, \alpha \, y\}$.

Suppose S is a finite nonabelian simple group, and consider the direct power S^n. An element of S^n may be viewed either as a function, $\mathbf{x} : \underline{n} \to S$,

---

[1] We learned of the main argument used in the proof from slides of a series of three lectures given by Péter Pálfy in 2009 [12]. Pálfy gives credit for the argument to Kurzweil and Netter.

from the set $\underline{n} = \{0, 1, \dots, n-1\}$ to S, or as the tuple of its values, that is, $\mathbf{x} = (x(0), x(1), \dots, x(n-1))$. As a function, $\mathbf{x}$ has kernel

$$\ker \mathbf{x} = \{(i, j) \in \underline{n}^2 \mid x(i) = x(j)\}.$$

The set of constant functions in S^n is a subgroup $D < S^n$, sometimes called the *diagonal subgroup*; that is,

$$D = \{(s, s, \dots, s) \mid s \in S\} \leqslant S^n.$$

For each $f \in \mathcal{ID}(n)$, define

$$Xf = \{\mathbf{x}f \mid \mathbf{x} \in S^n\} = \{(xf(0), xf(1), \dots, xf(n-1)) \mid \mathbf{x} \in S^n\}.$$

That is, Xf is the set of all compositions of f followed by $\mathbf{x} \in S^n$. Thus, $Xf = \{\mathbf{y} \in S^n \mid \ker f \leqslant \ker \mathbf{y}\}$. For example, if $f = (0, 0, 2, 3, 2) \in \mathcal{ID}(\underline{5})$, then $\ker f$ is the equivalence relation corresponding to the partition $|0, 1|2, 4|3|$, and Xf is the subgroup of all $\mathbf{y} = (y(0), y(1), y(2), y(3), y(4)) \in S^5$ satisfying $y(0) = y(1)$ and $y(2) = y(4)$. That is,

$$Xf = \{(x(0), x(0), x(2), x(3), x(2)) \mid \mathbf{x} \in S^5\} = \{\mathbf{y} \in S^5 \mid \ker f \leqslant \ker \mathbf{y}\}.$$

It's not hard to see that $D \leqslant Xf \leqslant S^n$, for all $f \in \mathcal{ID}(n)$.

| lem:latt-duals | **Lemma 2.1.** *The map $f \mapsto Xf$ is a dual lattice isomorphism from* $\mathbf{Eq}(n)$ *onto the interval sublattice* $[\![D, S^n]\!] \leqslant \mathrm{Sub}(S^n)$. |

Proof. This is clear since $\mathcal{ID}(n)$ is ordered by (2.1), and we have $f \sqsubseteq h$ if and only if $Xh = \{\mathbf{y} \in S^n \mid \ker h \leqslant \ker \mathbf{y}\} \leqslant \{\mathbf{y} \in S^n \mid \ker f \leqslant \ker \mathbf{y}\} = Xf$. $\square$

| thm:duals-interv-subl | **Theorem 2.2** (Kurzweil [6], Netter [10])**.** *If the finite lattice L is representable as the congruence lattice of a finite algebra, then so is the dual lattice L'.* |

Proof. Without loss of generality, we assume that L is represented as $L = \mathrm{Con}\,\langle n, F \rangle$. Also, by [9, Theorem 4.18], we can assume that F consists of unary operations: $F \subseteq n^n$. As above, let S be a nonabelian simple group and let D be the diagonal subgroup of S^n. Then the unary algebra $\langle S^n/D, S^n \rangle$ is a transitive S^n-set which has congruence lattice isomorphic to the interval $[\![D, S^n]\!]$. (See, for example, [9, Lemma 4.20].) By Lemma 2.1, this is the dual of the lattice $\mathbf{Eq}(n)$. That is, $\mathrm{Con}\,\langle S^n/D, S^n \rangle \cong (\mathbf{Eq}(n))'$.

Now, each operation $\varphi \in F$ gives rise to an operation on S^n by composition:

$$\hat{\varphi}(\mathbf{x}) = \mathbf{x}\varphi = (x(\varphi(0)), x(\varphi(1)), \dots, x(\varphi(n-1))).$$

Thus, φ induces an operation on S^n/D since, for $\mathbf{d} = (s, s, \dots, s) \in D$ and for $\mathbf{x} \in S^n$, we have

$$\mathbf{xd} = (x(0)d(0), x(1)d(1), \dots, x(n-1)d(n-1))$$
$$= (x(0)s, x(1)s, \dots, x(n-1)s).$$

Therefore,

$$\hat{\varphi}(\mathbf{xd}) = (x(\varphi(0))s, x(\varphi(1))s, \dots, x(\varphi(n-1))s) = \hat{\varphi}(\mathbf{x})\mathbf{d},$$

so $\hat{\varphi}(\mathbf{x}D) = \hat{\varphi}(\mathbf{x})D$. Finally, add the set of operations $\hat{F} = \{\hat{\varphi} \mid \varphi \in F\}$ to $\langle S^n/D, S^n \rangle$, yielding the new algebra $\langle S^n/D, S^n \cup \hat{F} \rangle$, and observe that a congruence $\theta \in \mathrm{Con}\, \langle S^n/D, S^n \rangle$ remains a congruence of $\langle S^n/D, S^n \cup \hat{F} \rangle$ if and only if it corresponds to a partition on n that is invariant under F. $\square$

TODO: Perhaps we should give more details in the last sentence of the proof.

2.2. Union of a filter and ideal. The lemma in this section was originally proved by John Snow using primitive positive formulas. Since it provides such a useful tool for proving that certain finite lattices are representable as congruence lattices, we give our own direct proof of the result below.

Before stating the lemma, we need a couple of definitions. (These will be discussed in greater detail in Section 3.2.) Given a relation $\theta \subseteq X \times X$, we say that the map $f : X^n \to X$ *respects* θ and we write $f(\theta) \subseteq \theta$ provided $(x_i, y_i) \in \theta$ implies $(f(x_1, \ldots, x_n), f(y_1, \ldots, y_n)) \in \theta$. For a set $L \subseteq \mathrm{Eq}\, X$ of equivalence relations we define

$$\lambda(L) = \{f \in X^X : (\forall \theta \in L)\ f(\theta) \subseteq \theta\},$$

which is the set of all unary maps on X which respect all relations in L.

Lemma 2.3. *Let X be a finite set. If $\mathbf{L} \leqslant \mathbf{Eq}(X)$ is representable and $\mathbf{L}_0 \leqslant \mathbf{L}$ is a sublattice with universe $\alpha^\uparrow \cup \beta^\downarrow$ where $\alpha^\uparrow = \{x \in L \mid \alpha \leqslant x\}$ and $\beta^\downarrow = \{x \in L \mid x \leqslant \beta\}$ for some $\alpha, \beta \in L$, then $\mathbf{L}_0$ is representable.*
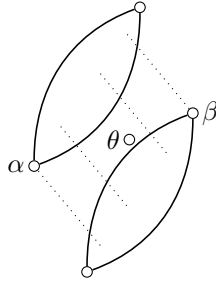

FIGURE 2. $L_0 \leq L_1$

Proof. Assume $\mathbf{L}_0 \not\cong \mathbf{2}$, otherwise the result holds trivially. Since $\mathbf{L} \leqslant \mathbf{Eq}(X)$ is representable, we have $\mathbf{L} = \mathbf{Con}\, \langle X, \lambda(L) \rangle$ (cf. Section 3.2). Take an arbitrary $\theta \in L \setminus L_0$. Since $\theta \notin \alpha^\uparrow$, there is a pair $(a, b) \in \alpha \setminus \theta$. Since $\theta \notin \beta^\downarrow$, there is a pair $(u, v) \in \theta \setminus \beta$. Define $h \in X^X$ as follows:

$$h(x) = \begin{cases} a, & x \in u/\beta, \\ b, & \text{otherwise.} \end{cases}$$

Then, $\beta \leqslant \ker h = (u/\beta)^2 \cup ((u/\beta)^c)^2$, where $(u/\beta)^c$ denotes the complement of the β class containing u. Therefore, h respects every $\gamma \leqslant \beta$. Furthermore, $(a, b) \in \gamma$ for all $\gamma \geqslant \alpha$, so h respects every γ above α. This proves that $h \in \lambda(L_0)$. Now, θ was arbitrary, so we have proved that for every $\theta \in L \setminus L_0$ there exists a function in $\lambda(L_0)$ which respects every $\gamma \in \alpha^\uparrow \cup \beta^\downarrow = L_0$, but violates θ. Finally, since $\mathbf{L}_0 \leqslant \mathbf{L}$, we have $\lambda(L) \subseteq \lambda(L_0)$. Combining these observations, we see that every $\theta \in \mathrm{Eq}\,X \setminus L_0$ is violated by some function in $\lambda(L_0)$. Therefore, $\mathbf{L}_0 = \mathbf{Con}\,\langle X, \lambda(L_0) \rangle$. $\qquad\square$

sec:ordinal-sums

2.3. Ordinal Sums I. TODO: Revise this section. Peter has written up some nice lemmas and theorems on this topic which now appear below in a subsection called "Ordinal Sums II," but that material should be integrated with and/or replace the material in this subsection.

The following theorem is a consequence of McKenzie's shift product construction [8].

thm:ordinal-sums

Theorem 2.4. *If $L_1, \ldots, L_n \in \mathscr{L}$ is a collection of representable lattices, then the ordinal sum and the adjoined ordinal sum, shown in Figure 2.3, are representable.*

A more direct proof of Theorem 2.4 follows the argument given by John Snow in [16]. As noted above, Jiří Tůma proved that the class of finite representable lattices is closed under direct products. Thus, if L_1 and L_2 are representable, then so is $L_1 \times L_2$. Now note that the adjoined ordinal sum of L_1 and L_2 is the union, $\alpha^\uparrow \cup \beta^\downarrow$, of a filter and ideal in the lattice $L_1 \times L_2$, where $\alpha = \beta = 1_{L_1} \times 0_{L_2}$. Therefore, by Lemma 2.3, the adjoined ordinal sum is representable. A trivial induction argument proves the result for adjoined ordinal sums of n lattices. The same result for ordinal sums (Figure 2.3 left) follows since the two element lattice is obviously representable.

fig:ord_adjord

2.4. Ordinal Sums II. TODO: Merge this subsection with the subsection "Ordinal Sums I."

The lattice of equivalence relations on an n-element set is denoted by $\mathrm{Equ}(n)$. For two lattices $\mathbf{L}, \mathbf{M}$ the *adjoined ordinal sum* is denoted by $\mathbf{L} \oplus_a \mathbf{M}$ and is defined on $L \uplus (M \setminus \{0\})$ by $x \leq y$ iff $x \in L, y \in M$ or $(x, y \in L$ and $x \leq^{\mathbf{L}} y)$ or $(x, y \in M$ and $x \leq^{\mathbf{M}} y)$.

Let $\mathbf{A}, \mathbf{B}$ be two finite algebras of cardinality m and n respectively, and let $\mathbf{L} = \mathrm{Con}(\mathbf{A})$ and $\mathbf{M} = \mathrm{Con}(\mathbf{B})$. In [16] it is proved that $\mathbf{L} \oplus_a \mathbf{M}$ is isomorphic to the congruence lattice of some finite algebra $\mathbf{C}$. Although the algebra $\mathbf{C}$ is not explicitly constructed, it is based on the direct product of $\mathbf{A}$ and $\mathbf{B}$, hence the ordinal sum is a sublattice of $\mathrm{Equ}(mn)$. Here we give a
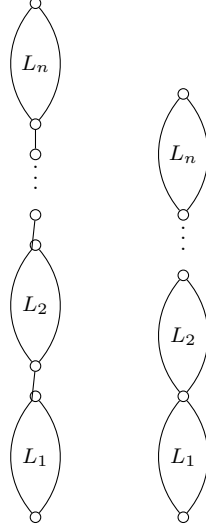
FIGURE 3. The ordinal sum (left) and the adjoined ordinal sum (right) of the lattices $L_1, \ldots, L_n$.

different construction of $\mathbf{C}$ that leads to a tighter representation of $\mathrm{Con}(\mathbf{C})$ as a sublattice of $\mathrm{Equ}(m + n - 1)$.

Define a unary algebra $\mathbf{A}_{m,n}$ with $m + n - 1$ elements as follows: the base set is $A \uplus B_1$ where $A = \{a_0, \ldots, a_{m-1}\}$, $B_1 = \{b_1, \ldots, b_{n-1}\}$ and for each function $h : B_1 \to A$ define a unary operation

$$\hat{h}(x) = \begin{cases} h(x) & \text{if } x \in B_1 \\ x & \text{otherwise.} \end{cases}$$

Lemma 2.5. *For $m, n \geq 1$ the lattice $\mathrm{Con}(\mathbf{A}_{m,n})$ is isomorphic to $\mathrm{Equ}(m) \oplus_a \mathrm{Equ}(n)$.*

Proof. Let α be the equivalence relation $A^2 \cup \{(b_1, b_1), \ldots, (b_{n-1}, b_{n-1})\}$, so as a partition it is $a_0, \ldots, a_{m-1} | b_1 | b_2 | \ldots | b_{n-1}$. Note that $\mathrm{Equ}(m) \oplus_a \mathrm{Equ}(n)$ is isomorphic to the sublattice of $\mathrm{Equ}(A \uplus B_1)$ of all equivalence relations comparable to α, since α has a unique non-singleton block of size m, and n blocks altogether. We claim that this sublattice is the congruence lattice of $\mathbf{A}_{m,n}$.

Suppose $\theta \leq \alpha$, and let $(x, y) \in \theta$. Then $x, y \in A$ or $x = y$, hence for any operation $\hat{h}$ we have $\hat{h}(x) = x$ and $\hat{h}(y) = y$ or $\hat{h}(x) = \hat{h}(y)$, so $(\hat{h}(x), \hat{h}(y)) \in \theta$.

Suppose $\alpha \leq \theta$, and let $(x, y) \in \theta$. Since $A^2 \subseteq \alpha$ and since the range of each $\hat{h}$ is A it follows that $(\hat{h}(x), \hat{h}(y)) \in \theta$.

Now suppose θ is incomparable with α. Then A^2 is not a subset of θ, hence there exist $(x, y) \in A^2 \setminus \theta$ and $(u, v) \in \theta \setminus \alpha$. If $u, v \in B_1$ then choose a function h (as in the definition of $\mathbf{A}_{m,n}$) such that $h(u) = x$ and $h(v) = y$, in which case $\hat{h}$ is an operation that shows θ is not a congruence. If $u \in B_1$, but $v \in A$,

note that we cannot have both (x, v) and (y, v) in θ (else $(x, y) \in \theta$). Assume without loss of generality that $(x, v) \notin \theta$ and choose h such that $h(u) = x$, then again $\hat{h}$ shows that θ is not a congruence. The case $u \in A$, $v \in B_1$ is similar, and $u, v \in A$ is excluded since $(u, v) \notin \alpha$.   □

Theorem 2.6. *Suppose* $\mathbf{A} = (A, F)$ *and* $\mathbf{B} = (B, G)$ *are unary algebras with* $A = \{a_0, \ldots, a_{m-1}\}$, $B = \{b_0, \ldots, b_{n-1}\}$ *and* $A \cap B = \{a_0\} = \{b_0\}$ *(so* a_0, b_0 *are identified). Let* $\mathbf{C}$ *be the algebra* $\mathbf{A}_{m,n}$ *expanded with the operations*

$$\hat{f}(x) = \begin{cases} f(x) & \text{if } x \in A \\ f(a_0) & \text{otherwise} \end{cases} \qquad \hat{g}(x) = \begin{cases} g(x) & \text{if } x \in B \\ g(b_0) & \text{otherwise} \end{cases}$$

for $f \in F$ *and* $g \in G$. *Then* $\mathrm{Con}(\mathbf{C})$ *is isomorphic to* $\mathrm{Con}(\mathbf{A}) \oplus_a \mathrm{Con}(\mathbf{B})$.

Proof. Since $\mathbf{C}$ is an expansion of $\mathbf{A}_{m,n}$ it follows from the preceding lemma that $\mathrm{Con}(\mathbf{C})$ is a sublattice of $\{\theta \in \mathrm{Equ}(A \cup B) : \theta \leq \alpha \text{ or } \alpha \leq \theta\}$ where, as before, $\alpha = A^2 \cup \mathrm{id}_B$. Note that $\alpha \in \mathrm{Con}(\mathbf{C})$, so it suffices to show that $\{\theta \in \mathrm{Con}(\mathbf{C}) : \theta \leq \alpha\}$ is isomorphic to $\mathrm{Con}(\mathbf{A})$ and $\{\theta \in \mathrm{Con}(\mathbf{C}) : \theta \leq \alpha\}$ is isomorphic to $\mathrm{Con}(\mathbf{B})$. The second isomorphism follows from the observation that $\mathbf{C}/\alpha$ is isomorphic to $\mathbf{B}$ via the map $A \mapsto b_0$ and $\{b_i\} \mapsto b_i$ for $i \geq 1$. For the first isomorphism, note that the operations $\hat{g}$, $\hat{h}$ preserve all equivalence relations below α. Similarly it is straight forward to check that $\hat{f}$ preserves $\theta \leq \alpha$ iff f preserves $\theta \cap A^2$. Hence the map $\theta \mapsto \theta \cap A^2$ is the required isomorphism.   □

Now assume $\mathbf{A}$ and $\mathbf{B}$ are minimal-size algebras with congruence lattices isomorphic to $\mathbf{L}$ and $\mathbf{M}$ respectively. Then it seems likely that the algebra $\mathbf{C}$ above is minimal in size with respect to having a congruence lattice isomorphic to $\mathbf{L} \oplus_a \mathbf{M}$. Suppose $\mathbf{C}'$ is a smaller algebra with the same congruence lattice, and let α be the congruence in the "middle" of the ordinal sum. Then $\mathbf{C}'/\alpha$ has a congruence lattice isomorphic to $\mathbf{M}$, hence $|\mathbf{C}'/\alpha| = |\mathbf{B}|$ = number of blocks in α. However, α does not need to have a unique nontrivial block, so it is not clear at the moment how to obtain a smaller algebra $\mathbf{A}'$ such that $\mathrm{Con}(\mathbf{A}')$ is isomorphic to $\mathbf{L}$.

3. Concrete Representations

sec:concr-repr

In this section, we introduce a strategy that has proven very useful for showing that a given lattice is representable as a congruence lattice of a finite algebra. We call it the *closure method*, and it has become especially useful with the advent of powerful computers which can search for such representations. Here, $\mathrm{Eq}\, X$ denotes the lattice of equivalence relations on X. Sometimes we abuse notation and take $\mathrm{Eq}\, X$ to mean the lattice of partitions of the set X. This never causes problems because these two lattices are isomorphic.

3.1. Concrete versus abstract representations. As Bjarni Jónsson explains in [5], there are two types of representation problems for congruence lattices, the concrete and the abstract. The *concrete representation problem* asks whether a specific family of equivalence relations on a set A is equal to Con $\mathbf{A}$ for some algebra $\mathbf{A}$ with universe A. The *abstract representation problem* asks whether a given lattice is isomorphic to Con $\mathbf{A}$ for some algebra $\mathbf{A}$.

These two problems are closely related, and have become even more so since the publication in 1980 of [13], in which Pavel Pudlák and Jiří Tůma prove that every finite lattice can be embedded as a spanning sublattice[2] of the lattice Eq X of equivalence relations on a finite set X. Given this result, we see that even if our goal is to solve the abstract representation problem for some (abstract) lattice L, then we can embed L into Eq X as $L \cong L_0 \leqslant \text{Eq } X$, for some finite set X, and then try to solve the concrete representation problem for L_0.

A point of clarification is in order here. The term *representation* has become a bit overused in the literature about the finite lattice representation problem. On the one hand, given a finite lattice L, if there is a finite algebra $\mathbf{A}$ such that $L \cong \text{Con } \mathbf{A}$, then L is called a *representable lattice.* On the other hand, given a sublattice $L_0 \leqslant \text{Eq } X$, if $L_0 \cong L$, then L_0 is sometimes called a *concrete representation* of the lattice L (whether or not it is the congruence lattice of an algebra). Below we will define the notion of a *closed concrete representation*, and if we have this special kind of concrete representation of a give lattice, then that lattice is indeed representable in the first sense.

As we will see below, there are many examples in which a particular concrete representation $L_0 \leqslant \text{Eq } X$ of L is not a congruence lattice of a finite algebra. (In fact, we will describe general situations in which we can guarantee that there are no non-trivial[3] operations which respect the equivalence relations of L_0.) This does not imply that $L \notin \mathscr{L}$. It may simply mean that L_0 is not the "right" concrete representation of L, and perhaps we can find some other $L \cong L_1 \leqslant \text{Eq } X$ such that $L_1 = \text{Con } \langle X, \lambda(L_1) \rangle$.

sec:closure-method

3.2. The closure method. The idea described in this section first appeared in *Topics in Universal Algebra* [5], pages 174–175, where Jónsson states, "these or related results were discovered independently by at least three different parties during the summer and fall of 1970: by Stanley Burris, Henry Crapo, Alan Day, Dennis Higgs and Warren Nickols at the University of Waterloo, by R. Quackenbush and B. Wolk at the University of Manitoba, and by B. Jónsson at Vanderbilt University."

Let X^X denote the set of all (unary) maps from the set X to itself, and let Eq X denote the lattice of equivalence relations on the set X. If $\theta \in \text{Eq } X$ and $h \in X^X$, we write $h(\theta) \subseteq \theta$ and say that "h respects θ" if and only if for all

---

[2]Recall, by a *spanning sublattice* of a bounded lattice L_0, we mean a sublattice $L \leqslant L_0$ that has the same top and bottom as L_0. That is $1_L = 1_{L_0}$ and $0_L = 0_{L_0}$.

[3]By a *non-trivial function* we mean a function that is not constant and not the identity.

$(x, y) \in X^2$ $(x, y) \in \theta$ implies $(h(x), h(y)) \in \theta$. If $h(\theta) \nsubseteq \theta$, we sometimes say that "h violates θ."

For $L \subseteq \operatorname{Eq} X$ define

$$\lambda(L) = \{h \in X^X : (\forall \theta \in L)\, h(\theta) \subseteq \theta\}.$$

For $H \subseteq X^X$ define

$$\rho(H) = \{\theta \in \operatorname{Eq} X \mid (\forall h \in H)\, h(\theta) \subseteq \theta\}.$$

The map $\rho\lambda$ is a *closure operator* on $\operatorname{Sub}[\operatorname{Eq} X]$. That is, $\rho\lambda$ is

- *idempotent:*[4] $\rho\lambda\rho\lambda = \rho\lambda$;
- *extensive:* $L \subseteq \rho\lambda(L)$ for every $L \leqslant \operatorname{Eq} X$;
- *order preserving:* $\rho\lambda(L) \leqslant \rho\lambda(L_0)$ if $L \leqslant L_0$.

Given $L \leqslant \operatorname{Eq} X$, if $\rho\lambda(L) = L$, then we say L is a *closed* sublattice of $\operatorname{Eq} X$, in which case we clearly have

$$L = \operatorname{Con} \langle X, \lambda(L)\rangle.$$

This suggests the following strategy for solving the representation problem for a given abstract finite lattice L: search for a concrete representation $L \cong L_0 \leqslant \operatorname{Eq} X$, compute $\lambda(L_0)$, compute $\rho\lambda(L_0)$, and determine whether $\rho\lambda(L_0) = L_0$. If so, then we have solved the abstract representation problem for L, by finding a *closed concrete representation*, or simply *closed representation*, of L_0. We call this strategy the *closure method*.

We now state without proof a well known theorem which shows that the finite lattice representation problem can be formulated in terms of closed concrete representations (cf. [5]).

Concrete-thm-3 **Theorem 3.1.** *If* $\mathbf{L} \leqslant \mathbf{Eq}(X)$, *then* $\mathbf{L} = \mathbf{Con\,A}$ *for some algebra* $\mathbf{A} = \langle X, F\rangle$ *if and only if* $\mathbf{L}$ *is closed.*

Before proceeding, we introduce a slightly different set-up than the one introduced above that we have found particularly useful for implementing the closure method on a computer. Instead of considering the set of equivalence relations on a finite set, we work with the set of idempotent decreasing maps. These were introduced above in Section 2.1, but we briefly review the definitions here for convenience.

Given a totally ordered set X, let the set $\mathcal{ID}(X) = \{f \in X^X : f^2 = f \text{ and } f(x) \leqslant x\}$ be partially ordered by $\sqsubseteq$ as follows:

$$f \sqsubseteq g \quad \Leftrightarrow \quad \ker f \leqslant \ker g.$$

As noted above, this makes $\mathcal{ID}(X)$ into a lattice that is isomorphic to $\mathbf{Eq}(X)$. Define a relation R on $X^X \times \mathcal{ID}(X)$ as follows:

$$(h, f) \in R \quad \Leftrightarrow \quad (\forall(x, y) \in \ker f)\, (h(x), h(y)) \in \ker f.$$

If $h\,R\,f$, we say that h *respects* f.

---

[4]In fact, $\rho\lambda\rho = \rho$ and $\lambda\rho\lambda = \lambda$.

Let $\mathscr{F} = \mathscr{P}(\mathcal{ID}(X))$ and $\mathscr{H} = \mathscr{P}(X^X)$ be partially ordered by set inclusion, and define the maps $\lambda : \mathscr{F} \to \mathscr{H}$ and $\rho : \mathscr{H} \to \mathscr{F}$ as follows:

$$\lambda(F) = \{h \in X^X : \forall f \in F, \, h \, R \, f\} \quad (F \in \mathscr{F})$$

$$\rho(H) = \{f \in \mathcal{ID}(X) : \forall h \in H, \, h \, R \, f\} \quad (H \in \mathscr{H})$$

The pair (λ, ρ) defines a *Galois correspondence* between $\mathcal{ID}(X)$ and X^X. That is, λ and ρ are antitone maps such that $\lambda\rho \geqslant \mathrm{id}_{\mathscr{H}}$ and $\rho\lambda \geqslant \mathrm{id}_{\mathscr{F}}$. In particular, for any set $F \in \mathscr{F}$ we have $F \subseteq \rho\lambda(F)$. These statements are all trivial verifications, and a couple of easy consequences are:

(1) $\rho\lambda\rho = \rho$ and $\lambda\rho\lambda = \lambda$,

(2) $\rho\lambda$ and $\lambda\rho$ are idempotent.

Since the map $\rho\lambda$ from $\mathscr{F}$ to itself is idempotent, extensive, and order preserving, it is a *closure operator* on $\mathscr{F}$, and we say a set $F \in \mathscr{F}$ is *closed* if and only if $\rho\lambda(F) = F$. Equivalently, F is closed if and only if $F = \rho(H)$ for some $H \in \mathscr{H}$.

4. Distributive lattices

sec:distr-latt

TODO: Cite Birkhoff result about every finite distributive lattice being the congruence lattice of a finite lattice.

TODO: We may want to omit the proof of Theorem 4.1

A lattice $\mathbf{L}$ is called *strongly representable* if whenever $\mathbf{L} \cong \mathbf{L}_0 \leqslant \mathbf{Eq}(X)$ for some X then there is an algebra based on X whose congruence lattice is $\mathbf{L}_0$. In other words, *every* distributive spanning sublattice of the lattice of equivalence relations on a finite set X is equal to the congruence lattice of an algebra $\langle X, F \rangle$, for some collection F of operations on X.

Theorem 4.1 (Berman [3], Quackenbush and Wolk [14])**.** *Every finite distributive lattice is strongly representable.*

Remarks. By Theorem 3.1 above, the result of Berman, Quackenbush and Wolk says, if $\mathbf{L}$ is a finite distributive lattice then every embedding $\mathbf{L} \cong \mathbf{L}_0 \leqslant \mathbf{Eq}(X)$ is closed. The following proof is only slightly shorter than to the original in [14], and the methods are similar.

Proof. Without loss of generality, suppose $\mathbf{L} \leqslant \mathbf{Eq}(X)$. Fix $\theta \in \mathrm{Eq}\,X \setminus L$ and define $\theta^* = \bigwedge\{\gamma \in L \mid \gamma \geqslant \theta\}$ and $\theta_* = \bigvee\{\gamma \in L \mid \gamma \leqslant \theta\}$. Let α be a join irreducible in L below θ^* and not below θ_*. Note that α is not below θ. Let $\beta = \bigvee\{\gamma \in L \mid \gamma \not\geqslant \alpha\}$. If β were above θ, then β would be above θ^*, and so β would be above α. But α is join prime, so β is not above θ.

Choose $(u, v) \in \alpha \setminus \theta$ and note that $u \neq v$. Choose $(x, y) \in \theta \setminus \beta$ and note that $x \neq y$. Let B be the β block of y and define $h \in X^X$ as in (**??**). Then it is clear that h violates θ, h respects all elements in the sets $\alpha^{\uparrow} = \{\gamma \in L : \alpha \leqslant \gamma\}$

$$X^X$$

$$\text{End}\,\mathbf{X} \qquad\qquad S_X$$
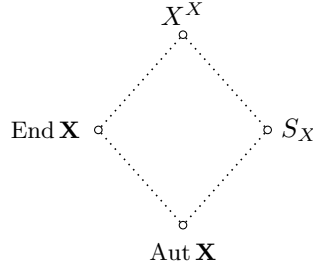
$$\text{Aut}\,\mathbf{X}$$

FIGURE 4.

and $\beta^\downarrow = \{\gamma \in L : \gamma \leqslant \beta\}$, and $L = \alpha^\uparrow \cup \beta^\downarrow$. Since θ was an arbitrary element of $\text{Eq}\,X \setminus L$, we can construct such an $h = h_\theta$ for each $\theta \in \text{Eq}\,X \setminus L$. Let $\mathscr{H} = \{h_\theta : \theta \in \text{Eq}\,X \setminus L\}$ and let $\mathbf{A}$ be the algebra $\langle X, \mathscr{H}\rangle$. Then, $\mathbf{L} = \mathbf{Con}\,(\mathbf{A})$. $\qquad\qquad\square$

5. Congruence Lattices of Group Actions

Let X be a finite set and consider the set X^X of all maps from X to itself, which, when endowed with composition of maps and the identity mapping, forms a monoid, $\langle X^X, \circ, \text{id}_X\rangle$. The submonoid S_X of all bijective maps in X^X is a group, the *symmetric group on X*. When the underlying set is more complicated, or for emphasis, we denote the symmetric group on X by $\text{Sym}(X)$. When the underlying set isn't important, we usually write S_n to denote the symmetric group on an n-element set.

If we have defined some set F of basic operations on X, so that $\mathbf{X} = \langle X, F\rangle$ is an algebra, then two other important submonoids of X^X are $\text{End}\,\mathbf{X}$, the set of maps in X^X which respect all operations in F, and $\text{Aut}\,\mathbf{X}$, the set of bijective maps in X^X which respect all operations in F. It is apparent from the definition that $\text{Aut}\,\mathbf{X} = S_X \cap \text{End}\,\mathbf{X}$, and $\text{Aut}\,\mathbf{X}$ is a submonoid of $\text{End}\,\mathbf{X}$ and a subgroup of S_X. These four fundamental monoids associated with the algebra $\mathbf{X}$, and their relative ordering under inclusion, are shown in the diagram below.

Given a finite group G, and an algebra $\mathbf{X} = \langle X, F\rangle$, a *representation* of G on $\mathbf{X}$ is a group homomorphism from G into $\text{Aut}\,\mathbf{X}$. That is, a representation of G is a mapping $\varphi : G \to \text{Aut}\,\mathbf{X}$ which satisfies $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$, where (as above) $\circ$ denotes composition of maps in $\text{Aut}\,\mathbf{X}$.

5.1. Transitive G-sets. A representation $\varphi : G \to \text{Aut}\,\mathbf{X}$ defines an action by G on the set X, as follows: $\varphi(g) : x \mapsto x^{\varphi(g)}$. If $\varphi(G) \leqslant \text{Aut}\,\mathbf{X}$ denotes the image of G under φ, we call the algebra $\langle X, \varphi(G)\rangle$ a *G-set*. The action is called *transitive* if for each pair $x, y \in X$ there is some $g \in G$ such that $x^{\varphi(g)} = y$. A group that acts transitively on some set is called a *transitive group*. (Without

specifying the set, however, this term is meaningless, since every group acts transitively on some sets and intransitively on others.) A representation φ is called *transitive* if the resulting action is transitive.

A representation $\varphi : G \to \operatorname{Aut} \mathbf{X}$ is called *faithful* if it is a monomorphism, in which case G is isomorphic to its image under φ, which is a subgroup of $\operatorname{Aut} \mathbf{X}$. We also say, in this case, that the group G acts faithfully, and call it a *permutation group*.

The *degree* of a group action on a set X is the cardinality of X. Finally, a *primitive group* is a group that contains a core-free maximal subgroup.

For our purposes the most important representation of a group G is its action on the set of cosets of a subgroup. That is, for any subgroup $H \leqslant G$, we define a transitive permutation representation of G, which we will denote by ρ_H. Specifically, ρ_H is a group homomorphism from G into the symmetric group $\operatorname{Sym}(G/H)$ of permutations on the set $G/H = \{H, Hx_1, Hx_2, \dots\}$ of *right* cosets of H in G.

When The action is simply right multiplication by elements of G. That is, $(Hx)^{\rho(g)} = Hxg$. Each Hx is a point in the set G/H, and the *point stabilizer* of Hx in G is defined by $G_{Hx} = \{g \in G \mid Hxg = Hx\}$. Notice that $G_H = \{g \in G \mid Hg = H\} = H$ is the point stabilizer of H in G, and

$$G_{Hx} = \{g \in G \mid Hxgx^{-1} = H\} = x^{-1}G_H x = x^{-1}Hx = H^x.$$

Thus, the kernel of the homomorphism ρ is

$$\ker \rho = \{g \in G \mid \forall x \in G,\ Hxg = Hx\} = \bigcap_{x \in G} G_{Hx} = \bigcap_{x \in G} x^{-1}Hx = \bigcap_{x \in G} H^x.$$

Note that $\ker \rho$ is the largest normal subgroup of G contained in H, also known as the *core* of H in G, which we denote by $\operatorname{core}_G(H)$.

If the subgroup H happens to be *core-free*, that is, $\operatorname{core}_G(H) = 1$, then $\rho : G \hookrightarrow \operatorname{Sym}(G/H)$, an embedding, so ρ is a faithful representation; hence G is a permutation group.

`thm:g-set-isomorphism2`

Theorem 5.1 (*G*-set Isomorphism Theorem). *Let $\mathbf{A} = \langle A, G \rangle$ be a transitive G-set and fix $a \in A$. Then the lattice $\operatorname{Con} \mathbf{A}$ is isomorphic to the interval $[\![G_a, G]\!]$ in the subgroup lattice of G.*

Since the foregoing theorem is so central to our work, we provide an alternative statement of it. This is the version typically found in group theory textbooks (e.g., [4]). Keeping these two alternative perspectives in mind can be useful.

Theorem 5.2 (*G*-set Isomorphism Theorem, version 2). *Let $\mathbf{A} = \langle A, \varphi(G) \rangle$ be a transitive G-set and fix $a \in A$. Let $\mathscr{B}$ be the set of all blocks B that contain a. Then there is a bijection $\Psi : \mathscr{B} \to [\![G_a, G]\!]$ given by $\Psi(B) = G(B)$, with inverse mapping $\Phi : [\![G_a, G]\!] \to \mathscr{B}$ given by $\Phi(H) = \{a^{\varphi(h)} \mid h \in H\}$. The mapping Ψ is order-preserving in the sense that $B_1 \subseteq B_2 \Leftrightarrow \Psi(B_1) \leqslant \Psi(B_2)$.*

Briefly, the poset $\langle \mathscr{B}, \subseteq \rangle$ is order-isomorphic to the poset $\langle [G_a, G], \leqslant \rangle$.

Corollary 5.3. *Let G act transitively on a set with at least two points. Then G is primitive if and only if each stabilizer G_a is a maximal subgroup of G.*

Since the point stabilizers of a transitive group are all conjugate, one stabilizer is maximal only when all of the stabilizers are maximal. In particular, a regular permutation group is primitive if and only if it has prime degree.

Next we describe (up to equivalence) all transitive permutation representations of a given group G. We call two representations (or actions) *equivalent* provided the associated G-sets are isomorphic. The foregoing implies that every transitive permutation representation of G is equivalent to $\hat{\lambda}_H$ for some subgroup $H \leqslant G$. The following lemma[5] shows that we need only consider a single representative H from each of the conjugacy classes of subgroups.

Lemma 5.4. *Suppose G acts transitively on two sets, A and B. Fix $a \in A$ and let G_a be the stabilizer of a (under the first action). Then the two actions are equivalent if and only if the subgroup G_a is also a stabilizer under the second action of some point $b \in B$.*

The point stabilizers of the action $\hat{\lambda}_H$ described above are the conjugates of H in G. Therefore, the lemma implies that, for any two subgroups $H, K \leqslant G$, the representations $\hat{\lambda}_H$ and $\hat{\lambda}_K$ are equivalent precisely when $K = xHx^{-1}$ for some $x \in G$. Hence, the transitive permutation representations of G are given, up to equivalence, by $\hat{\lambda}_{K_i}$ as K_i runs over a set of representatives of conjugacy classes of subgroups of G.

TODO: rewrite this section up to this point

5.2. Extensions of the Pálfy Pudlák Theorem. In [11] P. P. Pálfy and P. Pudlák showed the following statements are equivalent:

- every finite lattice is representable, that is $\mathscr{L}$ is all finite lattices;
- every finite lattice is isomorphic to an interval in the subgroup lattice of some finite group.

They did this by giving lattice conditions which force the nonconstant operations of a minimal representation to be permutations which generate a transitive group $\mathbf{G}$. By Theorem 5.1 the congruence lattice of such an algebra is isomorphic to the interval $[\![G_a, G]\!]$. Then they showed every finite lattice could be embedded as an interval into a finite lattice satisfying these conditions. However their equivalence is not global: it is possible that there is a representable lattice which is not isomorphic to an interval of the subgroup lattice of a finite group. So there are several interesting questions we can ask about a finite lattice $\mathbf{L}$:

is mim rep defined?

   (1) Is $\mathbf{L}$ representable (isomorphic to Con $\mathbf{A}$ for some finite algebra $\mathbf{A}$)?
   (2) If $\mathbf{L}$ is representable, what is the minimum size of $\mathbf{A}$ with $\mathbf{L} \cong$ Con $\mathbf{A}$?
   (3) Is there a group $\mathbf{G}$ of permutations on A such that $\mathbf{L} \cong \langle A, G \rangle$?

---

[5]Lemma 1.6B of [4].

    (4) Is there a transitive group **G** of permutations on A such that **L** $\cong$ $\langle A, G \rangle$? Equivalently is **L** isomorphic an interval in the subgroup lattice of a finite group (by Theorem 5.1).

    (5) If **L** $\cong \langle A, G \rangle$ for a group **G** what is the smallest such **G**?

As we mentioned, it is possible that (1) does not imply (4) but certainly (4) implies (1). Obviously we don't have an example of an **L** satisfying (1) but not (4), but in general representing **L** in the form of (4) is more difficult. For example, the lattices $\mathbf{L}_6$ and $\mathbf{L}_7$ diagrammed in Figure 5 can be represented on algebras of size 6 (and no fewer) but representing them with permutation groups is much harder; see Aschbacher [1].
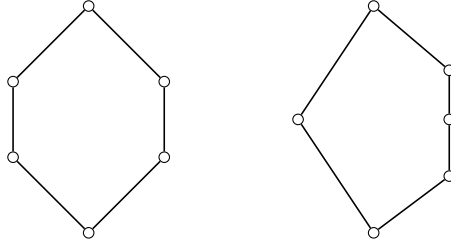
FIGURE 5. $\mathbf{L}_6$ and $\mathbf{L}_7$ fig:L6and7

Below we try to answer at least some of these questions for small lattices. As mentioned above Pálfy and Pudlák gave conditions on a lattice **L** such that if $\mathbf{L} \cong \mathrm{Con}\,\langle A, F \rangle$ then the nonconstant elements of F are permutations and the group they generate acts transitively on A. These conditions are

(A) **L** is simple.
(B) For each $x \neq 0$ in L, there are elements y and z such that $x \vee y = x \vee z = 1$ and $y \wedge z = 0$.
(C) $|L| \neq 2$ and each element of L that is not an atom or 0 contains at least four atoms.

If (A) and (B) hold then all nonconstant elements of F are permutations.

Let (B′) and (B″) be the conditions related to (B) found in McKenzie's paper [7]:

(B′) If $\varphi : L \to L$ is any meet-preserving map such that $\varphi(x) > x$ for $x \neq 1$, then $\varphi(x) = 1$ for all x.
(B″) The coatoms of **L** meet to 0.

Note that

$$(\mathrm{B}) \implies (\mathrm{B}'') \implies (\mathrm{B}').$$

Clearly (B″) implies (B′). To see that (B) implies (B″), let x be the meet of all the coatoms of **L**. If $x > 0$ then applying (B) gives y and z each joining with x to 1. But $x \vee y = 1$ implies $y = 1$. Similarly $z = 1$. But then $0 = y \wedge z = 1$.

McKenzie proves in [7] that, just like (A) and (B), (A) and (B′) imply that all nonconstant members of F are permutation. We record this as a theorem.

Theorem 5.5 (Pálfy-Pudlák [11], McKenzie [7])**.** *Let* **L** *be finite lattice and suppose* $\mathbf{L} \cong \operatorname{Con} \langle A, F \rangle$ *is a minimal representation. If* **L** *satisfies* (A) *and* (B′) *then all the nonconstant members of* F *are permutations. The same conclusion obtains if* **L** *satisfies* (A) *and either* (B) *or* (B″)*.*

As we mentioned, if condition (C) is also assumed to hold then F generates a transitive permutation group on A. This served well for the proof of the Pálfy-Pudĺak Theorem. But few lattices satisfy (C) so we seek something more general that guarentees the action is transitive. To do this we investigate properites of $\operatorname{Con} \langle A, G \rangle$ where G is a group that acts intransitively on A. It turns out such lattices are rather rare.

5.3. Intransitive group actions. Suppose $\mathbf{A} = \langle A, G \rangle$ is a G-set and let $\mathbf{A}_i = \langle A_i, G \rangle$, $i < k$, be the minimal subalgebras of $\mathbf{A}$; i.e. each set A_i is an orbit, or one-generated subuniverse, of $\mathbf{A}$. Define congruences on A by the partitions

$$\tau = |A_0|A_1| \cdots |A_{k-1}| \quad \text{(the blocks are the orbits)}$$
$$\tau_i = |A_i| \quad\quad\quad\quad\quad\quad\text{(at most one nontrivial block)}$$
$$\gamma_i = |A_i|A - A_i| \quad\quad\text{(exactly two blocks unless } A_i = A)$$

So $(a, b) \in \tau$ if and only if they both lie in the same orbit; $(a, b) \in \tau_i$ if and only if $a = b$ or both lie in A_i; $(a, b) \in \gamma_i$ if and only if both lie in A_i or both don't. We call τ the *intransitivity congruence*; G acts transitively if and only if $\tau = 1$.

| `thm:intrans` |

Theorem 5.6. *Let* $\mathbf{A} = \langle A, G \rangle$, *where* G *is a group, be a finite algebra. Let* τ, τ_i *and* γ_i *be the congruences defined above and let* $\theta \in \operatorname{Con} \mathbf{A}$.

`item1`	*(1) G acts transitively if and only if $\tau = 1_{\mathbf{A}}$.*
`item2`	*(2) The interval $[\![\tau, 1_{\mathbf{A}}]\!]$ is isomorphic to $\operatorname{Eq}(k)$.*
`item3`	*(3) The interval $[\![0_{\mathbf{A}}, \tau]\!]$ is isomorphic to $\prod_{i=0}^{k-1} \operatorname{Con}(A_i)$.*
`item4`	*(4) If, for some i, $\theta \geq \bigvee_{j \neq i} \tau_j$ then $\theta \geq \tau$ or $\theta \leq \gamma_i$.*
`item5`	*(5) If $\theta \wedge \tau \prec \tau$ then $\theta \leq \gamma_i$ for some i.*
`item6`	*(6) If $k > 1$ and $|A_i| = 1$ for all i except 0 then every coatom of $\operatorname{Con} \mathbf{A}$ lies above τ.*
`item7`	*(7) If $k > 1$ and $[\![0_{\mathbf{A}}, \tau]\!]$ is directly indecomposable then every coatom of $\operatorname{Con} \mathbf{A}$ lies above τ.*
`item8`	*(8) If $k = 2$ and $|A_1| = 1$ then τ is a coatom and everything is comparable with it.*
`item9`	*(9) If τ is a coatom and $[\![0_{\mathbf{A}}, \tau]\!]$ is directly indecomposable then everything is comparable with it.*

Proof. (1) is obvious. Since G acts trivially on $\mathbf{A}/\tau$, $\operatorname{Con}(\mathbf{A}/\tau)$ is the lattice of all partitions; that is, $\operatorname{Eq}(k)$. So (2) holds. For (3), we map $(\theta_0, \ldots, \theta_{k-1}) \in \prod_{i=0}^{k-1} \operatorname{Con}(A_i)$ to $\theta_0 \cup \cdots \cup \theta_{k-1}$. It is straightforward to to verify that this is an

isomorphism into $[\![0_{\mathbf{A}}, \tau]\!]$. The inverse map sends $\theta \in [\![0_{\mathbf{A}}, \tau]\!]$ to $(\theta_0, \ldots, \theta_{k-1})$, where $\theta_i = \theta \cap (A_i \times A_i)$. The details are left to the reader.

For (4) note that if $\theta \nleq \gamma_i$, then there are elements $a \in A_i$ and $b \notin A_i$ with $(a, b) \in \theta$. Let $b \in A_j$. Of course $j \neq i$. Let a' be any other element in A_i. Then, since G acts transitively on A_i, there is a $\sigma \in G$ with $\sigma(a) = a'$. Let $b' = \sigma(b)$ and note $b' \in A_j$ so $(b, b') \in \theta$ because $\theta \geq \bigvee_{r \neq i} \tau_r \geq \tau_j$. Now $(a', b') = (\sigma a, \sigma b) \in \theta$. So (a, b), (b, b') and (a', b') are all in θ. Hence $(a, a') \in \theta$. Since a' was arbitrary, we see $\theta \geq \tau_i$. So $\theta \geq \tau$, as desired.

(5) follows from (4). If $|A_i| = 1$ for $i > 0$ then $\tau_i = 0_{\mathbf{A}}$ for these i's. Hence $\bigvee_{i \neq 0} \tau_i = 0_{\mathbf{A}}$ and the result follows from (4) again. If $[\![0_{\mathbf{A}}, \tau]\!]$ is directly indecomposable, then, by (3), $|A_i| = 1$ for all but at most one i. So (7) follows from (6).

For (8), that τ is a coatom follows from (2). By (6), τ is the only coatom. The result follows from this. (9) follows from (8). $\hspace{2cm} \square$

5.4. Examples. We give some examples showing the uses of Theorem 5.6. In deciding if a lattice has a representation using an intransitive permutation group, we consider the possibilities for τ. By (2) of Theorem 5.6 the filter above τ must be isomorphic to a partition lattice. In particular, if the lattice has no filter isomorphic to $\mathbf{M}_3 \cong \mathrm{Eq}(3)$, then the only candidates for τ are the coatoms. When τ is a coatom, $k = 2$ by (2) and $\gamma_0 = \gamma_1 = \tau$
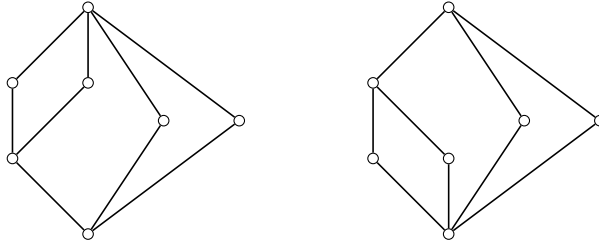
FIGURE 6. $\mathbf{L}_{14}$ (on the left) and $\mathbf{L}_{15}$ `fig:L14and15`

Consider the lattices $\mathbf{L}_{14}$ and its dual $\mathbf{L}_{15}$ of Figure 6. Since neither has $\mathbf{M}_3$ as a filter, the only possibilities for τ are cotatoms. For $\mathbf{L}_{14}$ the ideals below each of the coatoms is directly indecomposable so, by Theorem 5.6(9), it cannot be represented with a nontransitive permutation group. Conditions (A) and (B″) do hold and hence a minimal representation of $\mathbf{L}_{14}$ must be by a transitive group. (More precisely, if $\mathbf{L}_{14} \cong \mathrm{Con}\,\langle A, F \rangle$ then the nonconstant members of F generate a transitive permutation group.) In fact the first author has shown there is a subgroup H of A_6 of index 90 so that the interval of subgroups of A_6 containing H (the lattice of overgroups of H in A_6) is $\mathbf{L}_{14}$. Of course in this example the algebra has size 90; we do not know if this is the smallest example.

On the other hand the leftmost coatom of $\mathbf{L}_{15}$ is a candidate for τ and in fact $\mathbf{L}_{15}$ is the congruence of $\langle A, F \rangle$ where $A = \{0, 1, 2, 3\}$ and $F = \{f\}$ where f is the double transposition interchanging 0 and 1 and also 2 and 3. Conditions (A) and (B″) hold here too so the nonconstant operations of a minimal representation must be permutation. Clearly $\langle A, F \rangle$ is the minimal representation.

As we shall outline below, we have shown every lattice of size at most 7 elements is representable with only one possible exception: $\mathbf{L}_{10}$ diagrammed in Figure 7.
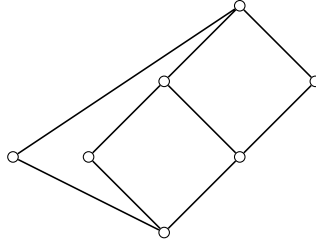
FIGURE 7. $\mathbf{L}_{10}$ fig:L10

This lattice cannot be represented using an intransitive permutation group. By Theorem 5.6(9), τ cannot be the leftmost or rightmost coatom. Suppose τ is the middle coatom. As mentioned above this implies $\gamma_0 = \gamma_1 = \tau$. Letting θ be the rightmost coatom we see that (5) is violated. $\mathbf{L}_{10}$ satisfies (A) and (B″) and thus a minimal representation, if one exists, must be by a transitive permutation group.

In Figure XXXX below all nondistributive lattices of size 7 or less which are not an ordinal sum are diagrammed. Very few of these can have a representation using a nontransitive group. The lattices $\mathbf{L}_2 = \mathbf{M}_3$, $\mathbf{L}_5$, $\mathbf{L}_{15}$, and $\mathbf{L}_{34}$ can be represented with an intransitive group. The algebra given in the figure for $\mathbf{L}_5$ is a minimal representation and does not generate a group. But it does have an intranstive representation on a six element set with the operations $(1, 2, 0, 4, 5, 3)$ and $(0, 1, 2, 3, 5, 4)$.

Using techniques similar to those above, one can prove that all of the remaining lattices cannot have a represnetation with an intransitive group. The one difficult case is $\mathbf{L}_{19}$ of Figure 8. Lemma 5.7 below covers this case.

lemma:complements   **Lemma 5.7.** *Let $\mathbf{A} = \langle A, G \rangle$ be a finite algebra, where G is an instransitive group of permutations on A. Suppose the intransitivity congruence τ is a coatom. Then there do not exist congruences $0_{\mathbf{A}} < \psi < \theta$ in Con $\mathbf{A}$ with $\theta \wedge \tau = 0_{\mathbf{A}}$.*

Proof. Since τ is a coatom, there are exactly two orbits; call them B and C. Since $\theta \wedge \tau = 0_{\mathbf{A}}$, if $(x, y) \in \theta$ then $x = y$ or one is in B and the other is in C. So θ defines a bipartite graph between B and C. Since G acts transitively on
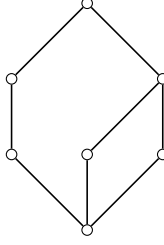
FIGURE 8. $\mathbf{L}_{19}$

both B and C, this graph corresponds to a bijection between B and C. The same applies to ψ. But equivalence relations corresponding to such graphs cannot be comparable. □

In [15] John Shareshian gave a class of finite lattices that he conjectured could not be represented as intervals in subgroup lattices. They are easy to describe. Let $m_1 \geq \cdots \geq m_t \geq 3$ with $t > 1$. Take the t lattices of subsets of sets of sizes m_i, $i = 1, \ldots, t$, remove the least and greatest element of each, line them up side by side, and add a new least and greatest element. While this conjecture is still open, much progress has been made, primarily by Aschbacher; see [2]. For example, the problem has been reduced to almost simple groups.

Arguments similar to those for $\mathbf{L}_{10}$ show that none of these lattices can be represented with an intransitive permutation group. They also satisfy (A) and (B″) so a minimal representation, if it exists, must be with a transitive group. Hence if any of Shareshian's lattices cannot be represented as an interval in a finite group, then that lattice has no (finite) representation at all.

Next consider $\mathbf{L}_{11}$ diagrammed in Figure 9. Again we can use Theorem 5.6(9) to show that it cannot be represented using an intransitive permutation group. However (A) and (B′) do not hold so we cannot conclude that a minimal representation is by a transitive permutation group. Nevertheless, with some help from GAP, we are able to show that it can be represented as an interval in the lattice of subgroups of a group. We do not know if this is the smallest representation.

We start with the group representation of the pentagon as the upper interval $[\![H, G]\!]$ where $G \cong ((C_3 \times C_3) : Q_8) : C_3$ and $H \cong C_6$. Here C_k denotes the cyclic group of order k, Q_8 denotes the quaternion group of order 8, and : denotes the usual semidirect product. We let $\alpha \prec \beta$ and γ denote the three subgroups inside the pentagon $[\![H, G]\!]$, as shown in the diagram below.

The entire subgroup lattice $\mathrm{Sub}[G]$ is the congruence lattice of an algebra. Therefore, if there is a minimal subgroup K ($1 \prec K \leqslant G$) that is below β, but not below α or γ, then lattice L_{11} is the union of the ideal $[\![1, K]\!]$ and the filter $[\![H, G]\!]$. This portion of $\mathrm{Sub}[G]$ is shown here:
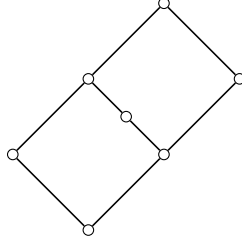
FIGURE 9. $\mathbf{L}_{11}$
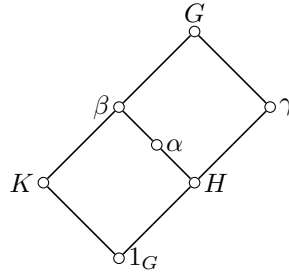
FIGURE 10.

Luckily, there is such a subgroup K. We can check this fact using GAP, as we now describe. A search of the GAP Library of Small Groups finds that the 153rd isomorphism class of groups of order 216—that is, the group returned by the function call `SmallGroup( 216, 153 )`—has structure description $((C_3 \times C_3) : Q_8) : C_3$. Upon inspection of the conjugacy classes of subgroups of this group, we find that the representative of the 8th class is a suitable candidate for H, so we define

```
G := SmallGroup( 216, 153 );;
ccsg := ConjugacyClassesSubgroups( G );;
H := Representative( ccsg[8] );
intHG := IntermediateSubgroups( G, H );
```

The last of these commands results in the following output:

```
rec(
     subgroups := [ Group([ f1, f4, f5*f6 ]),
                    Group([ f1, f2, f3*f4, f4 ]),
                    Group([ f1, f4, f5, f6 ]) ],

     inclusions := [ [ 0, 1 ], [ 0, 2 ], [ 1, 3 ],
                     [ 2, 4 ], [ 3, 4 ] ]
   )
```

This is a record where the `subgroups` field is a list of the subgroups K that lie strictly between H and G, that is, $H < K < G$, and the `inclusions`

field indicates the covering relations among the subgroups. GAP uses indices $0, 1, \ldots, 4$ to label the subgroups in $[\![H, G]\!]$, and

in the `inclusions` field the entry [1, 3], for example, indicates that `Group([ f1, f4, f5*f6 ])` is a maximal subgroup of `Group([ f1, f4, f5, f6 ])`. Therefore, the GAP output above shows that the interval $[\![H, G]\!]$ is a pentagon.

Next, we make the following definitions

```
A:=intHG.subgroups[1];   B:=intHG.subgroups[3];   C:=intHG.subgroups[2];
```

TODO: complete this section

6. Small unary algebras for congruence lattices of size ≤ 7

Distributive lattices and lattices that are ordinal sums of smaller lattices are omitted. The base set of each algebra is $\{0, 1, \ldots, n - 1\}$, and each unary operation is specified by a vector of values of these elements. Algebras of size less than 11 are known to be minimal-size algebras that produce the corresponding congruence lattice. The algebra for 33 (M_5) is also known to be minimal in size. Currently only one of the lattices (10) is not known to be the congruence lattice of a finite algebra.

x	0	1	2	3
$f(x)$	1	0	3	2
$g(x)$	1	0	1	0

1 2|3 4

1 3|2 4

1|2|3 4

1 (N_5)
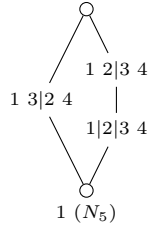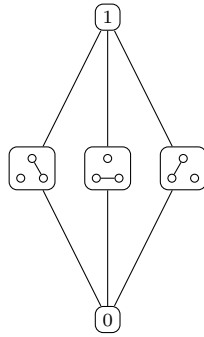
(1,0,3,2)
(2,3,0,1)

2 (M_3)

$p_0 = (0,1,2,1,2,1,0)$
$p_1 = (0,3,4,3,4,3,0)$
$p_2 = (6,5,2,5,2,5,6)$
$p_3 = (0,1,2,0,0,2,2)$
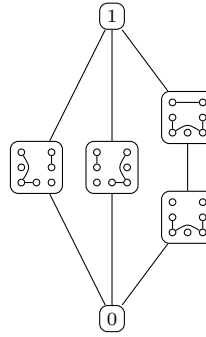
3 (V_1)

(1,2,3,4,5,0,7,8,9,10,11,6)
(6,11,10,9,8,7,0,5,4,3,2,1)
(0, 0, 0,6,0,0,0,0,6,0,0,0)
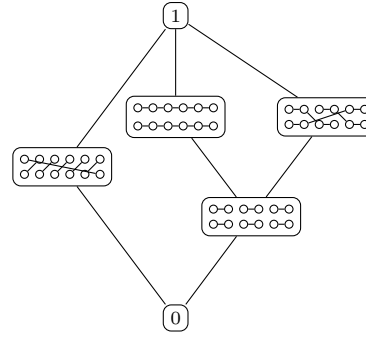
4 (L_5)

(1,0,3,2)
(0,0,2,2)
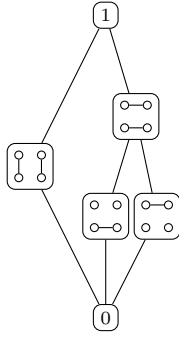
5 (L_4)

(2,2,1,5,5,4)
(3,4,4,0,1,1)
(4,5,3,4,5,3)
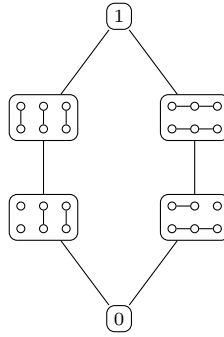
6

(1,0,0,4,3,3)
(4,5,5,1,2,2)
(3,3,4,3,3,4)
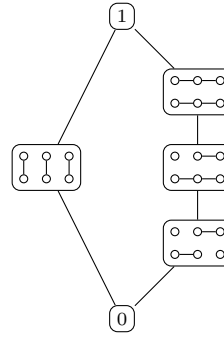
7

(1,2,0,4,5,3)
(3,5,4,0,2,1)
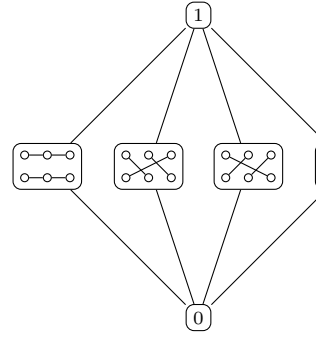
8 (M_4)

(0,0,0,0,0,0,2,1,2,1,3,4,5,3,4,5)
(0,0,0,0,0,0,6,7,6,7,10,11,12,10,11,12)
(13,14,15,1,9,8,15,14,13,15,1,9,8,8,1,9)
(R. Freese "rabbit ears")

9

(0,0,3,3,3,6,6,6,0)
(0,0,8,8,8,1,1,1,0)
(0,5,5,4,0,0,5,4,4)
(4,2,2,3,4,4,2,3,3)
(5,5,7,7,7,6,6,6,5)
(found by W. DeMeo)
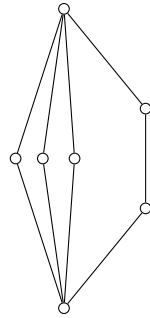
No finite algebra
known with this
congruence lattice
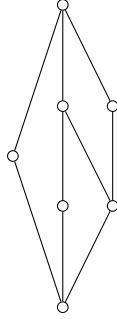
Finite algebra with
108 elements known (W. DeMeo)

10

11
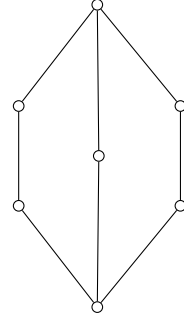
12

(0,1,2,1,2,1,0,0,1,2,2,1,0,0,1,2,1,2,0)
(0,1,2,0,0,2,2,0,3,4,0,4,4,6,5,2,6,6,2)
(0,1,2,3,4,5,6,0,1,2,4,5,6,0,1,2,3,4,6)
(7,8,9,3,10,11,12,3,3,3,3,3,3,11,11,11,
11,11,11),(13,14,15,16,17,5,18,13,16,17,
17,16,13,5,5,5,5,5,5)("rabbit ears")
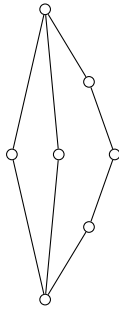
Upper interval in Sub(A_6)
algebra of size 90 (W. DeMeo)

(1,0,3,2)

13

14
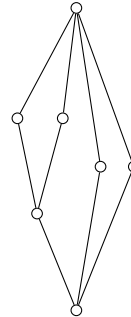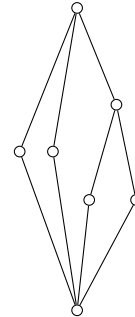
15

Upper interval in Sub($C_2.A_6$)
algebra of size 180 (W. DeMeo)
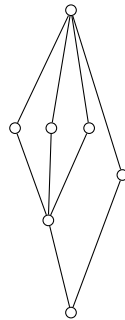
(1,0,3,2,5,4,7,6,9,8,11,10)
(4,7,5,6,8,11,9,10,0,3,1,2)
(0,0,0,0,5,5,5,5,10,10,10,10)
(W. DeMeo, filter-ideal in Sub(A_4))
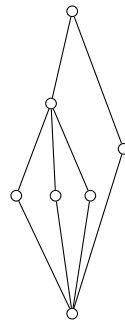
Dual of 19, no explicit
small representation known?

16

17
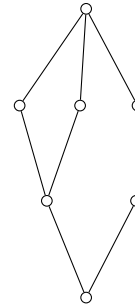
18

(0,1,1,0,4,5,5,4)
(0,2,3,1,0,2,3,1)
(7,6,6,7,3,2,2,3)
(P. Jipsen, search in Equ(8))
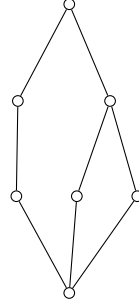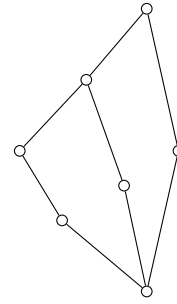
(W. DeMeo in GAP
SmallGroup(216,153))
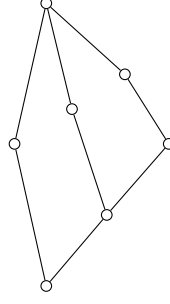
(3,3,4,8,8,2,2,3,4)
(0,0,6,1,1,0,0,5,6)
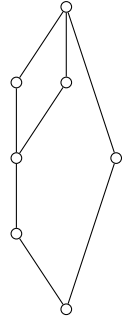(4,5,5,7,8,8,7,4,4)
(R. Freese, in Equ(9))

19

20

21

Dual of 23, no
explicit small
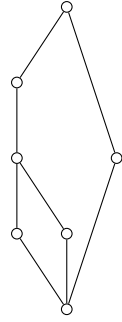representation
known?

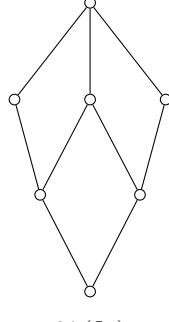(0,1,0,1,4,4)
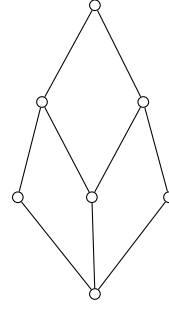(1,1,3,3,4,5)
(3,2,3,2,5,5)
(4,1,5,3,4,5)

(1,1,2,2)
(2,3,3,2)

(0,0,2,2,2)
(0,1,0,1,1)
(1,1,4,4,4)
(2,3,2,3,3)

(1,0,3,2,0,2)
(4,4,5,5,1,3)
(0,0,0,0,1,1)
(3,5,3,5,3,3)

22

23

24 (L_2)

25 (L_1)

26
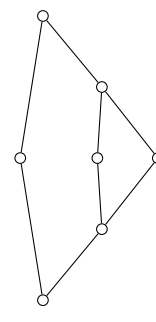
(0,1,2,3,4,5,0,0,0,0,0,2,2,2,2,2)
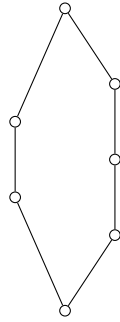(4,5,3,4,5,3,5,3,4,5,3,4,5,4,5,3)
(2,2,1,5,5,4,2,1,5,5,4,2,2,5,5,4)
(3,4,4,0,1,1,4,4,0,1,1,3,4,0,1,1)
(0,6,7,8,9,10,6,7,8,9,10,0,6,8,9,10)
(11,12,2,13,14,15,12,2,13,14,15,
11,12,13,14,15) ("rabbit ears")

(0,1,2,3,4,5,0,0,0,0,0,2,2,2,2,2)
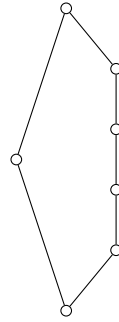(3,3,4,3,3,4,3,4,3,3,4,3,3,3,3,4)
(1,0,0,4,3,3,0,0,4,3,3,1,0,4,3,3)
(4,5,5,1,2,2,5,5,1,2,2,4,5,1,2,2)
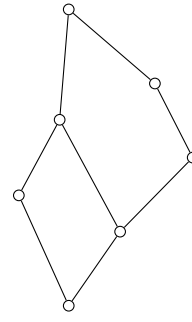(0,6,7,8,9,10,6,7,8,9,10,0,6,8,9,10)
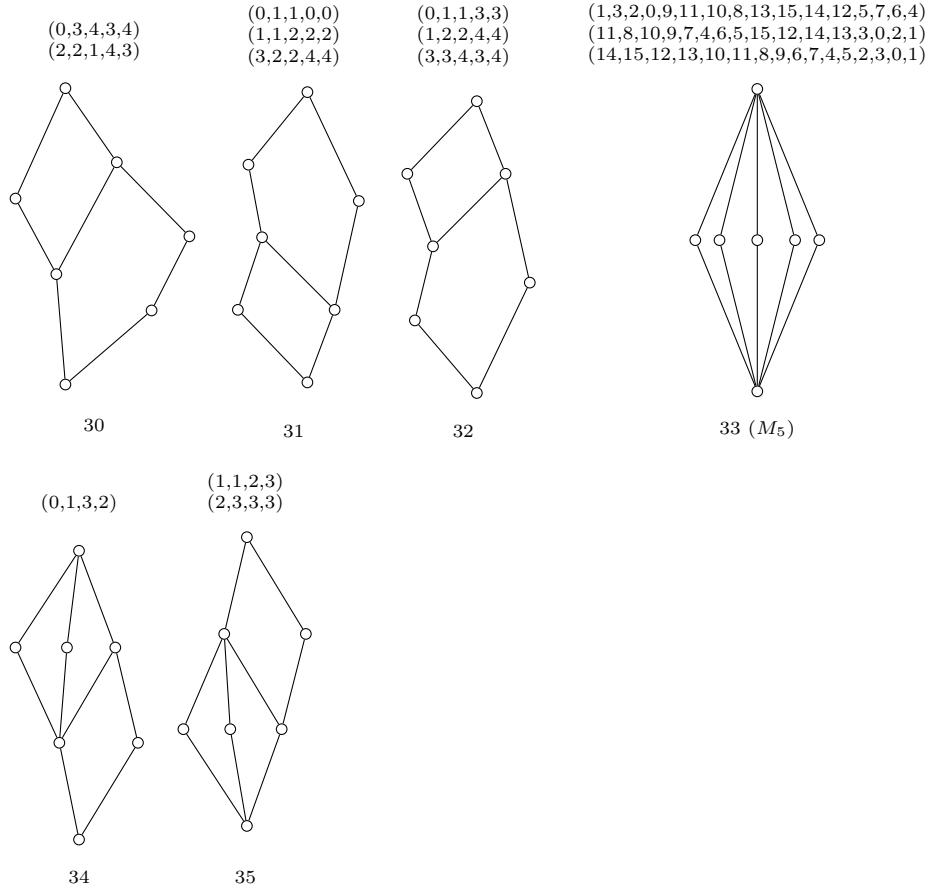(11,12,2,13,14,15,12,2,13,14,15,
11,12,13,14,15) ("rabbit ears")

(1,0,3,2,2)
(2,4,2,4,3)

27

28

29

(0,3,4,3,4) (0,1,1,0,0) (0,1,1,3,3) (1,3,2,0,9,11,10,8,13,15,14,12,5,7,6,4)
(2,2,1,4,3) (1,1,2,2,2) (1,2,2,4,4) (11,8,10,9,7,4,6,5,15,12,14,13,3,0,2,1)
             (3,2,2,4,4) (3,3,4,3,4) (14,15,12,13,10,11,8,9,6,7,4,5,2,3,0,1)

        30   31   32   33 (M_5)

(0,1,3,2)   (1,1,2,3)
             (2,3,3,3)

        34   35

REFERENCES

Aschbacher2008 [1] Michael Aschbacher. On intervals in subgroup lattices of finite groups. *J. Amer. Math. Soc.*, 21(3):809–830, 2008.

Aschbacher2013 [2] Michael Aschbacher. Overgroup lattices in finite groups of Lie type containing a parabolic. *J. Algebra*, 382:71–99, 2013.

Berman:1970 [3] Joel Berman. *Congruence lattices of finite universal algebras.* PhD thesis, University of Washington, 1970.

Dixon:1996 [4] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1996.

Jonsson:1972 [5] Bjarni Jónsson. *Topics in universal algebra.* Lecture Notes in Mathematics, Vol. 250. Springer-Verlag, Berlin, 1972.

Kurzweil:1985 [6] Hans Kurzweil. Endliche Gruppen mit vielen Untergruppen. *J. Reine Angew. Math.*, 356:140–160, 1985.

McKenzie1983 [7] R. McKenzie. Finite forbidden lattices. In R. Freese and O. Garcia, editors, *Universal Algebra and Lattice Theory*, pages 176–205. Springer-Verlag, New York, 1983. Lecture notes in Mathematics, vol. **1004**.

McKenzie:1984 [8] Ralph McKenzie. A new product of algebras and a type reduction theorem. *Algebra Universalis*, 18(1):29–69, 1984.

alvi:1987 [9] Ralph N. McKenzie, George F. McNulty, and Walter F. Taylor. *Algebras, lattices, varieties. Vol. I.* Wadsworth & Brooks/Cole, Monterey, CA, 1987.

Netter:1986 [10] R. Netter. Eine bemerkung zu kongruenzverbanden. preprint, 1986.

PalfyPudlak1980   [11] P. P. Pálfy and P. Pudlák. Congruence lattices of finite algebras and intervals in
                       subgroup lattices of finite groups. *Algebra Universalis*, 11:22–27, 1980.

Palfy:2009   [12] Péter Pál Pálfy. The finite congruence lattice problem, September 2009. Summer
                       School on General Algebra and Ordered Sets Stará Lesná, 6, 2009.

Pudlak:1980   [13] Pavel Pudlák and Jiří Tůma. Every finite lattice can be embedded in a finite partition
                       lattice. *Algebra Universalis*, 10(1):74–95, 1980.

Quack:1971   [14] R. Quackenbush and B. Wolk. Strong representation of congruence lattices. *Algebra
                       Universalis*, 1:165–166, 1971/72.

Shareshian2003   [15] John Shareshian. Topology of order complexes of intervals in subgroup lattices. *J.
                       Algebra*, 268(2):677–686, 2003.

Snow:2000   [16] John W. Snow. A constructive approach to the finite congruence lattice representation
                       problem. *Algebra Universalis*, 43(2-3):279–293, 2000.

Tuma:1986   [17] Jiří Tůma. Some finite congruence lattices. I. *Czechoslovak Math. J.*,
                       36(111)(2):298–330, 1986.

WILLIAM DeMEO

   Department of Mathematics, Iowa State University, Ames 50010, USA
   e-mail: williamdemeo@gmail.com
   URL: http://williamdemeo.github.io

RALPH FREESE

   Department of Mathematics, University of Hawaii, Honolulu 96822, USA
   e-mail: ralph@math.hawaii.edu
   URL: http://www.math.hawaii.edu/~ralph/

PETER JIPSEN

   School of Computational Sciences, Chapman University, Orange 92866, USA
   e-mail: jipsen@chapman.edu
   URL: http://www1.chapman.edu/~jipsen/