The finite congruence lattice problem

Péter P. Pálfy
Alfréd Rényi Institute of Mathematics,
Hungarian Academy of Sciences
and
Eötvös University, Budapest

Summer School on General Algebra and Ordered Sets
Stará Lesná, September 6, 2009

Outline

0. **Quick introduction**
1. **Reductions (today)**
   - minimal unary algebras
   - transitive permutation groups
   - almost simple groups
   - twisted wreath products
2. **Background (Wednesday)**
   - more details
   - some history
3. **Some constructions (Thursday)**
   - closure properties
   - hereditary congruence lattices

0. Quick introduction

Theorem (Grätzer György – Schmidt Tamás, 1963)
For every algebraic lattice L there exists an algebra with congruence lattice isomorphic to L.

L is **representable** (as a congruence lattice)

Proofs by Grätzer and Schmidt (1963), Lampe (1973), Pudlák (1976), Tůma (1989) (almost) always yield an infinite algebra, even if L is finite.

The finite congruence lattice problem
Is it true that for every finite lattice L there exists a finite algebra with congruence lattice isomorphic to L ?

L is **finitely representable** (as a congruence lattice)

1. Reductions

$\mathrm{Con}(U; F) = \mathrm{Con}(U; \mathrm{Pol}_1(U; F))$, so we will assume that the algebra is unary, and the operations form a transformation monoid.

If L is finitely representable, we will take a representation where $|U|$ is minimal such that $\mathrm{Con}(U; F) \cong L$.

Theorem (Pavel Pudlák – P^3, 1980)
If L satisfies certain assumptions , then the operations form a transitive permutation group .

1. Reductions

$\mathrm{Con}(U;F) = \mathrm{Con}(U;\mathrm{Pol}_1(U;F))$, so we will assume that the algebra is unary, and the operations form a transformation monoid.

If L is finitely representable, we will take a representation where $|U|$ is minimal such that $\mathrm{Con}(U;F) \cong L$.

Theorem (Pavel Pudlák – P^3, 1980)
If L satisfies certain assumptions (that will be specified in Lecture 2), then (in the minimal unary representation of L) the operations form a transitive permutation group (after removing the constant operations).

1. Reductions

$\mathrm{Con}(U; F) = \mathrm{Con}(U; \mathrm{Pol}_1(U; F))$, so we will assume that the algebra is unary, and the operations form a transformation monoid.

If L is finitely representable, we will take a representation where $|U|$ is minimal such that $\mathrm{Con}(U; F) \cong L$.

Theorem (Pavel Pudlák – P^3, 1980)
If L satisfies certain assumptions (that will be specified in Lecture 2), then (in the minimal unary representation of L) the operations form a transitive permutation group (after removing the constant operations).

This leads to the following equivalent formulation of the finite congruence representation problem:

Is it true that for every finite lattice L there exists a finite group G and a (core-free) subgroup $H \leq G$ such that the interval $\mathrm{Int}(H; G)$ of the subgroup lattice consisting of the subgroups containing H is isomorphic to L ?

Transitive permutation groups

G a group acting from the right on the set U

$(U; G)$ is also called a **G-set**

Notation: $u \mapsto u^g$ $(u \in U,\ g \in G)$

$u^{(g_1 g_2)} = (u^{g_1})^{g_2},\ u^1 = u$

stabilizer of $u \in U$: $G_u = \{g \in G \mid u^g = u\} \leq G$

$G_{u^g} = g^{-1} G_u g$

G is **transitive**: $\forall u, v \in U\ \exists g \in G : u^g = v$, i.e., the unary algebra $(U; G)$ has no proper subalgebra.

The core

The kernel of a transitive action of G on U is

$$\{g \in G \mid \forall v \in U : v^g = v\} = \bigcap_{v \in U} G_v = \bigcap_{g \in G} g^{-1} G_u g,$$

the largest normal subgroup of G contained in the stabilizer G_u, the **core** of G_u.

So we can assume that H is **core-free** in G, i.e., $\bigcap_{g \in G} g^{-1} H g = 1$.

In fact, if $N \lhd G$ and $N \leq H$, then $\mathrm{Int}(H; G) \cong \mathrm{Int}(H/N; G/N)$.

The strategy

Is it true that for every finite lattice L there exists a finite group G and a core-free subgroup $H \leq G$ such that $\mathrm{Int}(H; G) \cong L$?

We try to reduce the question to the case when G is an **almost simple group**: G has a normal subgroup S which is a nonabelian simple group and $\mathbf{C}_G(S) = 1$.
Hence G embeds into $\mathrm{Aut}(S)$. If we identify S with the subgroup of $\mathrm{Aut}(S)$ consisting of the inner automorphisms (the conjugations by elements of S), then we obtain $\mathrm{Inn}(S) \leq G \leq \mathrm{Aut}(S)$.

Fact (**Schreier's Conjecture**): For every finite simple group S, the **outer automorphism group** $\mathrm{Aut}(S)/\mathrm{Inn}(S)$ is solvable.
Established using the Classification of Finite Simple Groups (**CFSG**).

If the problem is reduced to the case of almost simple groups, then using the CFSG one can attack it by a case-by-case analysis.

Three important papers

Robert Baddeley, A new approach to the finite lattice representation problem, Periodica Mathematica Hungarica 36 (1998), 17–59.

Ferdinand Börner, A remark on the finite lattice representation problem, Contributions to General Algebra 11, Proceedings of the Olomouc Conference and the Summer School 1998, Verlag Johannes Heyn, Klagenfurt 1999, 5–38.

Michael Aschbacher, On intervals in subgroup lattices of finite groups, Journal of the American Mathematical Society 21 (2008), 809–830.

Their conclusion: G is almost simple

Three important papers

Robert Baddeley, A new approach to the finite lattice representation problem, Periodica Mathematica Hungarica 36 (1998), 17–59.

Ferdinand Börner, A remark on the finite lattice representation problem, Contributions to General Algebra 11, Proceedings of the Olomouc Conference and the Summer School 1998, Verlag Johannes Heyn, Klagenfurt 1999, 5–38.

Michael Aschbacher, On intervals in subgroup lattices of finite groups, Journal of the American Mathematical Society 21 (2008), 809–830.

Their conclusion: G is almost simple or a twisted wreath product.

What to do now?

Analyze the case of twisted wreath products.

Either show that such groups cannot represent all finite lattices, so get a reduction to the almost simple case,

or represent every finite lattice as an interval in the subgroup lattice of a twisted wreath product, perhaps in some "combinatorial" way.

The obstacle

Twisted wreath product (Bernhard H. Neumann, 1963)

Ingredients:

- base group B,
- outer group H,
- a subgroup $A \leq H$,
- a homomorphism $\alpha : A \to \mathrm{Aut}(B)$; it defines an action of A on B, which will be denoted — as before — by b^a (instead of $b^{\alpha(a)}$).

(If α maps every element of A to the identical automorphism of B, then we obtain the ordinary wreath product — without twist.)

Twisted wreath product (1)

Given: $H \geq A \to \mathrm{Aut}(B)$

Construction:

$B^H = \{f : H \to B\}$ (all functions). It is a group with pointwise multiplication, isomorphic to $B^{|H|} = B \times \cdots \times B$.

Define the action of H on B^H by

$$f^h(x) = f(hx) \qquad (f \in B^H, h \in H, x \in H).$$

It is indeed an action:
$f^{h_1 h_2}(x) = f((h_1 h_2)x) = f(h_1(h_2 x)) = f^{h_1}(h_2 x) = (f^{h_1})^{h_2}(x)$.

$f \mapsto f^h$ (for a fixed $h \in H$) is an automorphism of B^H:
$(f_1 f_2)^h(x) = (f_1 f_2)(hx) = f_1(hx) f_2(hx) = f_1^h(x) f_2^h(x)$.

(The semidirect product of H and B^H is the regular wreath product of B and H.)

Twisted wreath product (2)

Given: $H \geq A \to \mathrm{Aut}(B)$.
So far we have constucted B^H and the action of H on it.
Here comes the twist:

Let

$$U = \{u : H \to B \mid \forall x \in H, a \in A : u(xa) = u(x)^a\}.$$

It is a subgroup of B^H, and $U \cong B^{|H:A|}$. Namely, the value $u(x)$ determines the values on the whole left coset xA.

If $u \in U$, $h \in H$, then $u^h(xa) = u(hxa) = u(hx)^a = (u^h(x))^a$, so $u^h \in U$, i.e., U is an H-invariant subgroup of B^H.

HU is the **twisted wreath product** of the ingredients (B, H, A, α).
$(h_1 u_1)(h_2 u_2) = (h_1 h_2)(u_1^{h_2} u_2)$

The interval $\mathrm{Int}(H; HU)$

If $H \leq X \leq HU$, then $X = H(U \cap X)$, where $U \cap X$ is an H-invariant subgroup of U.

Conversely, if $V \leq U$ is H-invariant, then $H \leq HV \leq HU$.

So

$$\mathrm{Int}(H; HU) \cong \mathrm{Sub}^H(U),$$

the lattice of H-invariant subgroups of U.

Restrictive conditions

In general, $\mathrm{Sub}^H(U)$ is too complex, but the reduction in the papers of Baddeley, Börner, and Aschbacher leads to twisted wreath products with severely restricted ingredients.

- (a) B is a nonabelian simple group,
- (b) $\alpha(A) \geq \mathrm{Inn}(B)$,
- (c) $\mathrm{Ker}\,\alpha$ is core-free in H.

We have to determine $\mathrm{Sub}^H(U)$, the lattice of H-invariant subgroups of U under these hypotheses.

$\mathrm{Sub}^H(U)$ (1)

Let $1 \neq V \leq U \leq B^H$ be a nontrivial H-invariant subgroup.

Let $V(x) = \{v(x) \mid v \in V\} \leq B$ $(x \in H)$.

Since V is H-invariant,

$$V(x) = \{v(x1) \mid v \in V\} = \{v^x(1) \mid v \in V\} = V(1),$$

so $V(x)$ is independent of x.

For $a \in A$,

$$V(1) = V(a) = \{v(1a) \mid v \in V\} = \{v(1)^a \mid v \in V\} = V(1)^a.$$

Now since every inner automorphism of B is induced by some element of A (Condition (b)), $V(1)$ is a normal subgroup of B, hence by the simplicity of B (Condition (a)), $V(x) = V(1) = B$, i.e., V is a subdirect power of B.

Subdirect powers

What does a subdirect power of a nonabelian simple group look like?

(It is an essential ingredient in the proof of the O'Nan–Scott[–Aschbacher] Theorem on primitive permutation groups.)

Lemma. Let B be a nonabelian simple group and $V \leq B^n$ a subdirect power of B. Then V is isomorphic to B^m for some $1 \leq m \leq n$ via an isomorphism $B^m \to V$,

$$(b_1, \ldots, b_m) \mapsto (b_{i(1)}^{\beta_1}, \ldots, b_{i(n)}^{\beta_n}),$$

where $i : \{1, \ldots, n\} \to \{1, \ldots, m\}$ is a surjective map and $\beta_1, \ldots, \beta_n \in \mathrm{Aut}(B)$.

Example. $n = 5$, $m = 2$:
$V = \{(b_1, b_1^{\beta}, b_2, b_1^{\gamma}, b_2^{\beta}) \mid b_1, b_2 \in B\} \leq B^5$

$\mathrm{Sub}^H(U)$ (2)

Let $1 \neq V \leq U \leq B^H$ be a nontrivial H-invariant subgroup.

Define $T = \{t \in H \mid \forall v \in V : v(1) = 1 \implies v(t) = 1\}$, and for $t \in T$ let $\beta(t) \in \mathrm{Aut}(B)$ such that $v(t) = v(1)^{\beta(t)}$.

If $u \in U$, then $u(a) = u(1)^a$, hence $A \leq T$, and $\beta(a) = \alpha(a)$ for all $a \in A$.

$v(xt) = v^x(t) = v^x(1)^{\beta(t)} = v(x)^{\beta(t)}$ $(x \in H,\ t \in T)$,
$v(t_1 t_2) = v(t_1)^{\beta(t_2)} = v(1)^{\beta(t_1)\beta(t_2)}$ $(t_1, t_2 \in T)$, so T is a subgroup and $\beta(t_1 t_2) = \beta(t_1)\beta(t_2)$, i.e., $\beta : T \to \mathrm{Aut}(B)$ is a homomorphism.

Thus HV is the twisted wreath product constructed from the data (B, H, T, β).

Theorem. The dual of the lattice $\mathrm{Sub}^H(U) \cong \mathrm{Int}(H; HU)$ is isomorphic to the lattice of all extensions of α to subgroups of H with a largest element added.

Examples

$B = A_5$, $H = S_5 \times A_5$, $A = \{(a, a) \mid a \in A_5\}$, α the natural mapping $A \cong A_5 \to \mathrm{Aut}(B) = \mathrm{Aut}(A_5) \cong S_5$
The subgroups containing A are $A < A_5 \times A_5 < S_5 \times A_5 = H$.
There are two extensions of α to both $A_5 \times A_5$ and $S_5 \times A_5$ (the projections).
So $\mathrm{Int}(H; HU)$ is the hexagon.

Aschbacher gave a somewhat different example yielding the hexagon. It also provided an answer to a question about von Neumann algebras left open by Watatani (1996).
$B = A_5$, $H = A_6 \times A_6$, $A = \{(a, a) \mid a \in A_5\}$
The subgroups containing A are
$A < A_5 \times A_5 < A_6 \times A_5, A_5 \times A_6 < A_6 \times A_6 = H$.
There are two extensions of α to $A_5 \times A_5$, unique extensions to both $A_6 \times A_5$ and $A_5 \times A_6$, and no extension to $H = A_6 \times A_6$.

Happy birthday

I learned about the finite congruence lattice problem at Ervin Fried's seminar in 1976.

Ervin Fried was born on September 6, 1929.

Happy birthday!

The finite congruence lattice problem
2. More background and history

Péter P. Pálfy
Alfréd Rényi Institute of Mathematics,
Hungarian Academy of Sciences
and
Eötvös University, Budapest

Summer School on General Algebra and Ordered Sets
Stará Lesná, September 9, 2009

The finite congruence lattice problem

Is it true that for every finite lattice L there exists a finite algebra with congruence lattice isomorphic to L ?
L is **finitely representable** (as a congruence lattice)

$\mathrm{Con}(U; F) \cong \mathrm{Con}(U; \mathrm{Pol}_1(U; F))$,
since if $f \in F$, $f : U^n \to U$, and $u_1 \equiv v_1, \ldots, u_n \equiv v_n$, then
$f(u_1, u_2, u_3, \ldots, u_n) \equiv f(v_1, u_2, u_3, \ldots, u_n) \equiv$
$f(v_1, v_2, u_3, \ldots, u_n) \equiv \cdots \equiv f(v_1, v_2, v_3, \ldots, v_n)$.
So we assume that the algebra is unary, and the operations form a transformation monoid F.

If L is finitely representable, we will take a representation where $|U|$ is minimal such that $\mathrm{Con}(U; F) \cong L$.
Variation (Aschbacher): $|U|$ minimal such that $\mathrm{Con}(U; F)$ is isomorphic to L or its dual.
Börner uses self-dual lattices in his proof.

P^5

Theorem (Pavel Pudlák – P^3, 1980)
Let L be a finite lattice such that

- L is simple,
- $\forall\, 0 \neq x \in L\ \exists\, y_1, y_2 \in L : x \vee y_1 = x \vee y_2 = 1,\ y_1 \wedge y_2 = 0$,
- $|L| > 2$, and if $0 \neq x \in L$ is not an atom, then there are at least four atoms $< x$.

Suppose that $(U; F)$ is minimal such that $\mathrm{Con}(U; F) \cong L$, where F is a transformation monoid. Then F is a transitive permutation group (together with some constant operations).

Theorem (P^3, 1984)
Let $2 < |U| < \infty$. If $\mathrm{Pol}_1(U; F)$ is a permutation group together with all constants, then either the algebra is essentially unary, or it is polynomially equivalent to a vector space.

Tame Congruence Theory (Hobby–McKenzie, 1983)

The finite congruence lattice problem is a group theoretic problem.

Transitive permutation groups

If H is a subgroup of G then we get a transitive action of G on the set of right cosets of H by taking $(Hx)^g = Hxg$ $(x, g \in G)$. This G-set is denoted by $(G : H; G)$. Here the stabilizer of the coset H is H itself.

If G acts transitively on U, then choosing an element $u \in U$, the elements of U are in one-to-one correspondence with the right cosets of the stabilizer G_u, namely, $v \leftrightarrow \{g \in G \mid u^g = v\}$. Thus $(U; G) \cong (G : G_u; G)$.

So there is a one-to-one correspondence between the transitive actions of G and the conjugacy classes of subgroups in G.

If $\varphi : (U; G) \to (V; G)$ is a homomorphism, then clearly $G_u \leq G_{\varphi(u)}$. Conversely, if $H \leq K \leq G$, then $Hx \mapsto Kx$ gives a well-defined homomorphism $(G : H; G) \to (G : K; G)$.

Thus if G acts transitively on U, then $\mathrm{Con}(U; G) \cong \mathrm{Int}(G_u; G)$.

We will assume that the action is core-free, i.e., $\bigcap_{g \in G} g^{-1} H g = 1$.

Normal subgroups

Let $1 \neq N \lhd G$ be a normal subgroup, $X = HN$.
Then $X > H$, since H is core-free.
If $H \leq Y \leq G$, then $Y \vee X = YX = YN$, hence
$|Y| = |Y \vee X||Y \wedge X||X|^{-1}$.
So $\mathrm{Int}(H; G)$ cannot contain a pentagon with X and $Y_1 < Y_2$ such that $Y_1 \vee X = Y_2 \vee X$, $Y_1 \wedge X = Y_2 \wedge X$.
Hence $X = HN$ is a **modular element** in $\mathrm{Int}(H; G)$.

If there are no modular elements in L other than 0 and 1, then $HN = G$ for every nontrivial normal subgroup N, i.e., N acts transitively on $G : H$.
Such permutation groups are called **quasi-primitive**.

Example for such L.

Minimal normal subgroups

Let G be a finite group, $N \lhd G$ a minimal normal subgroup (so N is **characteristically simple**, i.e., no nontrivial proper subgroup of N is invariant for all automorphisms of N), then

- either N is an elementary abelian p-group (p prime),
- or $N = S_1 \times \cdots \times S_k$ ($k \geq 1$) is a direct product of pairwise isomorphic nonabelian simple groups.

In a quasiprimitive group $G = HN$, so

$$\mathrm{Int}(H; G) \cong \mathrm{Int}^H(H \cap N; N).$$

In the first case it is a sublattice of the subgroup lattice of an abelian group, hence modular.
Let us consider the second case, where N is a nonabelian characteristically simple group.

Characteristically simple groups

$N = S_1 \times \cdots \times S_k$

The only simple normal subgroups of N are $S_1, \ldots, S_k$.
They are permuted transitively by H (in the conjugation action).

Let $A = \mathbf{N}_H(S_1)$, then $|H : A| = k$; $\alpha : A \to \mathrm{Aut}(S_1)$.

If $H \cap N = 1$, then G is the twisted wreath product determined by (S_1, H, A, α).

How can we force $\alpha(A) \geq \mathrm{Inn}(S_1)$?

What happens if $H \cap N \neq 1$?

These questions are analyzed in the papers of Baddeley, Börner, and Aschbacher.

A little bit of taste

If $1 < R_1 < S_1$ is an A-invariant subgroup, then

$$\langle h^{-1} R_1 h | h \in H \rangle = R_1 \times R_2 \times \cdots \times R_k$$

is H-invariant.
If all subgroups in $\mathrm{Int}^H(H \cap N; N)$ have this form, then $\mathrm{Int}^H(H \cap N; N) \cong \mathrm{Int}^A(A \cap S_1; S_1) \cong \mathrm{Int}(A; AS_1)$.
AS_1 is not necessarily an almost simple group, but it has a simple normal subgroup (although maybe with a nontrivial centralizer).

If $H \cap N$ is a subdirect product in $N = S_1 \times \cdots \times S_k$, then we can use the description of subdirect powers of simple groups as it was given in the first lecture.

Signalizer lattices (1)

The twisted wreath product HU is built up form (B, H, A, α).

Theorem. The dual of the lattice $\mathrm{Sub}^H(U)$ is isomorphic to the lattice of all extensions of α to subgroups of H with a largest element added.

$\beta : T \to \mathrm{Aut}(B)$, $\beta\big|_A = \alpha$

$\mathrm{Aut}(B) \geq \beta(T) \geq \alpha(A) \geq \mathrm{Inn}(B)$

$\mathrm{Aut}(B)/\mathrm{Inn}(B)$ is solvable (Schreier's Conjecture) and "small".

We can extend the kernel, like in the example we had:
$A = \{(a, a) | a \in A_5\} < A_5 \times A_5 < S_5 \times A_5$.

Lemma (Aschbacher) If $\beta : T \to \mathrm{Aut}(B)$ extends $\alpha : A \to \mathrm{Aut}(B)$, then $\mathrm{Ker}\,\beta$ uniquely determines β.

Signalizer lattices (2)

So instead of talking about extensions of α, we can talk about pairs (T, K) with

- $A \leq T \leq H$,
- $K \lhd T$,
- $K \cap A = \operatorname{Ker} \alpha$, and
- T/K isomorphic to a subgroup of $\operatorname{Aut}(B)$.

Take the reverse order of these pairs
$(T_1, K_1) \leq (T_2, K_2) \iff T_1 \geq T_2$ and $K_1 \geq K_2$
$(T_2 \cap K_1 = K_2$

Signalizer lattices (2)

So instead of talking about extensions of α, we can talk about pairs (T, K) with

- $A \leq T \leq H$,
- $K \lhd T$,
- $K \cap A = \operatorname{Ker} \alpha$, and
- T/K isomorphic to a subgroup of $\operatorname{Aut}(B)$.

Take the reverse order of these pairs
$(T_1, K_1) \leq (T_2, K_2) \iff T_1 \geq T_2$ and $K_1 \geq K_2$
($T_2 \cap K_1 = K_2$ follows automatically)
and add a smallest element.

This is called a **signalizer lattice** by Aschbacher.

Proof of the Lemma

Lemma (Aschbacher) If $\beta : T \to \mathrm{Aut}(B)$ extends $\alpha : A \to \mathrm{Aut}(B)$, then $\mathrm{Ker}\,\beta$ uniquely determines β.

Proof. Let K be the kernel, then β gives an embedding of T/K into $\mathrm{Aut}(B)$ that extends a fixed embedding of $A/(A \cap K)$. If we have two β's with the same kernel K, then there is an isomorphism between two subgroups of $\mathrm{Aut}(B)$ which is the identity on $\mathrm{Inn}(B)$. Let $\sigma \mapsto \sigma'$ denote this isomorphism, and let ι_b be the conjugation by $b \in B$ (an inner automorphism). Then

$$\iota_{b^\sigma} = \sigma^{-1}\iota_b\sigma \mapsto (\sigma')^{-1}\iota'_b\sigma' = (\sigma')^{-1}\iota_b\sigma' = \iota_{b^{\sigma'}},$$

so $b^\sigma = b^{\sigma'}$ for all $b \in B$, thus $\sigma = \sigma'$.

The kernel

Excercise. Determine the kernel of the action of the twisted wreath product HU on U.

The stabilizer of $1 \in U$ is H, so we have to find

$$\{h \in H \mid \forall u \in U : u^h = u\}.$$

Rewrite: $\forall u \in U, \forall x \in H : u(hx) = u(x)$.

$u(x)$ determines the values of u on xA, the other values are independent of $u(x)$, hence $hx \in xA$, $hx = xa$ for some $a \in A$.

Then $u(x) = u(hx) = u(xa) = u(x)^a$, so $x^{-1}hx = a \in \operatorname{Ker}\alpha$ for all $x \in H$.

Therefore the kernel of the action of G on U is

$$\bigcap_{x \in H} x(\operatorname{Ker}\alpha)x^{-1},$$

the core of $\operatorname{Ker}\alpha$ in H.

M_n (1)

M_n is the (modular) lattice consisting of a smallest, a largest, and n pairwise incomparable elements.
Except for the three papers, most work have been devoted to the study of representing M_n's.
Over the finite field of q elements the 2-dimensional vector space has congruence lattice M_{q+1}, and here q is a prime-power. So we have finite representations of M_n with
$n = q + 1 = 3, 4, 5, 6, 8, 9, 10, 12, \ldots$.
For the smallest missing cases Feit (1983) found the following examples:
$\mathrm{Int}(31 \cdot 5, A_{31}) \cong M_7$ and $\mathrm{Int}(31 \cdot 3, A_{31}) \cong M_{11}$.
These cannot be generalized:
Theorem (Basile, 2001) If $\mathrm{Int}(H; A_d)$ or $\mathrm{Int}(H; S_d) \cong M_n$, then either $n \leq 3$ or one of the following holds:
$(n, d) = (5, 13), (7, 31), (11, 31)$.

M_n (2)

A series of examples was found by Lucchini (1994): M_n is finitely representable if

$$n = q + 2 \quad \text{or} \quad n = \frac{q^t + 1}{q + 1} + 1,$$

where q is a prime-power and t is an odd prime, so
$n = q + 2 = 4, 5, 6, 7, 9, 10, 11, 13, \ldots,$
$n = q^2 - q + 2 = 4, 8, 14, 22, 44, \ldots,$
$n = q^4 - q^3 + q^2 - q + 2 = 12, 62, \ldots,$ etc.
The remaining cases ($n = 16, 23, 35, \ldots$) are still open.
Baddeley–Lucchini 100-page paper (1997): reduction to questions about almost simple groups.
For example:
Problem. Describe all pairs (S, A), where S is a nonabelian simple group, $A \leq \mathrm{Aut}(S)$ such that there is exactly one proper nontrivial A-invariant subgroup of S.

The finite congruence lattice problem
3. Some constructions

Péter P. Pálfy
Alfréd Rényi Institute of Mathematics,
Hungarian Academy of Sciences
and
Eötvös University, Budapest

Summer School on General Algebra and Ordered Sets
Stará Lesná, September 10, 2009

Partition lattices

Obviously, the **partition lattice** $\mathrm{Part}(k)$ (the lattice of all equivalence relations on a k-element set) is a congruence lattice.

It is also an interval in a subgroup lattice, for example

$$\mathrm{Int}(S_1 \times S_2 \times S_4 \times \cdots \times S_{2^{k-1}}; S_{2^k-1}) \cong \mathrm{Part}(k).$$

Lemma. Let S be a finite nonabelian simple group, and $D = \{(s, s, \ldots, s) | s \in S\}$ the diagonal subgroup in S^k. Then $\mathrm{Int}(D; S^k)$ is the dual of $\mathrm{Part}(k)$.

Proof. Every subgroup $D \leq X \leq S^k$ is a subdirect power of the form $\{(s_{i(1)}^{\alpha_1}, s_{i(2)}^{\alpha_2}, \ldots, s_{i(k)}^{\alpha_k}) | s_1, \ldots, s_m \in S\}$, where $i : \{1, \ldots, k\} \to \{1, \ldots, m\}$ and $\alpha_1, \ldots, \alpha_k \in \mathrm{Aut}(S)$. Since $D \leq X$, all automorphisms can be taken to the identity. For example $X = \{(s_1, s_2, s_1, s_1, s_3, s_2) | s_1, s_2, s_3 \in S\}$. So X is determined by the kernel of the mapping i. The larger the kernel of i is, the smaller is the corresponding subgroup.

The dual lattice

Theorem (Kurzweil, 1985; Netter)
The dual of a finitely representable lattice is also finitely representable.

Proof. Let $L \cong \mathrm{Con}(U; F)$ for a unary algebra $(U; F)$. Take any finite nonabelian simple group S.

Take the permutation group (unary algebra) $(S^U : D; S^U)$, its congruence lattice is the dual of $\mathrm{Part}(U)$.

The elements of S^U are functions $U \to S$, the elements of the diagonal subgroup D are the constant functions.

The operations $f \in F$, $f : U \to U$ give rise to operations on S^U simply by composition: if $g : U \to S$, then $f(g) : U \to S$ is defined by $(f(g))(u) = g(f(u))$.

If we multiply g by a constant, then $f(g)$ will be multiplied by the same constant, therefore f can be defined on $S^U : D$ as well.

A congruence of $(S^U : D; S^U)$ remains a congruence of the algebra $(S^U : D; S^U \cup F)$ iff it corresponds to a partition invariant under all $f \in F$, that is, iff it is a congruence of $(U; F)$.

Intervals and sublattices

If $\vartheta \in \mathrm{Con}(U; F)$, then $\mathrm{Con}(U/\vartheta; F) \cong \mathrm{Int}(\vartheta; 1)$, so a filter in the congruence lattice is again a congruence lattice.

The theorem about the representation of the dual lattice then yields:
Corollary. Every interval is a finitely representable lattice is also finitely representable.
John Snow (2000) gave a direct proof.

Is every sublattice of a finitely representable lattice also finitely representable?
Theorem (Pudlák and Tůma, 1980)
Every finite lattice can be embedded into a suitable finite partition lattice.

HSP

Is every homomorphic image of a finitely representable lattice also finitely representable?

Lemma (P^5, 1980) Let $e \in \mathrm{Pol}_1(U; F)$ be an idempotent function ($e^2 = e$), then the restriction is a lattice homomorphism of $\mathrm{Con}(U; F)$ onto $\mathrm{Con}(e(U); eF)$ (the **induced algebra**).

Lemma. The direct product of finitely representable lattices is also finitely representable.
Proof. Take the product of transformation monoids containing all constants, then
$\mathrm{Con}(U_1 \times U_2; F_1 \times F_2) = \mathrm{Con}(U_1; F_1) \times \mathrm{Con}(U_2; F_2)$.
Here $(f_1, f_2)(u_1, u_2) = (f_1(u_1), f_2(u_2))$.

Snowmobile-1

Lemma 1 (Snow, 2000) Let $\alpha, \beta \in \mathrm{Con}(U; F)$. Then we can find additional operations F^* so that

$$\mathrm{Con}(U; F \cup F^*) = \{\gamma \in \mathrm{Con}(U; F) | \gamma \leq \alpha \,\mathrm{or}\, \gamma \geq \beta\}.$$

Proof. Let F^* consist of those unary operations whose kernel contains α and the image lies in one β-class.
If $\alpha \geq \gamma \in \mathrm{Con}(U; F)$, $f^* \in F^*$ and $(u, v) \in \gamma \leq \alpha$, then $f^*(u) = f^*(v)$, so f^* preserves γ.
If $\beta \leq \gamma \in \mathrm{Con}(U; F)$, $f^* \in F^*$ (and $(u, v) \in \gamma$), then $f^*(u)$ and $f^*(v)$ lie in the same β-class, so in the same γ-class, hence f^* preserves γ.
If $\gamma \in \mathrm{Con}(U; F)$ is such that $\alpha \not\geq \gamma$ and $\beta \not\leq \gamma$, then choose $(u, v) \in \gamma \setminus \alpha$ and $(u', v') \in \beta \setminus \gamma$. Let f^* take the value u' on the α-class of u and v' everywhere else. Then $f^* \in F^*$, $(u, v) \in \gamma$, but $(f^*(u), f^*(v)) = (u', v') \notin \gamma$.

Snowmobile-2

Lemma 2 (Snow) Let $\beta_1 \leq \alpha_1$, $\beta_2 \leq \alpha_2$ be congruences of $(U; F)$ such that $\beta_1 \vee \beta_2 = 1$ and $\alpha_1 \wedge \alpha_2 = 0$. Then we can find additional operations F^* so that

$$\mathrm{Con}(U; F \cup F^*) = \{0\} \cup \mathrm{Int}(\beta_1; \alpha_1) \cup \mathrm{Int}(\beta_2; \alpha_2) \cup \{1\}.$$

Proof. Take the additional operations provided by Lemma 1 both for the pair β_1, α_2 and for β_2, α_1. Then the congruences that remain are those which lie

(above β_1 or below α_2) and (above β_2 or below α_1),

that is

$$\gamma \geq \beta_1 \vee \beta_2 \text{ or } \beta_1 \leq \gamma \leq \alpha_1 \text{ or } \beta_2 \leq \gamma \leq \alpha_2 \text{ or } \gamma \leq \alpha_1 \wedge \alpha_2.$$

More Snow (1)

Theorem (Snow, 2000) The ordinal sum and the parallel sum of two finitely representable lattices are also finitely representable.

Proof. The **ordinal sum** of L_1 and L_2 is their disjoint union, where every element of L_1 is smaller than each element of L_2. A somewhat more natural version of the ordinal sum of two lattices is obtained from the usual ordinal sum if we identify the largest element of L_1 with the smallest element of L_2.
This construct will be denoted by $L_1 + L_2$.
(A noncommutative—but associative—addition!)
The usual ordinal sum of L_1 and L_2 is just $L_1 + \mathbf{2} + L_2$.
Now take a finite algebra with conguence lattice $L_1 \times L_2$ and use Snowmobile-1 with $\alpha = \beta = (1, 0)$. Then we obtain a finite algebra with congruence lattice $L_1 + L_2$.

More Snow (2)

The **parallel sum** of L_1 and L_2 is the disjoint union

$$\{0\} \cup L_1 \cup L_2 \cup \{1\},$$

where the elements of L_1 and L_2 are pairwise incomparable.
First we prove the claim when L_2 is the 1-element lattice, and we will denote the parallel sum of L and the 1-element lattice by L^+. (It has three additional elements: $0 < m < 1$.)
Let $\mathrm{Con}(U; F) \cong L$. Take the algebra $(U \times \{1, 2\}; F)$, where $f(u, i) = (f(u), i)$. Use Snowmobile-2 with the following congruences: α_1 has two classes $U \times \{1\}$ and $U \times \{2\}$, β_1 has one nonsingleton class $U \times \{1\}$, $\alpha_2 = \beta_2$ has 2-element classes $\{(u, 1), (u, 2)\}$.
So we obtain an algebra with congruence lattice isomorphic to L^+.
In general, the parallel sum of L_1 and L_2 can be obtained using Snowmobile-2 in the congruence lattice $L_1^+ \times L_2^+$ with $\alpha_1 = (1_1, m)$, $\beta_1 = (0_1, m)$, $\alpha_2 = (m, 1_2)$, $\beta_2 = (m, 0_2)$.

Some classes of finitely representable lattices

Definition A finite(ly generated) lattice L is **lower bounded** if there exists an epimorphism $\varphi : FL(X) \to L$ such that $\forall a \in L : \{w \in FL(X) | \varphi(w) \geq a\}$ has a least element.

Theorem. A finite lattice L is lower bounded iff L and $\mathrm{Con}(L)$ has the same number of join irreducible elements.

Theorem (Pudlák and Tůma, 1976)
The finite lower bounded lattices are finitely representable.
(They called these lattices **finitely fermentable**.)

Theorem (Snow, 2000) Every finite lattice which contains no three element antichains is finitely representable.

Theorem (Snow, 2003) Every finite lattice in the variety generated by M_3 is finitely representable.

Hereditary congruence lattices

The idea of Snow's proof is this:
If L is a finite lattice in the variety generated by M_3, then L is a 0–1-sublattice of M_3^k for some k. $M_3 \cong \mathrm{Part}(3)$, so L can be considered as a 0–1-sublattice of $\mathrm{Part}(3)^k \subset \mathrm{Part}(3^k)$. He then proves that every 0–1-sublattice of $\mathrm{Part}(3)^k$ is the congruence lattice of some algebra on the 3^k-element set.

Definition (Hegedűs and P^3, 2005) A 0–1-sublattice L of all equivalence relations on a finite set U is called a **hereditary congruence lattice** if every 0–1-sublattice $L' \subseteq L$ is the congruence lattice of a suitable algebra on U. Furthermore, L is called **power-hereditary** if L^k as a lattice of equivalence relations on U^k is a hereditary congruence lattice for every $k \geq 1$.

In this language Snow's result says that the lattice of all equivalences on the 3-element set is power-hereditary.

Snakes

$\mathrm{Con}(Z_2 \times Z_2)$ ($\cong M_3$) is also power-hereditary (Hegedűs and P^3), but there are non-power-hereditary representations of M_3 as well (P^3, 2006).

Problem. Is there a hereditary congruence lattice isomorphic to M_4? That is $\mathrm{Con}(U; F) \cong M_4$ and for every nontrivial congruence ϑ_i ($i = 1, \ldots, 4$) there is a unary function f_i^* such that $\mathrm{Con}(U, F \cup \{f_i^*\}) = \mathrm{Con}(U; F) \setminus \{\vartheta_i\}$.

A **snake** of length $n \geq 2$ is a modular lattice glued together from $n - 1$ M_3's.

Theorem (Hegedűs and P^3, 2005) Every finite lattice in the variety generated by all snakes is finitely representable.

We construct operator groups $(A; +, F)$, where $(A; +)$ is an elementary abelian 2-group and F is a suitable ring of endomorphisms of $(A; +)$.