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!