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., $\bigcap_{g \in G} g^{-1}Hg = 1$.

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

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

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

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

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 $x^{-1}hx = a \in \mathrm{Ker}\,\alpha$ for all $x \in H$.

Therefore the kernel of the action of G on U is

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

the core of $\mathrm{Ker}\,\alpha$ 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.