The Finite Lattice Representation Problem:

intervals in subgroup lattices and the dawn of tame congruence theory

William DeMeo

University of Hawai‘i at Mānoa

Math 613: Group Theory
November 2009

Outline

1. Introduction
   - algebras and their congruences
2. Lattices
   - subgroup lattices and congruence lattices
   - the finite lattice representation problem
3. Groups
   - G-sets
   - intervals in subgroup lattices
4. Milestones
   - the theorem of Pálfy-Pudlák
   - the seminal lemma of tct

Background and problem statement

Theorem (Grätzer-Schmidt, 1963)

Every algebraic lattice is isomorphic to the congruence lattice of an algebra.

What if the lattice is finite?

Problem: Given a finite lattice $\mathbf{L}$, does there exist a *finite* algebra $\mathbf{A}$ such that $\mathbf{Con}\,\mathbf{A} \cong \mathbf{L}$?

status: open

age: 45+ years

difficulty: *what do you think?*

Background and problem statement

Theorem (Grätzer-Schmidt, 1963)

Every algebraic lattice is isomorphic to the congruence lattice of an algebra.

What if the lattice is finite?

Problem: Given a finite lattice $\mathbf{L}$, does there exist a *finite* algebra $\mathbf{A}$ such that $\mathbf{Con}\mathbf{A} \cong \mathbf{L}$?

status: open

age: 45+ years

difficulty: *what do you think?*

Background and problem statement

Theorem (Grätzer-Schmidt, 1963)

Every algebraic lattice is isomorphic to the congruence lattice of an algebra.

What if the lattice is finite?

Problem: Given a finite lattice $\mathbf{L}$, does there exist a *finite* algebra $\mathbf{A}$ such that $\mathbf{Con}\,\mathbf{A} \cong \mathbf{L}$?

status: open

age: 45+ years

difficulty: *what do you think?*

Background and problem statement

Theorem (Grätzer-Schmidt, 1963)

Every algebraic lattice is isomorphic to the congruence lattice of an algebra.

What if the lattice is finite?

Problem: Given a finite lattice $\mathbf{L}$, does there exist a *finite* algebra $\mathbf{A}$ such that $\mathbf{Con}\,\mathbf{A} \cong \mathbf{L}$?

status: open

age: 45+ years

difficulty: *what do you think?*

What is an algebra?

Definition (algebra)

A (universal) algebra $\mathbf{A}$ is an ordered pair $\mathbf{A} = \langle A, F \rangle$ where

- A is a nonempty set, called the *universe* of $\mathbf{A}$
- F is a family of finitary operations on $\mathbf{A}$

An algebra $\langle A, F \rangle$ is *finite* if $|A|$ is finite.

Definition (arity)

The arity of an operation $f \in F$ is the number of operands.

- f is *n-ary* if it maps A^n into A
- *nullary*, *unary*, *binary*, and *ternary* operations have arities 0, 1, 2, and 3, respectively

What is an algebra?

Definition (algebra)

A (universal) algebra $\mathbf{A}$ is an ordered pair $\mathbf{A} = \langle A, F\rangle$ where

A is a nonempty set, called the *universe* of $\mathbf{A}$

F is a family of finitary operations on $\mathbf{A}$

An algebra $\langle A, F\rangle$ is *finite* if $|A|$ is finite.

Definition (arity)

The arity of an operation $f \in F$ is the number of operands.

- f is *n-ary* if it maps A^n into A
- *nullary*, *unary*, *binary*, and *ternary* operations have arities 0, 1, 2, and 3, respectively

What is an algebra?

Definition (algebra)

A (universal) algebra $\mathbf{A}$ is an ordered pair $\mathbf{A} = \langle A, F\rangle$ where

A is a nonempty set, called the *universe* of $\mathbf{A}$

F is a family of finitary operations on $\mathbf{A}$

An algebra $\langle A, F\rangle$ is *finite* if $|A|$ is finite.

Definition (arity)

The arity of an operation $f \in F$ is the number of operands.

- f is *n-ary* if it maps A^n into A
- *nullary*, *unary*, *binary*, and *ternary* operations have arities 0, 1, 2, and 3, respectively

What is an algebra?

Definition (algebra)

A (universal) algebra $\mathbf{A}$ is an ordered pair $\mathbf{A} = \langle A, F \rangle$ where

A is a nonempty set, called the *universe* of $\mathbf{A}$

F is a family of finitary operations on $\mathbf{A}$

An algebra $\langle A, F \rangle$ is *finite* if $|A|$ is finite.

Definition (arity)

The arity of an operation $f \in F$ is the number of operands.

- f is *n-ary* if it maps A^n into A
- *nullary*, *unary*, *binary*, and *ternary* operations have arities 0, 1, 2, and 3, respectively

What is an algebra?

Definition (algebra)

A (universal) algebra $\mathbf{A}$ is an ordered pair $\mathbf{A} = \langle A, F \rangle$ where

A is a nonempty set, called the *universe* of $\mathbf{A}$

F is a family of finitary operations on $\mathbf{A}$

An algebra $\langle A, F \rangle$ is *finite* if $|A|$ is finite.

Definition (arity)

The arity of an operation $f \in F$ is the number of operands.

- f is *n-ary* if it maps A^n into A
- *nullary*, *unary*, *binary*, and *ternary* operations have arities 0, 1, 2, and 3, respectively

Example: *groups!*

Definition (group)

A group **G** is an algebra $\langle G, \cdot, ^{-1}, 1\rangle$ with a binary, unary, and nullary operation satisfying, $\forall x, y, z \in G$,

G1: $x \cdot (y \cdot z) \approx (x \cdot y) \cdot z$

G2: $x \cdot 1 \approx 1 \cdot x \approx x$

G3: $x \cdot x^{-1} \approx x^{-1} \cdot x \approx 1$

Congruence relations defined

Definition (congruence relation)

Given $\mathbf{A} = \langle A, F \rangle$, an equivalence relation $\theta \in \mathrm{Eq}(A)$ is a congruence on $\mathbf{A}$ if θ "admits" F

i.e., for n-ary $f \in F$, and elements $a_i, b_i \in A$,

$$\text{if} \quad (a_i, b_i) \in \theta, \quad \text{then} \quad (f(a_1, \dots, a_n), f(b_1, \dots, b_n)) \in \theta$$

or "*f respects* θ" for all $f \in F$.

The set of all congruence relations on $\mathbf{A}$ is denoted $\mathrm{Con}(\mathbf{A})$.

Congruence relations defined

Definition (congruence relation)

Given $\mathbf{A} = \langle A, F \rangle$, an equivalence relation $\theta \in \mathrm{Eq}(A)$ is a congruence on $\mathbf{A}$ if θ "admits" F

i.e., for n-ary $f \in F$, and elements $a_i, b_i \in A$,

$$\text{if } \ (a_i, b_i) \in \theta, \ \text{ then } \ (f(a_1, \dots, a_n), f(b_1, \dots, b_n)) \in \theta$$

or "f *respects* θ" for all $f \in F$.

The set of all congruence relations on $\mathbf{A}$ is denoted $\mathrm{Con}(\mathbf{A})$.

Congruence relations defined

Definition (congruence relation)

Given $\mathbf{A} = \langle A, F \rangle$, an equivalence relation $\theta \in \mathrm{Eq}(A)$ is a congruence on $\mathbf{A}$ if θ "admits" F

i.e., for n-ary $f \in F$, and elements $a_i, b_i \in A$,

$$\text{if } \ (a_i, b_i) \in \theta, \ \text{ then } \ (f(a_1, \dots, a_n), f(b_1, \dots, b_n)) \in \theta$$

or "f *respects* θ" for all $f \in F$.

The set of all congruence relations on $\mathbf{A}$ is denoted $\mathrm{Con}(\mathbf{A})$.

Congruence relations defined

Definition (congruence relation)

Given $\mathbf{A} = \langle A, F \rangle$, an equivalence relation $\theta \in \mathrm{Eq}(A)$ is a congruence on $\mathbf{A}$ if θ "admits" F

i.e., for n-ary $f \in F$, and elements $a_i, b_i \in A$,

$$\text{if } \ (a_i, b_i) \in \theta, \ \text{ then } \ (f(a_1, \dots, a_n), f(b_1, \dots, b_n)) \in \theta$$

or "f *respects* θ" for all $f \in F$.

The set of all congruence relations on $\mathbf{A}$ is denoted $\mathrm{Con}(\mathbf{A})$.

Example: *groups!*

What are the congruences of a group?

For a group $\mathbf{G} = \langle G, \cdot, ^{-1}, 1\rangle$, an equivalence $\theta \in \mathrm{Eq}(G)$ is a congruence on $\mathbf{G}$ provided, $\forall a, b, a_i, b_i \in G$,

$$(a, b) \in \theta \quad \Rightarrow \quad (a^{-1}, b^{-1}) \in \theta, \quad \text{and}$$

$$(a_i, b_i) \in \theta \quad \Rightarrow \quad (a_1 \cdot a_2, b_1 \cdot b_2) \in \theta.$$

Example: *groups!*

What are the congruences of a group?

For a group $\mathbf{G} = \langle G, \cdot, ^{-1}, 1\rangle$, an equivalence $\theta \in \mathrm{Eq}(G)$ is a congruence on $\mathbf{G}$ provided, $\forall a, b, a_i, b_i \in G$,

$$(a, b) \in \theta \quad \Rightarrow \quad (a^{-1}, b^{-1}) \in \theta, \quad \text{and}$$

$$(a_i, b_i) \in \theta \quad \Rightarrow \quad (a_1 \cdot a_2, b_1 \cdot b_2) \in \theta.$$

Example: *groups!*

What are the congruences of a group?

For a group $\mathbf{G} = \langle G, \cdot, ^{-1}, 1\rangle$, an equivalence $\theta \in \mathrm{Eq}(G)$ is a congruence on $\mathbf{G}$ provided, $\forall a, b, a_i, b_i \in G$,

$$(a, b) \in \theta \quad \Rightarrow \quad (a^{-1}, b^{-1}) \in \theta, \quad \text{and}$$

$$(a_i, b_i) \in \theta \quad \Rightarrow \quad (a_1 \cdot a_2, b_1 \cdot b_2) \in \theta.$$

Example: *groups!*

What are the congruences of a group?

For a group $\mathbf{G} = \langle G, \cdot, ^{-1}, 1\rangle$, an equivalence $\theta \in \mathrm{Eq}(G)$ is a congruence on $\mathbf{G}$ provided, $\forall a, b, a_i, b_i \in G$,

$$(a, b) \in \theta \quad \Rightarrow \quad (a^{-1}, b^{-1}) \in \theta, \text{ and}$$

$$(a_i, b_i) \in \theta \quad \Rightarrow \quad (a_1 \cdot a_2, b_1 \cdot b_2) \in \theta.$$

What is a lattice?

Definition (lattice)

A lattice is an algebra $\mathbf{L} = \langle L, \wedge, \vee \rangle$ with universe L, a partially ordered set, and binary operations:

$$x \wedge y = \text{g.l.b.}(x, y) \quad \text{the "meet" of } x \text{ and } y$$

$$x \vee y = \text{l.u.b.}(x, y) \quad \text{the "join" of } x \text{ and } y$$

Examples

- Subsets of a set
- Closed subsets of a topology.
- Subgroups of a group.

What is a lattice?

Definition (lattice)

A lattice is an algebra $\mathbf{L} = \langle L, \wedge, \vee \rangle$ with universe L, a partially ordered set, and binary operations:

$$x \wedge y = \text{g.l.b.}(x, y) \quad \text{the "meet" of } x \text{ and } y$$

$$x \vee y = \text{l.u.b.}(x, y) \quad \text{the "join" of } x \text{ and } y$$

Examples

- Subsets of a set
- Closed subsets of a topology.
- Subgroups of a group.

What is a lattice?

Definition (lattice)

A lattice is an algebra $\mathbf{L} = \langle L, \wedge, \vee \rangle$ with universe L, a partially ordered set, and binary operations:

$$x \wedge y = \text{g.l.b.}(x, y) \quad \text{the “meet” of } x \text{ and } y$$

$$x \vee y = \text{l.u.b.}(x, y) \quad \text{the “join” of } x \text{ and } y$$

Examples

- Subsets of a set
- Closed subsets of a topology.
- Subgroups of a group.

Example: **Sub**[**G**]

- The **lattice of subgroups** of a group **G**, denoted

$$\mathbf{Sub}[\mathbf{G}] = \langle \mathrm{Sub}[\mathbf{G}], \subseteq \rangle = \langle \mathrm{Sub}[\mathbf{G}], \wedge, \vee \rangle,$$

  has universe Sub[**G**], the set of subgroups of **G**.

- For subgroups $H, K \in \mathrm{Sub}[\mathbf{G}]$,

  meet is set intersection:

$$H \wedge K = H \cap K$$

  join is the subgroup generated by the union:

$$H \vee K = \bigcap \{J \in \mathrm{Sub}[\mathbf{G}] \mid H \cup K \subseteq J\}$$

Example: **Sub**[**G**]

- The **lattice of subgroups** of a group **G**, denoted

$$\mathbf{Sub}[\mathbf{G}] = \langle \mathrm{Sub}[\mathbf{G}], \subseteq \rangle = \langle \mathrm{Sub}[\mathbf{G}], \wedge, \vee \rangle,$$

  has universe Sub[**G**], the set of subgroups of **G**.

- For subgroups $H, K \in \mathrm{Sub}[\mathbf{G}]$,

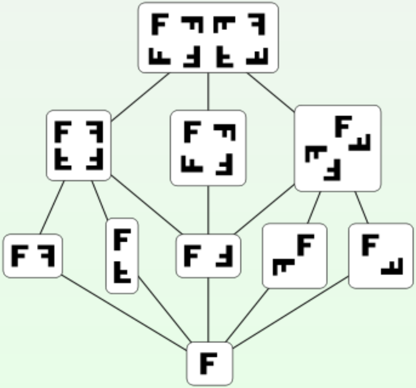
  meet is set intersection:

$$H \wedge K = H \cap K$$

  join is the subgroup generated by the union:

$$H \vee K = \bigcap \{ J \in \mathrm{Sub}[\mathbf{G}] \mid H \cup K \subseteq J \}$$

Example: Hasse diagram of **Sub**$[D_4]$



The lattice of subgroups of the dihedral group D_4, represented as groups of rotations and reflections of a plane figure.

...ok, but is it useful?

Lattice-theoretic information (about **Sub**[**G**]) can be used to obtain group-theoretic information (about **G**).

Examples:

- **G** is locally cyclic if and only if **Sub**[**G**] is distributive.

  Ore, "Structures and group theory," *Duke Math. J.* (1937)

- Similar lattice-theoretic characterizations exist for solvable and perfect groups.

  Suzuki, "On the lattice of subgroups of finite groups," *Trans. AMS* (1951)

...ok, but is it useful?

Lattice-theoretic information (about **Sub**[**G**]) can be used to obtain group-theoretic information (about **G**).

Examples:

- **G** is locally cyclic if and only if **Sub**[**G**] is distributive.

  Ore, "Structures and group theory," *Duke Math. J.* (1937)

- Similar lattice-theoretic characterizations exist for solvable and perfect groups.

  Suzuki, "On the lattice of subgroups of finite groups," *Trans. AMS* (1951)

...ok, but is it useful?

Lattice-theoretic information (about **Sub**[**G**]) can be used to obtain group-theoretic information (about **G**).

Examples:

- **G** is locally cyclic if and only if **Sub**[**G**] is distributive.

  Ore, “Structures and group theory,” *Duke Math. J.* (1937)
- Similar lattice-theoretic characterizations exist for solvable and perfect groups.

  Suzuki, “On the lattice of subgroups of finite groups,” *Trans. AMS* (1951)

...ok, but is it useful?

Lattice-theoretic information (about **Sub**[**G**]) can be used to obtain group-theoretic information (about **G**).

Examples:

- **G** is locally cyclic if and only if **Sub**[**G**] is distributive.

  Ore, "Structures and group theory," *Duke Math. J.* (1937)

- Similar lattice-theoretic characterizations exist for solvable and perfect groups.

  Suzuki, "On the lattice of subgroups of finite groups," *Trans. AMS* (1951)

ConA is a lattice

- The set Con(**A**), ordered by set inclusion, is a 0-1 lattice:

$$\mathbf{ConA} = \langle \mathrm{Con}(\mathbf{A}), \subseteq \rangle = \langle \mathrm{Con}(\mathbf{A}), \wedge, \vee \rangle$$

  - The greatest congruence is the *all* relation

$$\nabla = A \times A$$

  - The least congruence is the *diagonal*

$$\Delta = \{(x, y) \in A \times A \mid x = y\}$$

  - What are meet and join?

Con A is a lattice

- The set Con(**A**), ordered by set inclusion, is a 0-1 lattice:

$$\mathbf{Con A} = \langle \mathrm{Con}(\mathbf{A}), \subseteq \rangle = \langle \mathrm{Con}(\mathbf{A}), \wedge, \vee \rangle$$

  - The greatest congruence is the *all* relation

$$\nabla = A \times A$$

  - The least congruence is the *diagonal*

$$\Delta = \{(x, y) \in A \times A \mid x = y\}$$

  - What are meet and join?

Con A is a lattice

- The set Con(**A**), ordered by set inclusion, is a 0-1 lattice:

$$\mathbf{Con\,A} = \langle \mathrm{Con}(\mathbf{A}), \subseteq \rangle = \langle \mathrm{Con}(\mathbf{A}), \wedge, \vee \rangle$$

  - The greatest congruence is the *all* relation

$$\nabla = A \times A$$

  - The least congruence is the *diagonal*

$$\Delta = \{(x, y) \in A \times A \mid x = y\}$$

  - What are meet and join?

Con A is a lattice

- The set Con(**A**), ordered by set inclusion, is a 0-1 lattice:

$$\mathbf{Con\,A} = \langle \mathrm{Con}(\mathbf{A}), \subseteq \rangle = \langle \mathrm{Con}(\mathbf{A}), \wedge, \vee \rangle$$

  - The greatest congruence is the *all* relation

$$\nabla = A \times A$$

  - The least congruence is the *diagonal*

$$\Delta = \{(x, y) \in A \times A \mid x = y\}$$

  - What are meet and join?

The finite lattice representation problem

Definition (representable lattice)

Call a finite lattice representable if it is (isomorphic to) the congruence lattice of a finite algebra.

The ($\leq$ \$1m) question

Is every finite lattice representable?

Equivalently, given a finite lattice $\mathbf{L}$, does there exist a finite algebra $\mathbf{A}$ such that $\mathbf{Con}\mathbf{A} \cong \mathbf{L}$?

The finite lattice representation problem

Definition (representable lattice)

Call a finite lattice representable if it is (isomorphic to) the congruence lattice of a finite algebra.

The ($\leq$ \$1m) question

Is every finite lattice representable?

Equivalently, given a finite lattice $\mathbf{L}$, does there exist a finite algebra $\mathbf{A}$ such that $\mathbf{Con A} \cong \mathbf{L}$?

The finite lattice representation problem

Definition (representable lattice)

Call a finite lattice representable if it is (isomorphic to) the congruence lattice of a finite algebra.

The ($\leq$ \$1m) question

Is every finite lattice representable?

Equivalently, given a finite lattice $\mathbf{L}$, does there exist a finite algebra $\mathbf{A}$ such that $\mathbf{Con A} \cong \mathbf{L}$?

What is a G-set?

Let $\mathbf{G} = \langle G, \cdot, ^{-1}, 1_G \rangle$ be a group, A a set.

Definition (G-set)

A G-set is a unary algebra $\mathbf{A} = \langle A, \overline{G} \rangle$, where $\overline{G} = \{\bar{g} : g \in G\}$, $\overline{1_G} = \mathrm{id}_A$, and $\overline{g_1} \circ \overline{g_2} = \overline{g_1 \cdot g_2}$, for all $g_i \in G$.

Definition (stabilizer)

For any $a \in A$, the stabilizer of a is the set

$$\mathrm{Stab}(a) = \{g \in G \mid \bar{g}(a) = a\}$$

What is a G-set?

Let $\mathbf{G} = \langle G, \cdot, ^{-1}, 1_G \rangle$ be a group, A a set.

Definition (G-set)

A G-set is a unary algebra $\mathbf{A} = \langle A, \overline{G} \rangle$, where $\overline{G} = \{\bar{g} : g \in G\}$, $\overline{1_G} = \mathrm{id}_A$, and $\overline{g_1} \circ \overline{g_2} = \overline{g_1 \cdot g_2}$, for all $g_i \in G$.

Definition (stabilizer)

For any $a \in A$, the stabilizer of a is the set

$$\mathrm{Stab}(a) = \{g \in G \mid \bar{g}(a) = a\}$$

What is a G-set?

Let $\mathbf{G} = \langle G, \cdot, ^{-1}, 1_G \rangle$ be a group, A a set.

Definition (G-set)

A G-set is a unary algebra $\mathbf{A} = \langle A, \overline{G} \rangle$, where $\overline{G} = \{\bar{g} : g \in G\}$, $\overline{1_G} = \mathrm{id}_A$, and $\overline{g_1} \circ \overline{g_2} = \overline{g_1 \cdot g_2}$, for all $g_i \in G$.

Definition (stabilizer)

For any $a \in A$, the stabilizer of a is the set

$$\mathrm{Stab}(a) = \{g \in G \mid \bar{g}(a) = a\}$$

G-sets: basic facts and transitivity

Basic facts about the G-set $\langle A, \overline{G}\rangle$ (efts)

1. Each $\bar{g} \in \overline{G}$ is a permutation of A.
2. If $[a]$ is the subalgebra generated by $a \in A$, then

$$[a] = \{\bar{g}(a) \mid g \in G\} = \text{ the orbit of } a \text{ in } A.$$

3. The stabilizer $\mathbf{Stab}(a)$ is a subgroup of $\mathbf{G}$.

Definition (trasitive G-set)

If $\mathbf{A} = \langle A, \overline{G}\rangle$ has only one orbit, we say $\mathbf{G}$ acts transitively on $\mathbf{A}$, or $\mathbf{A}$ is a transitive G-set.

G-sets: basic facts and transitivity

Basic facts about the G-set $\langle A, \overline{G}\rangle$ (efts)

1. Each $\bar{g} \in \overline{G}$ is a permutation of A.
2. If $[a]$ is the subalgebra generated by $a \in A$, then

$$[a] = \{\bar{g}(a) \mid g \in G\} = \text{ the orbit of } a \text{ in } A.$$

3. The stabilizer $\mathbf{Stab}(a)$ is a subgroup of $\mathbf{G}$.

Definition (trasitive G-set)

If $\mathbf{A} = \langle A, \overline{G}\rangle$ has only one orbit, we say $\mathbf{G}$ acts transitively on $\mathbf{A}$, or $\mathbf{A}$ is a transitive G-set.

G-sets: basic facts and transitivity

Basic facts about the G-set $\langle A, \overline{G} \rangle$ (efts)

1. Each $\bar{g} \in \overline{G}$ is a permutation of A.
2. If $[a]$ is the subalgebra generated by $a \in A$, then

$$[a] = \{\bar{g}(a) \mid g \in G\} = \text{ the orbit of } a \text{ in } A.$$

3. The stabilizer $\mathbf{Stab}(a)$ is a subgroup of $\mathbf{G}$.

Definition (trasitive G-set)

If $\mathbf{A} = \langle A, \overline{G} \rangle$ has only one orbit, we say $\mathbf{G}$ acts transitively on $\mathbf{A}$, or $\mathbf{A}$ is a transitive G-set.

G-sets: basic facts and transitivity

Basic facts about the G-set $\langle A, \overline{G}\rangle$ (efts)

1. Each $\bar{g} \in \overline{G}$ is a permutation of A.
2. If $[a]$ is the subalgebra generated by $a \in A$, then

$$[a] = \{\bar{g}(a) \mid g \in G\} = \text{ the orbit of } a \text{ in } A.$$

3. The stabilizer $\mathbf{Stab}(a)$ is a subgroup of $\mathbf{G}$.

Definition (trasitive G-set)

If $\mathbf{A} = \langle A, \overline{G}\rangle$ has only one orbit, we say $\mathbf{G}$ acts transitively on $\mathbf{A}$, or $\mathbf{A}$ is a transitive G-set.

G-sets: basic facts and transitivity

Basic facts about the G-set $\langle A, \overline{G}\rangle$ (efts)

1. Each $\bar{g} \in \overline{G}$ is a permutation of A.
2. If $[a]$ is the subalgebra generated by $a \in A$, then

$$[a] = \{\bar{g}(a) \mid g \in G\} = \text{ the orbit of } a \text{ in } A.$$

3. The stabilizer $\mathbf{Stab}(a)$ is a subgroup of $\mathbf{G}$.

Definition (trasitive G-set)

If $\mathbf{A} = \langle A, \overline{G}\rangle$ has only one orbit, we say $\mathbf{G}$ acts transitively on $\mathbf{A}$, or $\mathbf{A}$ is a transitive G-set.

Fundamental theorem of transitive G-sets

Definition (interval in a subgroup lattice)

If $\mathbf{G}$ is a group and $\mathbf{H} \in \mathrm{Sub}[\mathbf{G}]$ is a subgroup, define

$$[\mathbf{H}, \mathbf{G}] = \langle \{\mathbf{K} \in \mathrm{Sub}[\mathbf{G}] \mid \mathbf{H} \subseteq \mathbf{K}\}, \subseteq \rangle$$

Call $[\mathbf{H}, \mathbf{G}]$ an *(upper) interval* in the lattice $\mathbf{Sub}[G]$.

Theorem

If $\mathbf{A} = \langle A, \overline{G} \rangle$ is a transitive G-set, then for any $a \in A$,

$$\mathbf{Con}\mathbf{A} \cong [\mathbf{Stab}(a), \mathbf{G}]$$

Fundamental theorem of transitive G-sets

Definition (interval in a subgroup lattice)

If $\mathbf{G}$ is a group and $\mathbf{H} \in \mathrm{Sub}[\mathbf{G}]$ is a subgroup, define

$$[\mathbf{H}, \mathbf{G}] = \langle \{\mathbf{K} \in \mathrm{Sub}[\mathbf{G}] \mid \mathbf{H} \subseteq \mathbf{K}\}, \subseteq \rangle$$

Call $[\mathbf{H}, \mathbf{G}]$ an *(upper) interval* in the lattice $\mathbf{Sub}[G]$.

Theorem

If $\mathbf{A} = \langle A, \overline{G} \rangle$ is a transitive G-set, then for any $a \in A$,

$$\mathbf{Con}\mathbf{A} \cong [\mathbf{Stab}(a), \mathbf{G}]$$

A pair of groundbreaking results

Theorem (Pudlák and Tůma, AU 10, 1980)

A finite lattice can be embedded in $Eq(X)$, for some finite X.

Theorem (Pálfy and Pudlák, AU 11, 1980)

The following statements are equivalent:

(i) *Any finite lattice is isomorphic to the congruence lattice of a finite algebra.*

(ii) *Any finite lattice is isomorphic to an interval in the subgroup lattice of a finite group.*

A pair of groundbreaking results

Theorem (Pudlák and Tůma, AU 10, 1980)

A finite lattice can be embedded in Eq(X), for some finite X.

Theorem (Pálfy and Pudlák, AU 11, 1980)

The following statements are equivalent:

(i) *Any finite lattice is isomorphic to the congruence lattice of a finite algebra.*

(ii) *Any finite lattice is isomorphic to an interval in the subgroup lattice of a finite group.*

The Pálfy-Pudlák theorem: what does it (not) say?

A quote from MathSciNet reviews

"In AU 11, Pálfy and Pudlák proved that...a finite lattice is representable if and only if it occurs as an interval in the subgroup lattice of a finite group."

False!

The Pálfy-Pudlák theorem: what does it (not) say?

A quote from MathSciNet reviews

"In AU 11, Pálfy and Pudlák proved that...a finite lattice is representable if and only if it occurs as an interval in the subgroup lattice of a finite group."

False!

The Pálfy-Pudlák theorem: what does it (not) say?

A quote from MathSciNet reviews

"In AU 11, Pálfy and Pudlák proved that...a finite lattice is representable if and only if it occurs as an interval in the subgroup lattice of a finite group."

False!

The seminal lemma of tct

Lemma

Let $\mathbf{A} = \langle A, F \rangle$ *be a unary algebra with* $e^2 = e \in F$.

Define $\mathbf{B} = \langle B, G \rangle$ *with*

$$B = e(A) \quad \text{and} \quad G = \{ef|_B : f \in F\}$$

Then

$$Con(\mathbf{A}) \ni \theta \mapsto \theta \cap (B \times B) \in Con(\mathbf{B})$$

is a lattice epimorphism.

The seminal lemma of tct

Lemma

Let $\mathbf{A} = \langle A, F\rangle$ *be a unary algebra with* $e^2 = e \in F$.

Define $\mathbf{B} = \langle B, G\rangle$ *with*

$$B = e(A) \quad \text{and} \quad G = \{ef|_B : f \in F\}$$

Then

$$Con(\mathbf{A}) \ni \theta \mapsto \theta \cap (B \times B) \in Con(\mathbf{B})$$

is a lattice epimorphism.

Consequence of the seminal lemma

Theorem

Let $\mathbf{L}$ *be a finite lattice satisfying conditions (A), (B), (C).*

Let $\mathbf{A} = \langle A, F \rangle$ *be a finite unary algebra of minimal cardinality such that* $\mathbf{Con}\mathbf{A} \cong \mathbf{L}$.

Then $\mathbf{A}$ *is a transitive G-set.*

$$\therefore \quad \mathbf{L} \cong \mathbf{Con}\mathbf{A} \cong [\mathbf{Stab}(a), \mathbf{G}]$$

Consequence of the seminal lemma

Theorem

Let $\mathbf{L}$ *be a finite lattice satisfying conditions (A), (B), (C).*

Let $\mathbf{A} = \langle A, F\rangle$ *be a finite unary algebra of minimal cardinality such that* $\mathbf{Con}\mathbf{A} \cong \mathbf{L}$.

Then $\mathbf{A}$ *is a transitive G-set.*

$$\therefore \quad \mathbf{L} \cong \mathbf{Con}\mathbf{A} \cong [\mathbf{Stab}(a), \mathbf{G}]$$

Consequence of the seminal lemma

Theorem

Let $\mathbf{L}$ *be a finite lattice satisfying conditions (A), (B), (C).*

Let $\mathbf{A} = \langle A, F\rangle$ *be a finite unary algebra of minimal cardinality such that* $\mathbf{Con}\mathbf{A} \cong \mathbf{L}$*.*

Then $\mathbf{A}$ *is a transitive G-set.*

$$\therefore \quad \mathbf{L} \cong \mathbf{Con}\mathbf{A} \cong [\mathbf{Stab}(a), \mathbf{G}]$$

Summary

- Problem: Given a finite lattice $\mathbf{L}$, does there exist a finite algebra $\mathbf{A}$ such that $\mathbf{L} \cong \mathbf{Con}\mathbf{A}$?
- It is generally believed the answer is no.
- About 30 years ago Pálfy and Pudlák translated it into one for the group theorists, but still no answer...
- Outlook: *bleak*
  - Something you haven't solved.
  - Something else you haven't solved.

Summary

- Problem: Given a finite lattice $\mathbf{L}$, does there exist a finite algebra $\mathbf{A}$ such that $\mathbf{L} \cong \mathbf{Con}\mathbf{A}$?
- It is generally believed the answer is no.
- About 30 years ago Pálfy and Pudlák translated it into one for the group theorists, but still no answer...
- Outlook: *bleak*
  - Something you haven't solved.
  - Something else you haven't solved.

Summary

- Problem: Given a finite lattice $\mathbf{L}$, does there exist a finite algebra $\mathbf{A}$ such that $\mathbf{L} \cong \mathbf{Con}\mathbf{A}$?
- It is generally believed the answer is no.
- About 30 years ago Pálfy and Pudlák translated it into one for the group theorists, but still no answer...
- Outlook: *bleak*
  - Something you haven't solved.
  - Something else you haven't solved.

Summary

- Problem: Given a finite lattice $\mathbf{L}$, does there exist a finite algebra $\mathbf{A}$ such that $\mathbf{L} \cong \mathbf{Con}\,\mathbf{A}$?
- It is generally believed the answer is no.
- About 30 years ago Pálfy and Pudlák translated it into one for the group theorists, but still no answer...
- Outlook: *bleak*
  - Something you haven't solved.
  - Something else you haven't solved.

Summary

- Problem: Given a finite lattice $\mathbf{L}$, does there exist a finite algebra $\mathbf{A}$ such that $\mathbf{L} \cong \mathbf{Con A}$?
- It is generally believed the answer is no.
- About 30 years ago Pálfy and Pudlák translated it into one for the group theorists, but still no answer...
- Outlook: *bleak*
  - Something you haven't solved.
  - Something else you haven't solved.

Summary

- Problem: Given a finite lattice $\mathbf{L}$, does there exist a finite algebra $\mathbf{A}$ such that $\mathbf{L} \cong \mathbf{Con}\mathbf{A}$?
- It is generally believed the answer is no.
- About 30 years ago Pálfy and Pudlák translated it into one for the group theorists, but still no answer...
- Outlook: *bleak*
  - Something you haven't solved.
  - Something else you haven't solved.