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

By the Gratzër-Schmidt Theorem every algebraic, and hence every finite, lattice is the congruence lattice of an algebra. But the algebras in this construction are always infinite even when the lattice is finite. This leaves open the question: *is every finite lattice isomorphic to the congruence lattice of a finite algebra?* In 1980 P. P. Pálfy and P. Pudlák reduced this to a group theoretic problem by showing the following two statements are equivalent.

(1) Every finite lattice is isomorphic to the congruence lattice of a finite algebra.
(2) Every finite lattice is isomorphic to an interval in the subgroups lattice of a finite group.

If L is isomorphic to the lattice of subgroups of G containing a subgroup H, then L is isomorphic to the congruence lattice of the algebra whose elements are the left cosets of H and whose operations are left multiplication by elements of G; that is, the group action of G on the left cosets of H; see [3, 11]. Conversely, if $\mathbf{A} = \langle A, F\rangle$ is a finite algebra with each element of F a permutation on A, then the congruence lattice $\mathrm{Con}(\mathbf{A})$ of $\mathbf{A}$ is isomorphic to the lattice of all subgroups of G containing H (the overgroups of H in G), where G is the group generated by F and $H = G_a$ is the stabilizer of a point.

On the other hand, the Pálfy-Pudlák theorem does not prove that if a particular lattice L is a congruence lattice of a finite algebra then it is (isomorphic to) an interval of a subgroup lattice of a finite group so it is possible that there is a congruence lattice L of a finite algebra that is not an interval sublattice of a finite group.

Presented by ...
Received ...; accepted in final form ...
2010 *Mathematics Subject Classification*: Primary: 08A30; Secondary: 06B15, 08A60, 06B10, 20D30.
Key words and phrases: congruence lattice, subgroup lattice, finite algebra, finite lattice representations.

In this paper we review some of the well known methods, as well as some more recently developed methods, for constructing a finite algebra whose congruence lattice is isomorphic to a given finite lattice. Using these methods we show that with one possible exception ($\mathbf{L}_{10}$ in the last section) every lattice with at most 7 elements is (isomorphic to) the congruence lattice of a finite lattice. In most but not all cases we are able to show that the algebra we construct is of minimal size. (Section 1.2 below explains what we mean by *size* of a representation.)

We call a (finite) lattice *group representable* if it is isomorphic to an interval in the subgroup lattice of a (finite) group. That is, L is group representable if there exist groups $H \leqslant G$ such that L is isomorphic to the interval

$$[\![H, G]\!] := \{K \mid H \leqslant K \leqslant G\}. \tag{1.1}$$ eq:1

In this case, we call $[\![H, G]\!]$ a *group representation of* L. We take the *size* of a group representation to be the index $[G : H]$, since this is the size of the algebra $\mathbf{A} = \langle G/H, G\rangle$ that has congruence lattice $\mathrm{Con}(\mathbf{A}) \cong L$.

Not surprisingly many lattices with a group representation can also be represented as a congruence lattice of a much smaller algebra. For example, the hexagon lattice, denoted $\mathbf{L}_6$ in Section 6 below, is the congruence lattice of an algebra with 6 elements. Palfy [13] and Aschbacher [1] have found groups $H < G$ such that the interval from H to G is $\mathbf{L}_6$, but $[G : H]$, which is the size of the algebra, is considerably larger.

Another interesting example is the pentagon, which is typically denoted by N_5, but in our table in Section 6 we label it $\mathbf{L}_1$. A search of GAPs Small Groups Library [6] reveals that the smallest group G in whose subgroup lattice N_5 appears as an upper interval is `SmallGroup(216,153)`. It is easy to verify that there is a six-element subgroup $H \leqslant G$ such that $[\![H, G]\!] \cong N_5$, so the index is $[G : H] = 36$. Therefore, the algebra given by this group representation has 36 elements in this case. (We do not know if this is the smallest possible group representation of N_5.) On the other hand, the smallest algebra that represents N_5 has just four elements. (See Section 6.)

TODO: Add appendix section that includes GAP code for finding upper intervals so the reader can verify that SmallGroup(216,153) is the smallest group with pentagonal upper interval.

For some lattices it can be shown that in a minimal representation every nonconstant operation must be a permutation. For such a lattice L, a minimal representation comes from a group G acting on a set X, which is a group representation of the type described in (1.1). Specifically, $L \cong [\![G_x, G]\!]$, where G_x denotes the stabilizer of an arbitrary element $x \in X$. Finding a representation is typically harder in such cases, and finding a minimal representation can be especially hard.

In Section 5 we investigate when a lattice can be represented by an intransitive group acting instransitively on a set. We show that most lattices can never be so represented. For such lattices group representations must use transitive groups and so the action is isomorphic to a group acting on the cosets of a subgroup by left multiplication. For example, $\mathbf{L}_6$ is in this category.

For the 7-element lattice not known to be representable, $\mathbf{L}_{10}$, we show that a minimal size representation must be via a transitive permutation group action.

TODO: check the gg statement
(wjd: I don't know what the "gg statement" is.)

TODO: Expand the introduction.

1.1. Notation. A lattice is denoted by $\mathbf{L} = \langle L, \wedge, \vee \rangle$, where L is the universe of elements of the lattice. However, unless the context calls for emphasizing that this is an algebraic structure, we often refer to a lattice by the name of its universe. (Notable exceptions to this convention are lattices with special names like those appearing in the list in Section . These are always typeset in bold font.)

sec:small-unary-algebras

We use $\mathcal{L}_{fin}$ to denote the class of all finite lattices, and $\mathcal{L}_{con}$ to denote the class of finite lattices that are isomorphic to congruence lattices of finite algebras. The notation $\mathcal{L}_{grp}$ will stand for the class of finite lattices that are isomorphic to intervals in subgroup lattices of finite groups. A lattice that belongs to $\mathcal{L}_{con}$ (resp., $\mathcal{L}_{grp}$) is called *representable* (resp., *group representable*). Since we use these special notations so often in the sequel, let us repeat them here for easy reference:

$$\mathcal{L}_{fin} = \text{ all finite lattices}$$
$$\mathcal{L}_{con} = \{L \in \mathcal{L}_{fin} \mid \exists \text{ finite algebra } \mathbf{A} \text{ such that } L \cong \operatorname{Con}(\mathbf{A})\}$$
$$\mathcal{L}_{grp} = \{L \in \mathcal{L}_{fin} \mid \exists \text{ finite groups } H \leqslant G \text{ such that } L \cong [\![H, G]\!]\}$$

Let L be a lattice and suppose α and β are members of 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, $[\![\alpha, \beta]\!] = \{\theta \in L \mid \alpha \leqslant \theta \leqslant \beta\}$. (If $\alpha \nleqslant \beta$, then $[\![\alpha, \beta]\!] = \emptyset$.)

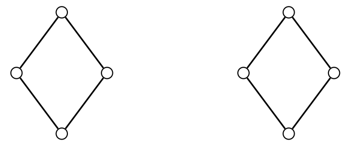
For a lattice (or, more generally, a partially ordered set) L, the *dual* of L, denoted L', is the lattice (poset) with the inverse order. That is, $x \leqslant y$ holds in L if and only if $y \leqslant x$ holds in L'. The dual of L can be depicted by flipping the Hasse diagram for L upside down. In a broader sense, two lattices (posets) are also said to be duals if they are dually isomorphic.

sec:minim-repr

1.2. Minimal Representations. We now define the "size" of a representation and explain what we mean by a "minimal" representation. The *size* of a representation $\operatorname{Con}(\mathbf{A}) \cong L$ is the cardinality $|A|$ of the universe of $\mathbf{A}$. We call such a representation *minimal* if $\operatorname{Con}(\mathbf{B}) \cong L$ implies $|A| \leqslant |B|$.

Suppose $L \in \mathcal{L}_{grp}$. We could ask, what is the smallest group G such that $L \cong [\![H, G]\!]$ for some $H \leqslant G$? From our perspective, the more relevant question is what is the smallest number n such that there are finite groups $H \leqslant G$ with index $n = [G : H]$ and satisfying $L \cong [\![H, G]\!]$? The reason this question seems

Figure 1. Transitive G-set congruence lattices in Eq(10) fig:10



$[\![C_2, C_3 \times S_3]\!]$ TransitiveGroup(9,4) $\quad$ $[\![\langle e\rangle, C_{10}]\!]$ TransitiveGroup(10,1)

more natural to us is because the algebra representing L is the group G acting on the set of cosets of H, and this algebra has $n = [G : H]$ elements. In this context, the index $[G : H]$ seems more relevant than the size of the group G.

Now, suppose G is a group of minimal order among those in whose subgroup lattices L appears as an upper interval, say $L \cong [\![H, G]\!]$. It's possible that there is a larger group G^+ in whose subgroup lattice L appears, but with a smaller index. That is, we may have

$$[\![H, G]\!] \cong L \cong [\![H^+, G^+]\!], \quad |G| < |G^+|, \quad [G^+ : H^+] < [G : H].$$

We now give an example of this phenomenon.

In Figure 1 there appears the lattice $\mathbf{2} \times \mathbf{2}$. On the left, this lattice is presented as the upper interval $[\![C_2, C_3 \times S_3]\!]$. On the right, it is the upper interval $[\![\langle e\rangle, C_{10}]\!]$. Of course, the groups C_{10} and $C_3 \times S_3$ have orders 10 and 18, but the respective indices are $[C_{10} : \langle e\rangle] = 10$ and $[C_3 \times S_3 : C_2] = 9$.

2. Closure properties of the class of representable lattices

sec:clos-prop-class

This section describes some *closure properties* of the class $\mathcal{L}_{con}$ of representable lattices. 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 $\mathcal{L}_{con}$ is *closed under* O provided $\mathsf{O}(\mathcal{K}) \subseteq \mathcal{L}_{con}$ for all $\mathcal{K} \subseteq \mathcal{L}_{con}$. For example, if $\mathsf{S}(\mathcal{K})$ is all sublattices of lattices in $\mathcal{K}$, it is unknown whether $\mathcal{L}_{con}$ 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 $\mathrm{Eq}(X)$. By a celebrated theorem of Pudlák and Tůma [16], for every finite lattice L there is a finite set X such that $L \leqslant \mathrm{Eq}(X)$. Therefore, $\mathcal{L}_{con}$ would contain all finite lattices if it were closed under S.

The following is a list of operations under which $\mathcal{L}_{con}$ 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 $\mathcal{L}_{con}$ of lattices isomorphic to congruence lattices of finite algebras is closed under the following operations:

item:0 (0) principal filters: all elements above a given element (the correspondence theorem [3]),

item:1 (1) lattice duals (Hans Kurzweil [8] and Raimund Netter [12], 1986),

item:2 (2) interval sublattices (follows from (1), see Remark a. below),

(3) direct products (Jiří Tůma [22], 1986),

(4) ordinal sums (Ralph McKenzie [10], 1984; John Snow [19], 2000),

(5) parallel sums (John Snow [19], 2000),

item:6 (6) certain sublattices of lattices in $\mathcal{L}_{con}$ – namely, those which are obtained as a union of a filter and an ideal of a lattice in $\mathcal{L}_{con}$ (John Snow [19], 2000).

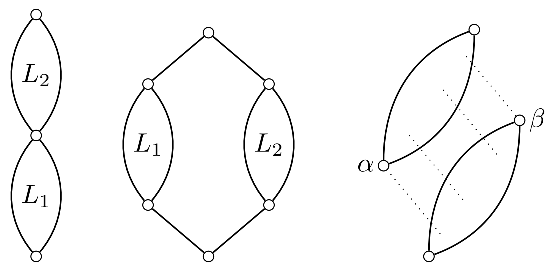


FIGURE 2. The adjoined ordinal sum (left) and parallel sum (middle) of the lattices L_1 and L_2; a union of an order filter $\alpha^{\uparrow}$ and order ideal $\beta^{\downarrow}$ (right).

fig:ord_par_fil-uni

Remarks.

a. The first two items combine to show that $\mathcal{L}_{con}$ is closed under principal ideals and this fact, together with (1), proves (2).

b. By the ordinal sum of two lattices L_1, L_2, we mean the lattice on the left of Figure 2. By the parallel sum of two lattices L_1, L_2, we mean the lattice in the middle of Figure 2.

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 $\mathcal{L}_{con}$ is closed under homomorphic images is open.

:duals-interv-subl-detail

2.1. Lattice duals: the theorem of Kurzweil and Netter. As mentioned above, the class $\mathcal{L}_{con}$ – 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 [12], generalizing the idea of his advisor, Hans Kurzweil [8]. 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 $\{f \mid f : X \to G\}$ 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 unary *idempotent contractions*, that is, for all $x \in X$, $f(f(x)) = f(x)$ and $f(x) \leqslant x$ for all $x \in X$. We denote this set by $\mathcal{IC}(X)$, so

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

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

$$f \sqsubseteq g \quad \Leftrightarrow \quad \ker f \leqslant \ker g, \tag{2.1}$$ eq:MID111

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 $\mathcal{IC}(X)$. In fact, under this ordering, $\mathcal{IC}(X)$ is a lattice that is isomorphic to $\mathrm{Eq}(X)$. Indeed, a lattice isomorphism from $\mathrm{Eq}(X)$ to $\mathcal{IC}(X)$ is given by the function Θ defined for $\alpha \in \mathrm{Eq}(X)$ and $x \in X$ by $\Theta(\alpha)(x) = \bigwedge x/\alpha$; that is, the least element in the α-class containing x. It is easy to check that Θ preserves all meets and joins of $\mathrm{Eq}(X)$. The inverse isomorphism is $\ker : \mathcal{IC}(X) \to \mathrm{Eq}(X)$. That is, ker preserves all meets and joins of $\mathcal{IC}(X)$ (with lattice order $\sqsubseteq$), $\ker \Theta$ is the identity on $\mathrm{Eq}(X)$, and $\Theta \ker$ is the identity on $\mathcal{IC}(X)$.

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, $\mathbf{x} : \underline{n} \to S$, from the set $\underline{n} = \{0, 1, \ldots, n-1\}$ to S, or as the tuple of its values, that is, $\mathbf{x} = (x(0), x(1), \ldots, x(n-1))$. 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,

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

For each $f \in \mathcal{IC}(\underline{n})$, define $\hat{f} : S^n \to S^n$ as follows:[2] for $\mathbf{x} \in S^n$,

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

Then,

$$\hat{f}[S^n] = \{\mathbf{x}f \mid \mathbf{x} \in S^n\} = \{(xf(0), xf(1), \ldots, xf(n-1)) \mid \mathbf{x} \in S^n\}.$$

[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 [15]. Pálfy gives credit for the argument to Kurzweil and Netter.

[2]Here, $\widehat{\ }$ is the functor that lifts $f : \underline{n} \to \underline{n}$ to $\hat{f} : S^n \to S^n$ by way of composition. That is, $\hat{f}\mathbf{x}$ is the usual function composition of $f : \underline{n} \to \underline{n}$ followed by $\mathbf{x} : \underline{n} \to S$.

This is the set of all compositions consisting of f followed by $\mathbf{x} \in S^n$. Equivalently, $\hat{f}[S^n] = \{\mathbf{y} \in S^n \mid \ker f \leqslant \ker \mathbf{y}\}$, which is easily verified.

Should we insert proof of equivalence of expression with $\ker f \leqslant \ker \mathbf{y}$?

For example, if $f = (0,0,2,3,2) \in \mathcal{IC}(\underline{5})$, then $\ker f$ is the equivalence relation corresponding to the partition $|0,1|2,4|3|$, and $\hat{f}[S^n]$ 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,

$$\begin{aligned}\hat{f}[S^n] &= \{(y(0), y(1), y(2), y(3), y(4)) \in S^5 \mid y(1) = y(0) \text{ and } y(2) = y(4)\} \\ &= \{\mathbf{y} \in S^5 \mid \ker f \leqslant \ker \mathbf{y}\}.\end{aligned}$$

It's not hard to see that $D \leqslant \hat{f}[S^n] \leqslant S^n$, for all $f \in \mathcal{IC}(\underline{n})$.

Should we insert proof that $\hat{f}[S^n]$ is a subgroup above D?

lem:latt-duals

Lemma 2.1. *The map $f \mapsto \hat{f}[S^n]$ is a dual lattice isomorphism from* $\mathrm{Eq}(\underline{n})$ *to the interval sublattice $[\![D, S^n]\!] \leqslant \mathrm{Sub}(S^n)$.*

Proof. This is clear since $\mathcal{IC}(\underline{n})$ is ordered by (2.1), and we have $f \sqsubseteq h$ if and only if $\hat{h}[S^n] = \{\mathbf{y} \in S^n \mid \ker h \leqslant \ker \mathbf{y}\} \leqslant \{\mathbf{y} \in S^n \mid \ker f \leqslant \ker \mathbf{y}\} = \hat{f}[S^n]$. □

thm:duals-interv-subl

Theorem 2.2 (Kurzweil [8], Netter [12]). *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 $L = \mathrm{Con}\langle \underline{n}, F\rangle$. Also, by [11, Theorem 4.18], we can assume that F consists of unary operations: $F \subseteq \underline{n}^{\underline{n}}$. 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, [11, Lemma 4.20].) By Lemma 2.1, this is the dual of the lattice $\mathrm{Eq}(\underline{n})$. That is, $\mathrm{Con}\langle S^n/D, S^n\rangle \cong (\mathrm{Eq}(\underline{n}))'$.

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

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

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. □

Remarks.

(1) If the original lattice L is representable as the congruence lattice of an algebra with n elements, then the method described in the proof of Theorem 2.2 above gives a representation of the dual L' as the congruence lattice of the algebra $\langle S^n/D, S^n \cup \hat{F}\rangle$, which has $|S^n/D| = |S|^{n-1}$ elements. Since the smallest simple nonabelian group is A_5, which has 60 elements, the resulting algebra with have at least 60^{n-1} elements.

(2) Elaborating on the last sentence of the proof of Theorem 2.2, take $\mathbf{z} \in \hat{f}[S^n]$ with $\ker \mathbf{z} = \ker f$, so $f(i) = f(j)$ iff $z(i) = z(j)$. Now suppose $\varphi \in F$ does not respect $\ker f$, so there exists $(i,j) \in \ker f$ such that $(\varphi(i), \varphi(j)) \notin \ker f$. Then $\varphi \mathbf{z} \notin \hat{f}[S^n]$, since $z(\varphi(i)) \neq z(\varphi(j))$.

`sec:union-filter-ideal`

2.2. Union of a filter and ideal. The lemma in this section (Lemma 2.3) was originally proved by John Snow (see [20] and [21]), using primitive positive formulas. We provide an alternative proof for two reasons. First, the lemma is a useful tool for proving that certain finite lattices are representable as congruence lattices, and providing a proof helps to keep the paper self-contained. More importantly, however, our proof is more direct than the proof via primitive positive fomulas in that we construct the algebras that the lemma claims exist. For our purposes this is preferable since, when trying to prove that a given lattice is representable, whenever possible we construct an algebra that represents it.

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:union-filter-ideal`

Lemma 2.3. *Let X be a finite set. If $L \leqslant \mathrm{Eq}(X)$ is representable and $L_0 \leqslant L$ 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 L_0 is representable.*

Proof. Assume $L_0 \not\cong \mathbf{2}$, otherwise the result holds trivially. Since $L \leqslant \mathrm{Eq}(X)$ is representable, we have $L = \mathrm{Con}\langle X, \lambda(L)\rangle$ (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:

$$h(x) = \begin{cases} a, & x \in u/\beta, \\ b, & \text{otherwise.} \end{cases} \tag{2.2}$$

`eq:h`

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,

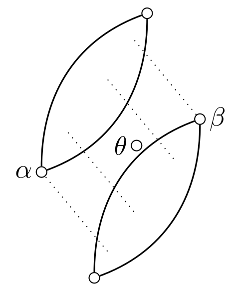


FIGURE 3. $L_0 \leq L_1$

$(a, b) \in \gamma$ 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 $L_0 \leqslant L$, 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, $L_0 = \mathrm{Con}\langle X, \lambda(L_0)\rangle$. □

sec:ordinal-sums

2.3. Ordinal Sums. For two lattices L, M the *adjoined ordinal sum* is denoted by $L \oplus_a M$ 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 $x \leq^L y$) or ($x, y \in M$ and $x \leq^M y$). The *ordinal sum* $L \oplus M$ is defined as $L \oplus_a \mathbf{2} \oplus_a M$ (see Figure 2.3).

The following theorem is a consequence of McKenzie's shift product construction [10].

thm:ordinal-sums

Theorem 2.4. *If $L_1, \ldots, L_n \in \mathcal{L}_{con}$ 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 [19]. As noted above, Jiří Tůma proved that the class of finite representable lattices is closed under direct products. In fact, if L_1 and L_2 are representable as congruence lattices of algebras of cardinality m and n respectively, then $L_1 \times L_2$ is the congruence lattice of an algebra of cardinality mn. 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.

Rather than using an algebra of cardinality mn, we now show that $L_1 \oplus_a L_2$ is representable as the congruence lattice of an algebra of cardinality $m+n-1$. Let $\mathbf{A}, \mathbf{B}$ be two finite algebras with universes $A = \{a_0, \ldots, a_{m-1}\}$ and $B = \{b_0, \ldots, b_{n-1}\}$ respectively, such that $L_1 = \mathrm{Con}(\mathbf{A})$ and $L_2 = \mathrm{Con}(\mathbf{B})$. Define fig:ord_adjord

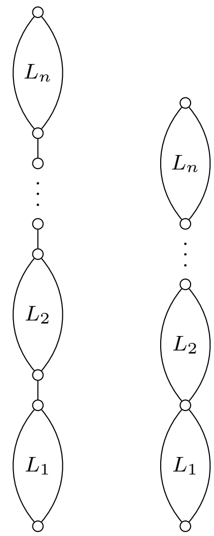


FIGURE 4. The ordinal sum (left) and the adjoined ordinal sum (right) of the lattices $L_1, \ldots, L_n$.

a unary algebra $\mathbf{A}_{m,n}$ with $m+n-1$ elements as follows: the universe $A_{m,n} = A \uplus B_1$ where $B_1 = \{b_1, \ldots, b_{n-1}\} \subset B$, and for each function $h : B_1 \to A$ define a unary operation on $A_{m,n}$ by

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

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

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 $\mathrm{Eq}(\underline{m}) \oplus_a \mathrm{Eq}(\underline{n})$ is isomorphic to the sublattice of $\mathrm{Eq}(A \uplus B_1)$ 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 $(u, v) \notin \alpha$. $\square$

Theorem 2.6. *Suppose* $\mathbf{A} = \langle A, F\rangle$ *and* $\mathbf{B} = \langle B, G\rangle$ *are unary algebras with* $A = \{a_0, \dots, a_{m-1}\}$, $B = \{b_0, \dots, b_{n-1}\}$ *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*

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

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

Proof. Since $\mathbf{C}$ is an expansion of $\mathbf{A}_{m,n}$ it follows from the preceding lemma that $\operatorname{Con}(\mathbf{C})$ is a sublattice of $\{\theta \in \operatorname{Eq}(A \cup B) : \theta \leq \alpha \text{ or } \alpha \leq \theta\}$ where, as before, $\alpha = A^2 \cup \mathrm{id}_B$. Note that $\alpha \in \operatorname{Con}(\mathbf{C})$, so it suffices to show that $\{\theta \in \operatorname{Con}(\mathbf{C}) : \theta \leq \alpha\}$ is isomorphic to $\operatorname{Con}(\mathbf{A})$ and $\{\theta \in \operatorname{Con}(\mathbf{C}) : \alpha \leq \theta\}$ is isomorphic to $\operatorname{Con}(\mathbf{B})$. 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. $\square$

3. Concrete Representations

sec:concr-repr

In this section, we introduce a strategy called the *closure method* that is sometimes useful for constructing a finite algebra with a congruence lattice of a given shape.

Recall that $\operatorname{Eq}(X)$ denotes the lattice of equivalence relations on X. We often abuse notation and identify $\operatorname{Eq}(X)$ with the lattice of partitions of the set X.

3.1. Concrete versus abstract representations. As Bjarni Jónsson explains in [7], 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 $\operatorname{Con}(\mathbf{A})$ for some algebra $\mathbf{A}$ with universe A. The *abstract representation problem* asks whether a given lattice is isomorphic to $\operatorname{Con}(\mathbf{A})$ for some algebra $\mathbf{A}$.

These two problems are closely related, and have become even more so since the publication in 1980 of [16], in which Pavel Pudlák and Jiří Tůma prove that every finite lattice can be embedded as a spanning sublattice[3] of the lattice $\operatorname{Eq}(X)$ 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 $\operatorname{Eq}(X)$ as $L \cong L_0 \leqslant \operatorname{Eq}(X)$, for

[3] 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.

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* is 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 $L \cong \mathrm{Con}(\mathbf{A})$, then L is called a *representable lattice*. On the other hand, if L is isomorphic to a sublattice $L_0 \leqslant \mathrm{Eq}(X)$, then L_0 is sometimes called a *concrete representation* of L (whether or not L_0 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 L, then L is indeed representable in the first sense (that is, L is isomorphic to the congruence lattice of a finite algebra).

As we will see below, there are many examples in which a particular concrete representation $L_0 \leqslant \mathrm{Eq}(X)$ 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[4] operations which respect the equivalence relations of L_0.) This does not imply $L \notin \mathcal{L}_{con}$. It may be that L_0 is not the "right" concrete representation of L, and perhaps we can find some other sublattice of $\mathrm{Eq}(X)$ that is both a congruence lattice and isomorphic to L.

sec:closure-method

3.2. The closure method. The idea described in this section first appeared in *Topics in Universal Algebra* [7], 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 $\mathrm{Eq}(X)$ denote the lattice of equivalence relations on the set X. If $\theta \in \mathrm{Eq}(X)$ and $h \in X^X$, we write $h(\theta) \subseteq \theta$ and say that "h respects θ" if and only if for all $(x, y) \in X^2$ $(x, y) \in \theta$ implies $(h(x), h(y)) \in \theta$. If $h(\theta) \nsubseteq \theta$, we sometimes say that "h violates θ."

For $L \subseteq \mathrm{Eq}(X)$ define

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

For $H \subseteq X^X$ define

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

The map $\rho\lambda$ is a *closure operator* on $\mathrm{Sub}(\mathrm{Eq}(X))$. That is, $\rho\lambda$ is

- *idempotent:*[5] $\rho\lambda\rho\lambda = \rho\lambda$;
- *extensive:* $L \subseteq \rho\lambda(L)$ for every $L \leqslant \mathrm{Eq}(X)$;
- *order preserving:* $\rho\lambda(L) \leqslant \rho\lambda(L_0)$ if $L \leqslant L_0$.

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

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

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

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

This suggests the following strategy for solving the representation problem for a given abstract finite lattice L: search for a concrete representation $L \cong L_0 \leqslant \mathrm{Eq}(X)$, 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. [7]).

Concrete-thm-3

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

As above, given a totally ordered set X, we let $\mathcal{IC}(X) = \{f \in X^X : f^2 = f \text{ and } f(x) \leqslant x\}$, and define the partial order $\sqsubseteq$ on this set as follows:

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

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

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

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

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

The pair (λ, ρ) defines a *Galois correspondence* between $\mathcal{IC}(X)$ and X^X. That is, λ and ρ are antitone maps such that $\lambda\rho \geqslant \mathrm{id}_{\mathcal{H}}$ and $\rho\lambda \geqslant \mathrm{id}_{\mathcal{F}}$. In particular, for any set $F \in \mathcal{F}$ we have $F \subseteq \rho\lambda(F)$ and

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

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

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

4. Distributive lattices

sec:distr-latt

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

A lattice L is called *strongly representable* if whenever $L \cong L_0 \leqslant \mathrm{Eq}(X)$ for some X then there is an algebra based on X whose congruence lattice is 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 [4], Quackenbush and Wolk [17])**.** *Every finite distributive lattice is strongly representable.*

Remarks. By Theorem 3.1 above, the result of Berman, Quackenbush and Wolk says, if L is a finite distributive lattice then every embedding $L \cong L_0 \leqslant \mathrm{Eq}(X)$ is closed. The following proof is only slightly shorter than to the original in [17], and the methods are similar.

Proof. Without loss of generality, suppose $L \leqslant \mathrm{Eq}(X)$. 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 $\beta = \bigvee\{\gamma \in L \mid \gamma \ngeqslant \alpha\}$. 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. Therefore, there exist $(u, v) \in \alpha \setminus \theta$ and $(x, y) \in \theta \setminus \beta$. As in (2.2), define

wjd: should we keep or delete this proof?

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

It is clear that h_θ violates θ but respects all relations in $\alpha^\uparrow = \{\gamma \in L : \alpha \leqslant \gamma\}$ and $\beta^\downarrow = \{\gamma \in L : \gamma \leqslant \beta\}$. Also, $L = \alpha^\uparrow \cup \beta^\downarrow$. Finally, since θ was arbitrary, such an h_θ exists for each $\theta \in \mathrm{Eq}(X) \setminus L$, so we have $L = \mathrm{Con}\langle X, \mathcal{H}\rangle$, where $\mathcal{H} = \{h_\theta : \theta \in \mathrm{Eq}(X) \setminus L\}$. $\square$

5. Congruence Lattices of Group Actions

sec:congr-latt-group

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, $\langle X^X, \circ, \mathrm{id}_X\rangle$. 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 $\mathrm{Sym}(X)$. When the underlying set isn't important, we usually write S_n to denote the symmetric group on an n-element set.

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 $\mathrm{Aut}(\mathbf{X})$. That is, a representation of G is a mapping $\varphi : G \to \mathrm{Aut}(\mathbf{X})$ which satisfies $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$, where (as above) $\circ$ denotes composition of maps in $\mathrm{Aut}(\mathbf{X})$.

5.1. Transitive G-sets. A representation $\varphi : G \to \operatorname{Aut}(\mathbf{X})$ defines an action by G on the set X, as follows: $\varphi(g) : x \mapsto x^{\varphi(g)}$. If $\varphi(G) \leqslant \operatorname{Aut}(\mathbf{X})$ 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*.

Suppose G acts on the set X and supposed U is the set of "unmoved" points in X. That is, $u \in U$ if every element of G leaves u fixed. The *degree* of such a group action is the cardinality of $|X \setminus U|$, that is, the cardinality of the set of moved points.

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.

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

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

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.

Finally, a *primitive group* is a group that contains a core-free maximal subgroup.

Corollary 5.1. *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 shows that we need only consider a single representative H from each of the conjugacy classes of subgroups.

Lemma 5.2 (Lem. 1.6B [5])**.** *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 [14] P. P. Pálfy and P. Pudlák showed the following statements are equivalent:

- every finite lattice is representable, that is $\mathscr{L}_{con}$ 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 G. By a fundamental isomorphism theorem for transitive G-sets—see [11, Lemma 4.20] (general algebra version) or [5, Theorem 1.5A] (group-theoretic version)—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 L:

question1 (1) Is L representable (isomorphic to $\mathrm{Con}(\mathbf{A})$ for some finite algebra $\mathbf{A}$)?
question2 (2) If L is representable, what is the minimum size of $\mathbf{A}$ with $L \cong \mathrm{Con}(\mathbf{A})$?
question3 (3) Is there a group G of permutations on A such that $L \cong \mathrm{Con}\langle A, G\rangle$?
question4 (4) Is there a transitive group G of permutations on A such that $L \cong \mathrm{Con}\langle A, G\rangle$? Equivalently is L isomorphic an interval in the subgroup lattice of a finite group (by the basic isomorphism theorem for transitive G-sets; see [11, Lemma 4.20] or [5, Theorem 1.5A]).
question5 (5) If $L \cong \mathrm{Con}\langle A, G\rangle$ 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].

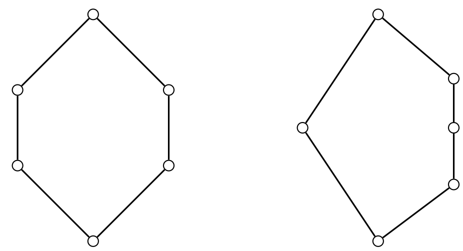


Figure 5. $\mathbf{L}_6$ and $\mathbf{L}_7$ fig:L6and7

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 $L \cong \mathrm{Con}\langle A, F\rangle$ 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 [9]:

(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

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

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 [9] 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 5.3 (Pálfy-Pudlák [14], McKenzie [9]). *Let L be finite lattice and suppose $L \cong \mathrm{Con}\langle A, F\rangle$ 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 $\mathrm{Con}\langle A, G\rangle$ 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

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

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 $\tau = 1$. Of course A_i is a subuniverse of $\mathbf{A}$; the subalgebra is denoted $\mathbf{A}_i$.

thm:intrans **Theorem 5.4.** *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 $\theta \in \mathrm{Con}(\mathbf{A})$.*

item1 *(1) G acts transitively if and only if $\tau = 1_{\mathbf{A}}$.*

item2 *(2) The interval $[\![\tau, 1_{\mathbf{A}}]\!]$ is isomorphic to $\mathrm{Eq}(k)$.*

item3 *(3) The interval $[\![0_{\mathbf{A}}, \tau]\!]$ is isomorphic to $\prod_{i=0}^{k-1} \mathrm{Con}(\mathbf{A}_i)$.*

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 $\mathrm{Con}(\mathbf{A})$ lies above τ.*

item7 *(7) If $k > 1$ and $[\![0_{\mathbf{A}}, \tau]\!]$ is directly indecomposable then every coatom of $\mathrm{Con}(\mathbf{A})$ 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 $\mathbf{A}/\tau$, $\mathrm{Con}(\mathbf{A}/\tau)$ is the lattice of all partitions; that is, $\mathrm{Eq}(k)$. So (2) holds. For (3), we map $(\theta_0, \ldots, \theta_{k-1}) \in \prod_{i=0}^{k-1} \mathrm{Con}(A_i)$ 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 $\theta \not\leq \gamma_i$, 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). □

5.4. Examples. We give some examples showing the uses of Theorem 5.4. In deciding if a lattice has a representation using an intransitive permutation group, we consider the possibilities for τ. By (2) of Theorem 5.4 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 $\gamma_0 = \gamma_1 = \tau$

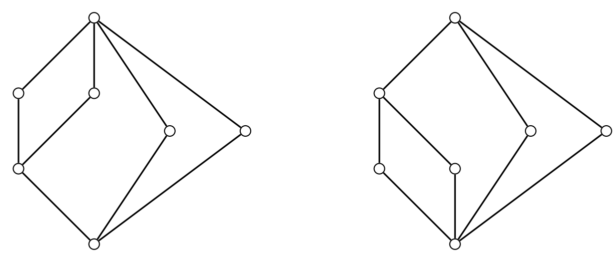


FIGURE 6. $\mathbf{L}_{14}$ (on the left) and $\mathbf{L}_{15}$ fig:L14and15

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 5.4(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.

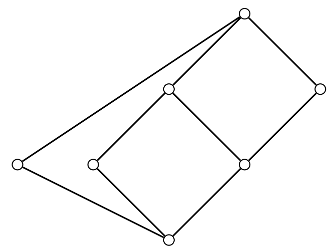


FIGURE 7. $\mathbf{L}_{10}$ fig:L10

This lattice cannot be represented using an intransitive permutation group. By Theorem 5.4(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 5.5 below covers this case.

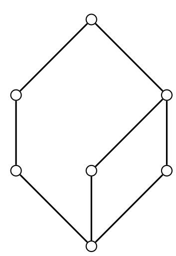


FIGURE 8. $\mathbf{L}_{19}$ fig:L19

lemma:complements **Lemma 5.5.** *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* $\mathrm{Con}(\mathbf{A})$ *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 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 [18] 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 set $\{\mathbf{2}^{m_i} \mid 1 \leqslant i \leqslant t\}$ of lattices of subsets of sets of sizes m_i for each $i \in \{1, \ldots, t\}$, remove the least and greatest element of each, line them up side by side, and adjoin them into one large lattice by giving them all a new common least element and a new common greatest element. An example of such a lattice appears in the diagram in Figure 9.

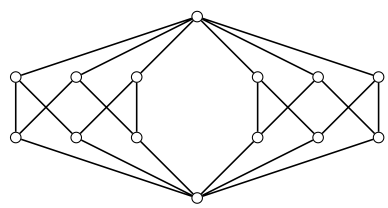


Figure 9. A possibly non-representable lattice. fig:shareshian

While the conjecture—that this lattice is not representable as a congruence lattice of a finite algebra—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 used above to analyze $\mathbf{L}_{10}$ also show that a minimal representation of one of Shareshian's lattices could not come from an *intransitive* permutation group. This is because such lattices satisfy conditions (A) and (B$''$), so a minimal representation, if it exists, would have to be the congruence lattice of a transitive G-set. Hence, if one of Shareshian's lattices does not occur as an interval in the subgroup lattice of a finite group, then that lattice has no finite representation at all.

Next consider $\mathbf{L}_{11}$ diagrammed in Figure 10 (left). Again, we can use Theorem 5.4(9) to show that it's not possible to represent $\mathbf{L}_{11}$ using an intransitive permutation group. However (A) and (B$'$) do not hold in this case, so we cannot conclude that a minimal representation must come from 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.

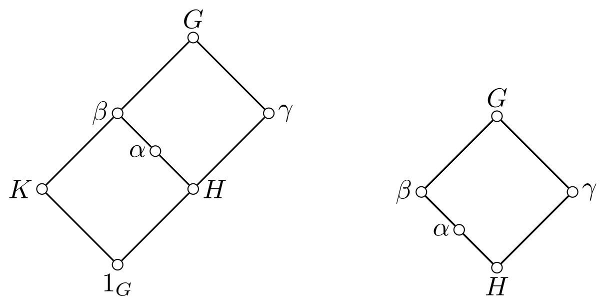


FIGURE 10. $\mathbf{L}_{11}$ (left) and an upper interval (right) fig:L11

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 Figure 10 (right).

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 $\mathbf{L}_{11}$ is the union of the ideal $[\![1, K]\!]$ and the filter $[\![H, G]\!]$. 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 )`, which happens to have 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 the correspondence is given in the following table:

4	G
3	`Group([ f1, f4, f5, f6 ])`
2	`Group([ f1, f2, f3*f4, f4 ])`
1	`Group([ f1, f4, f5*f6 ])`
0	H

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 ])`. So, the GAP output above shows that the interval $[\![H, G]\!]$ is a pentagon.

Next, we define the following groups in GAP:

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

Here, `A` $<$ `B` are the comparable generators of the pentagon and `C` is the incomparable generator. We consider the conjugacy classes of the subgroups of `B` (using the GAP command `ccsgB:=ConjugacyClassesSubgroups(B);`) and by looking at the subgroup lattice in XGAP, we notice that there is a conjugacy class of subgroups of `B` containing six subgroups each of index 72 in `G` (order 3), and the subgroups in this class are not subgroups of `A` or `C`.

```
List(ccsgB, x->Size((x)));
# returns [ 1, 9, 1, 3, 3, 6, 3, 9, 9, 1, 1, 2, 1, 3, 1, 1 ]
List(ccsgB, x->Order(Representative(x)));
# returns [ 1, 2, 3, 3, 3, 3, 6, 6, 6, 9, 9, 9, 18, 18, 27, 54 ]
```

Thus the only conjugacy class of size 6 whose elements have order 3 is the sixth class. So let `K:=Representative(ccsgB[6]);`. Note that `K` is a minimal subgroup since $|K| = 3$. Finally, check that `K` is a subgroup of `B`, and not a subgroup of `A` or `C`:

```
IsSubgroup(A,K);  # returns false
IsSubgroup(B,K);  # returns true
IsSubgroup(C,K);  # returns false
```

This shows lattice $\mathbf{L}_{11}$ is representable on a set of size 216. In this example, where $[\![H, G]\!]$ is the pentagon, the index is $[G : H] = 36$.

Now, there might be a nontrivial subgroup $M < H$ such that in the interval $[\![M, G]\!]$ there is a union of a filter and ideal in $\mathrm{Sub}(G)$ that is isomorphic to $\mathbf{L}_{11}$. This would give us a representation of $\mathbf{L}_{11}$ on smaller set than 216. Indeed, looking at the subgroup lattice of G in XGAP, we see that, H has only two nontrivial proper subgroups. These are

```
M1:=Representative(ccsgB[2]);
M2:=Representative(ccsgB[4]);
IsSubgroup(H,Representative(ccsgB[2]));  # returns true
IsSubgroup(H,Representative(ccsgB[4]));  # returns true
```

We need to find a subgroup that covers one of these two subgroups and is not below `A` or `C`.

```
intM1B:=IntermediateSubgroups(B,M1);
# returns
#  rec(
#    subgroups := [
#      Group([ f4, f5 ]), Group([ f4, f6 ]),
#      Group([ f1^2, f4 ]), Group([ f4, f5*f6 ]),
#      Group([ f4, f5^2*f6 ]), Group([ f4, f5, f6 ]),
#      Group([ f1^2, f4, f5*f6 ])
#    ],
#    inclusions := [
#      [ 0, 1 ], [ 0, 2 ], [ 0, 3 ], [ 0, 4 ],
#      [ 0, 5 ], [ 1, 6 ], [ 2, 6 ], [ 3, 7 ],
#      [ 4, 6 ], [ 4, 7 ], [ 5, 6 ], [ 6, 8 ], [ 7, 8 ]
#    ]
#  )
```

`M1` is maximal in the intermediate subgroups 1, 2, 3, 4, and 5. We now check whether these are subgroups of `A` or `C`.

```
IsSubgroup(A,intM1B.subgroups[1]);   # returns false
IsSubgroup(B,intM1B.subgroups[1]);   # returns true (of course)
IsSubgroup(C,intM1B.subgroups[1]);   # returns false
```

So $\mathbf{L}_{11}$ is the union of $[\![$`M1, intM1B.subgroups[1]`$]\!]$ and $[\![H, G]\!]$, and the command `Index(G,M1);` returns 108, so we have a representation of $\mathbf{L}_{11}$ on 108 elements.

Next consider `M2`.

```
Index(G,M2);  # returns 72
intM2B:=IntermediateSubgroups(B,M2);
# returns
#  rec(
#    subgroups := [
#        Group([ f1, f4 ]), Group([ f1, f4*f5*f6 ]),
#        Group([ f1, f4*f5^2*f6^2 ]), Group([ f1, f5*f6 ]),
#        Group([ f1, f4, f5*f6 ]), Group([ f1, f4*f5, f5^2*f6^2 ]),
#        Group([ f1, f4*f6, f5*f6 ]), Group([ f1, f5, f6 ])
#    ],
#    inclusions := [
#        [ 0, 1 ], [ 0, 2 ], [ 0, 3 ], [ 0, 4 ], [ 1, 5 ],
#        [ 2, 5 ], [ 3, 5 ], [ 4, 5 ], [ 4, 6 ], [ 4, 7 ],
#        [ 4, 8 ], [ 5, 9 ], [ 6, 9 ], [ 7, 9 ], [ 8, 9 ]
#    ]
#  )
```

So `M2` is maximal in the intermediate subgroups 1, 2, 3, and 4. We can check whether one of these is not a subgroup of `A` or `C`:

```
IsSubgroup(A,intM2B.subgroups[1]);   # returns true
IsSubgroup(C,intM2B.subgroups[1]);   # returns true

IsSubgroup(A,intM2B.subgroups[2]);   # returns true
IsSubgroup(C,intM2B.subgroups[2]);   # returns false

IsSubgroup(A,intM2B.subgroups[3]);   # returns true
```

```
IsSubgroup(C,intM2B.subgroups[3]);   # returns false

IsSubgroup(A,intM2B.subgroups[3]);   # returns true
IsSubgroup(C,intM2B.subgroups[3]);   # returns false
```

So, using this method and this group, the smallest set on which we can represent $\mathbf{L}_{11}$ is 108.

TODO: complete this section: perhaps we should actually perform the closure, get the operations and produce the algebra that has $\mathbf{L}_{11}$ as a representation (although, this is not absolutely necessary since the above suffices to prove that $\mathbf{L}_{11}$ is, in indeed, representable).

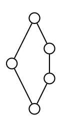
6. Small unary algebras for congruence lattices of size ≤ 7

sec:small-unary-algebras

Distributive lattices and lattices that are ordinal sums of smaller lattices are omitted. This leaves 35 lattices listed below with the names $\mathbf{L}_1, \ldots, \mathbf{L}_{35}$. In most cases, each lattice $\mathbf{L}_i$ is followed by a unary algebra denoted $\mathbf{B}_i$ with the property that $\mathbf{L}_i = \mathrm{Con}(\mathbf{B}_i)$. The base set of each algebra is $\{0, 1, \ldots, n-1\}$, and each unary operation $f, g, h, \ldots$ is specified by a vector of values of these elements. Algebras of cardinality less than 11 are known to be minimal-size algebras that produce the corresponding congruence lattice. The algebra $\mathbf{B}_{33}$ is also known to be of minimal cardinality. Currently only $\mathbf{L}_{10}$ is not known to be the congruence lattice of a finite algebra.

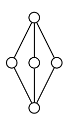
PJ: should this be less than or equal to 11???

$\mathbf{L}_1$



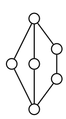
$\mathbf{B}_1$	0	1	2	3
$f(x)$	1	0	3	2
$g(x)$	1	0	1	0

$\mathbf{L}_2$



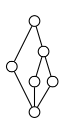
$\mathbf{B}_2$	0	1	2	3
$f(x)$	1	0	3	2
$g(x)$	2	3	0	1

$\mathbf{L}_3$



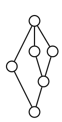
$\mathbf{B}_3$	0	1	2	3	4	5	6
$f(x)$	0	1	2	1	2	1	0
$g(x)$	0	3	4	3	4	3	0
$h(x)$	6	5	2	5	2	5	6
$k(x)$	0	1	2	0	0	2	2

$\mathbf{L}_4$



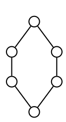
$\mathbf{B}_4$	0	1	2	3
$f(x)$	1	0	3	2
$g(x)$	0	0	2	2

$\mathbf{L}_5$

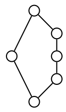


$\mathbf{B}_5$	0	1	2	3	4	5	6	7	8	9	10	11
$f(x)$	1	2	3	4	5	0	7	8	9	10	11	6
$g(x)$	6	11	10	9	8	7	0	5	4	3	2	1
$h(x)$	0	0	0	6	0	0	0	0	6	0	0	0

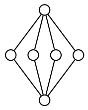
$\mathbf{L}_6$



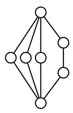
$\mathbf{B}_6$	0	1	2	3	4	5
$f(x)$	2	2	1	5	5	4
$g(x)$	3	4	4	0	1	1
$h(x)$	4	5	3	4	5	3

$\mathbf{L}_7$ 

$\mathbf{B}_7$	0	1	2	3	4	5
$f(x)$	1	0	0	4	3	3
$g(x)$	4	5	5	1	2	2
$h(x)$	3	3	4	3	3	4

$\mathbf{L}_8$ 

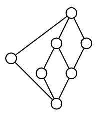
$\mathbf{B}_8$	0	1	2	3	4	5
$f(x)$	1	2	0	4	5	3
$g(x)$	3	5	4	0	2	1

$\mathbf{L}_9$ 

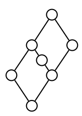
$\mathbf{B}_9$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(x)$	0	0	0	0	0	0	2	1	2	1	3	4	5	3	4	5
$g(x)$	0	0	0	0	0	0	6	7	6	7	10	11	12	10	11	12
$h(x)$	13	14	15	1	9	8	15	14	13	15	1	9	8	8	1	9

Method: overalgebras

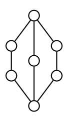
need to have some discussion of the overalgebras method in the text?

$\mathbf{L}_{10}$ 

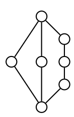
No finite algebra known with this congruence lattice

$\mathbf{L}_{11}$ 

A finite algebra with 108 elements known.
(See discussion after Fig. 10)

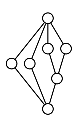
$\mathbf{L}_{12}$ 

$\mathbf{B}_{12}$	0	1	2	3	4	5	6	7	8
$f(x)$	0	0	3	3	3	6	6	6	0
$g(x)$	0	0	8	8	8	1	1	1	0
$h(x)$	0	5	5	4	0	0	5	4	4
$k(x)$	4	2	2	3	4	4	2	3	3
$l(x)$	5	5	7	7	7	6	6	6	5

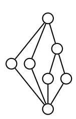
$\mathbf{L}_{13}$ 

$\mathbf{B}_{13}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$f(x)$	0	1	2	1	2	1	0	0	1	2	2	1	0	0	1	2	1	2	0
$g(x)$	0	1	2	0	0	2	2	0	3	4	0	4	4	6	5	2	6	6	2
$h(x)$	0	1	2	3	4	5	6	0	1	2	4	5	6	0	1	2	3	4	6
$k(x)$	7	8	9	3	10	11	12	3	3	3	3	3	3	11	11	11	11	11	11
$l(x)$	13	14	15	16	17	5	18	13	16	17	17	16	13	5	5	5	5	5	5

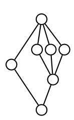
Method:
overalgebras

$\mathbf{L}_{14}$ 

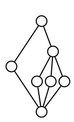
Upper interval in $\mathrm{Sub}(A_6)$,
algebra of size 90

$\mathbf{L}_{15}$ 

$\mathbf{B}_{15}$	0	1	2	3
$f(x)$	1	0	3	2

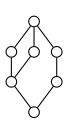
$\mathbf{L}_{16}$ 

Upper interval in $\mathrm{Sub}(C_2.A_6)$
algebra of size 180

$\mathbf{L}_{17}$ 

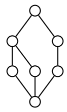
$\mathbf{B}_{17}$	0	1	2	3	4	5	6	7	8	9	10	11
$f(x)$	1	0	3	2	5	4	7	6	9	8	11	10
$g(x)$	4	7	5	6	8	11	9	10	0	3	1	2
$h(x)$	0	0	0	0	5	5	5	5	10	10	10	10

Method: filter-ideal in $\mathrm{Sub}(A_4)$

$\mathbf{L}_{18}$ 

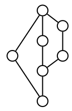
Dual of 19, no explicit
small representation known

$\mathbf{L}_{19}$



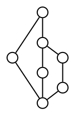
$\mathbf{B}_{19}$	0	1	2	3	4	5	6	7
$f(x)$	0	1	1	0	4	5	5	4
$g(x)$	0	2	3	1	0	2	3	1
$h(x)$	7	6	6	7	3	2	2	3

$\mathbf{L}_{20}$



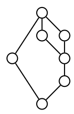
Method: filter-ideal in SmallGroup(216,153) in GAP

$\mathbf{L}_{21}$



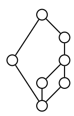
$\mathbf{B}_{21}$	0	1	2	3	4	5	6	7	8
$f(x)$	3	3	4	8	8	2	2	3	4
$g(x)$	0	0	6	1	1	0	0	5	6
$h(x)$	4	5	5	7	8	8	7	4	4

$\mathbf{L}_{22}$



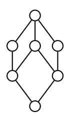
Dual of 23, no explicit small
representation known

$\mathbf{L}_{23}$



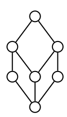
$\mathbf{B}_{23}$	0	1	2	3	4	5
$f(x)$	0	1	0	1	4	4
$g(x)$	1	1	3	3	4	5
$h(x)$	3	2	3	2	5	5
$k(x)$	4	1	5	3	4	5

$\mathbf{L}_{24}$



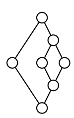
$\mathbf{B}_{24}$	0	1	2	3
$f(x)$	1	1	2	2
$g(x)$	2	3	3	2

$\mathbf{L}_{25}$



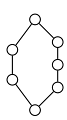
$\mathbf{B}_{25}$	0	1	2	3	4
$f(x)$	0	0	2	2	2
$g(x)$	0	1	0	1	1
$h(x)$	1	1	4	4	4
$k(x)$	2	3	2	3	3

$\mathbf{L}_{26}$



$\mathbf{B}_{26}$	0	1	2	3	4	5
$f(x)$	1	0	3	2	0	2
$g(x)$	4	4	5	5	1	3
$h(x)$	0	0	0	0	1	1
$k(x)$	3	5	3	5	3	3

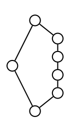
$\mathbf{L}_{27}$



$\mathbf{B}_{27}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(x)$	0	1	2	3	4	5	0	0	0	0	0	2	2	2	2	2
$g(x)$	4	5	3	4	5	3	5	3	4	5	3	4	5	4	5	3
$h(x)$	2	2	1	5	5	4	2	1	5	5	4	2	2	5	5	4
$k(x)$	3	4	4	0	1	1	4	4	0	1	1	3	4	0	1	1
$l(x)$	0	6	7	8	9	10	6	7	8	9	10	0	6	8	9	10
$m(x)$	11	12	2	13	14	15	12	2	13	14	15	11	12	13	14	15

Method:
overalgebras

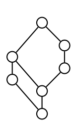
$\mathbf{L}_{28}$



$\mathbf{B}_{28}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(x)$	0	1	2	3	4	5	0	0	0	0	0	2	2	2	2	2
$g(x)$	3	3	4	3	3	4	3	4	3	3	4	3	3	3	3	4
$h(x)$	1	0	0	4	3	3	0	0	4	3	3	1	0	4	3	3
$k(x)$	4	5	5	1	2	2	5	5	1	2	2	4	5	1	2	2
$l(x)$	0	6	7	8	9	10	6	7	8	9	10	0	6	8	9	10
$m(x)$	11	12	2	13	14	15	12	2	13	14	15	11	12	13	14	15

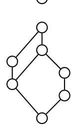
Method:
overalgebras

$\mathbf{L}_{29}$

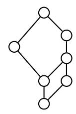


$\mathbf{B}_{29}$	0	1	2	3	4
$f(x)$	1	0	3	2	2
$g(x)$	2	4	2	4	3

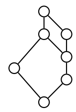
$\mathbf{L}_{30}$



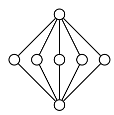
$\mathbf{B}_{30}$	0	1	2	3	4
$f(x)$	0	3	4	3	4
$g(x)$	2	2	1	4	3

$\mathbf{L}_{31}$ 

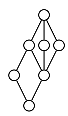
$\mathbf{B}_{31}$	0	1	2	3	4
$f(x)$	0	1	1	0	0
$g(x)$	1	1	2	2	2
$h(x)$	3	2	2	4	4

$\mathbf{L}_{32}$ 

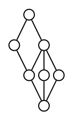
$\mathbf{B}_{32}$	0	1	2	3	4
$f(x)$	0	1	1	3	3
$g(x)$	1	2	2	4	4
$h(x)$	3	3	4	3	4

$\mathbf{L}_{33}$ 

$\mathbf{B}_{33}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(x)$	1	3	2	0	9	11	10	8	13	15	14	12	5	7	6	4
$g(x)$	11	8	10	9	7	4	6	5	15	12	14	13	3	0	2	1
$h(x)$	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1

$\mathbf{L}_{34}$ 

$\mathbf{B}_{34}$	0	1	2	3
$f(x)$	0	1	3	2

$\mathbf{L}_{35}$ 

$\mathbf{B}_{35}$	0	1	2	3
$f(x)$	1	1	2	3
$g(x)$	2	3	3	3

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.

Bergman2012 [3] Clifford Bergman. *Universal algebra. Fundamentals and selected topics*, volume 301 of *Pure and Applied Mathematics*. CRC Press, Boca Raton, FL, 2012.

Berman:1970 [4] Joel Berman. *Congruence lattices of finite universal algebras*. PhD thesis, University of Washington, 1970.

Dixon:1996 [5] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

GAP4 [6] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.8.3*, 2016.

Jonsson:1972 [7] Bjarni Jónsson. *Topics in universal algebra*. Lecture Notes in Mathematics, Vol. 250. Springer-Verlag, Berlin, 1972.

Kurzweil:1985 [8] Hans Kurzweil. Endliche Gruppen mit vielen Untergruppen. *J. Reine Angew. Math.*, 356:140–160, 1985.

McKenzie1983 [9] 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 [10] Ralph McKenzie. A new product of algebras and a type reduction theorem. *Algebra Universalis*, 18(1):29–69, 1984.

alvi:1987 [11] Ralph N. McKenzie, George F. McNulty, and Walter F. Taylor. *Algebras, lattices, varieties. Vol. I*. Wadsworth & Brooks/Cole, Monterey, CA, 1987.

Netter:1986 [12] R. Netter. Eine Bemerkung zu Kongruenzverbänden. preprint, 1986.

Palfy1988 [13] P. P. Pálfy. On Feit's examples of intervals in subgroup lattices. *J. Algebra*, 116:471–479, 1988.

PalfyPudlak1980 [14] 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 [15] Péter Pál Pálfy. The finite congruence lattice problem, September 2009. Summer School on General Algebra and Ordered Sets Stará Lesná, 6, 2009.

Pudlak:1980 [16] Pavel Pudlák and Jiří Túma. Every finite lattice can be embedded in a finite partition lattice. *Algebra Universalis*, 10(1):74–95, 1980.

Quack:1971 [17] R. Quackenbush and B. Wolk. Strong representation of congruence lattices. *Algebra Universalis*, 1:165–166, 1971/72.

Shareshian2003 [18] John Shareshian. Topology of order complexes of intervals in subgroup lattices. *J. Algebra*, 268(2):677–686, 2003.

Snow:2000 [19] John W. Snow. A constructive approach to the finite congruence lattice representation problem. *Algebra Universalis*, 43(2-3):279–293, 2000.

MR1774743 [20] John W. Snow. A constructive approach to the finite congruence lattice representation problem. *Algebra Universalis*, 43(2-3):279–293, 2000.

MR2026829 [21] John W. Snow. Every finite lattice in $\mathcal{V}(\mathbf{M}_3)$ is representable. *Algebra Universalis*, 50(1):75–81, 2003.

Tuma:1986 [22] 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/`