Quick course in Universal Algebra and Tame Congruence Theory

Ross Willard

University of Waterloo, Canada

Workshop on Universal Algebra and the Constraint Satisfaction Problem

Nashville, June 2007

(with revisions added after the presentation)

Outline

0. Apology

PART I: Basic universal algebra

1. Algebras, term operations, varieties
2. Congruences
3. Classifying algebras by congruence properties
4. The abelian/nonabelian dichotomy

PART II: Tame congruence theory

5. Polynomial subreducts
6. Minimal sets and traces (of a minimal congruence)
7. The 5-fold classification and types
8. Classifying algebras by the types their varieties omit

1. Algebras, term operations, varieties

An algebra: $\mathbf{A} = (A;\, F)$
$= (\textit{universe};\, \{\textit{fundamental operations}\})$

term: any formal expression built from [names for] the fundamental operations and variables

terms in n variables define n-ary **term operations** of $\mathbf{A}$.

Definition

The **clone of A** is $\mathrm{Clo}(\mathbf{A}) = \{\text{all term operations of } \mathbf{A}\} = \langle F \rangle$.

$\mathrm{Clo}(\mathbf{A})$ is the fundamental invariant of $\mathbf{A}$.

Definition

$\mathbf{A}, \mathbf{B}$ are **term-equivalent** if they have the same universe and same term functions.

Definition

- $f : A^n \to A$ is **idempotent** if $f(x, x, \dots, x) = x \quad \forall x \in A$.
- $\mathbf{A} = (A, F)$ is **idempotent** if every $f \in F$ (equivalently, $f \in \langle F \rangle$) is idempotent.

CSP'ers care only about idempotent algebras.

This tutorial is **not** specifically focussed on idempotent algebras.

Oh well.

Varieties

Definition

A class of algebras is

- **equational** if it can be axiomatized by **identities**, i.e. (universally quantified) equations between terms.
- a **variety** if it is closed under forming homomorphic images (**H**), subalgebras (**S**), and products (**P**).

Basic theorems

1. (G. Birkhoff) Varieties = equational classes.
2. (Tarski) The smallest variety $\mathrm{var}(\mathcal{K})$ containing $\mathcal{K}$ is $\mathrm{var}(\mathcal{K}) = \mathbf{HSP}(\mathcal{K})$.

$\mathrm{var}(\mathbf{A})$, the *variety generated by* **A**, is another useful invariant of **A**.

2. Congruences

Suppose $\mathbf{A}, \mathbf{B}$ are algebras "in the same language" and $\sigma : \mathbf{A} \to \mathbf{B}$ is a homomorphism.

[Picture]

The pre-images of σ partition A.

Definition

- $\ker(\sigma)$ = the equivalence relation on A given by this partition.
- **congruence** of $\mathbf{A}$: any kernel of a homomorphism with domain $\mathbf{A}$.

Alternatively: congruences of $\mathbf{A}$ are the equivalence relations θ on A which

- Are compatible with F ($\forall f \in F$, $a \stackrel{\theta}{\sim} a' \Rightarrow f(a, b, \ldots) \stackrel{\theta}{\sim} f(a', b, \ldots)$, etc.)
- Support a natural construction of $\mathbf{A}/\theta$ on the θ-classes.

Definition

$\mathrm{Con}(\mathbf{A}) = \{$set of all congruences of $\mathbf{A}\}$.

$(\mathrm{Con}(\mathbf{A}), \subseteq)$ is a poset with top $= A^2$ and bottom $= \{(a,a) : a \in A\}$ ...

[Picture]

...and is a **lattice**: any two θ, φ have a g.l.b. (**meet**) and a l.u.b. (**join**):

$$\begin{aligned} \theta \wedge \varphi &= \theta \cap \varphi \\ \theta \vee \varphi &= \text{transitive closure of } \theta \cup \varphi \\ &= \{\text{all } (a,b) \text{ connected by alternating } \theta, \varphi\text{-paths}\}. \end{aligned}$$

$(\mathrm{Con}(\mathbf{A}); \wedge, \vee)$ is a surprisingly useful invariant of $\mathbf{A}$.

3. Classifying algebras by congruence properties

Distributive law (for lattices): $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ and dually.

Modular law: distributive law restricted to non-antichain triples (x, y, z).

Definitiion

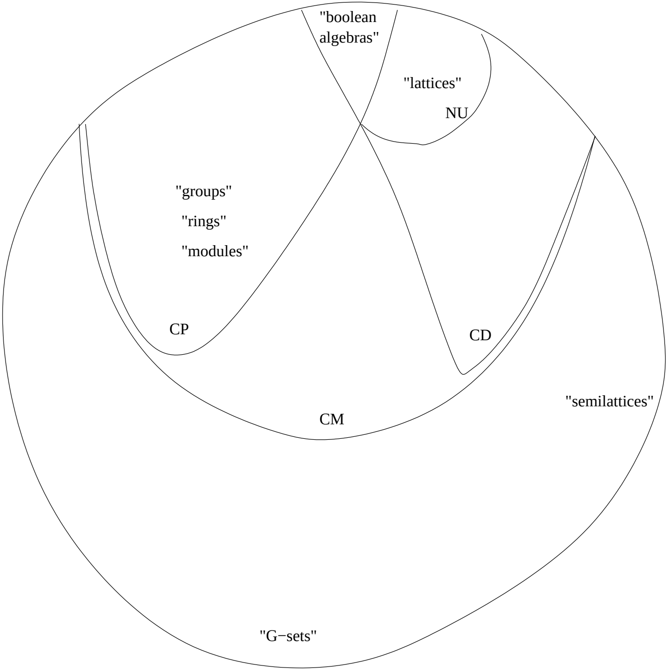
Say **A** is		if $\mathrm{Con}(\mathbf{A})$
congruence distributive	(CD)	is distributive
congruence modular	(CM)	is modular
congruence permutable	(CP)	satisfies $x \circ y = y \circ x$

First approx. to $\theta \vee \varphi$:

$$\theta \circ \varphi \stackrel{def}{=} \{(a, c) : \exists b,\ a \stackrel{\theta}{\sim} b \stackrel{\varphi}{\sim} c\}.$$

Fact: For an algebra **A**, TFAE and imply CM:

- $\theta \vee \varphi = \theta \circ \varphi \quad \forall \theta, \varphi \in \mathrm{Con}(\mathbf{A})$.
- $\theta \circ \varphi = \varphi \circ \theta \quad \forall \theta, \varphi \in \mathrm{Con}(\mathbf{A})$.


"boolean
algebras"
"lattices"
NU
"groups"
"rings"
"modules"
CP
CD
CM
"semilattices"
"G−sets"

A connection: existence of term operations satisfying certain identities $\Leftrightarrow$ congruence lattice properties. For example:

Definition

Let $m(x, y, z)$ be a 3-ary term for **A**.

- m is a **majority** (or **3-NU**) term for **A** if

$$\mathbf{A} \models m(x, x, y) \approx m(x, y, x) \approx m(y, x, x) \approx x.$$

- m is a **Mal'tsev** term for **A** if

$$\mathbf{A} \models m(x, x, y) \approx m(y, x, x) \approx y.$$

Examples

- Using lattice ops, $m(x, y, z) := (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$ is 3-NU.
- Using group ops, $m(x, y, z) := x \cdot y^{-1} \cdot z$ (or $x - y + z$) is Mal'tsev.

Theorem

- $\mathbf{A}$ has a 3-NU term $\Rightarrow$ every $\mathbf{B} \in \mathrm{var}(\mathbf{A})$ is CD.
- $\mathbf{A}$ has a Mal'tsev term $\Leftrightarrow$ every $\mathbf{B} \in \mathrm{var}(\mathbf{A})$ is CP.

Proof of 2nd item (Mal'tsev term $\Leftrightarrow$ $\mathrm{var}(\mathbf{A})$ is CP).

($\Rightarrow$). Let $m(x, y, z)$ be a Mal'tsev term for $\mathbf{A}$. Let $\mathbf{B} \in \mathrm{var}(\mathbf{A})$ and $\theta, \varphi \in \mathrm{Con}(\mathbf{B})$. It suffices to show $\theta \circ \varphi \subseteq \varphi \circ \theta$. Assume $(a, c) \in \theta \circ \varphi$, say $a \overset{\theta}{\sim} b \overset{\varphi}{\sim} c$.

m is also a Mal'tsev term for $\mathbf{B}$, so

$$a = m(a, c, c) \overset{\varphi}{\sim} m(a, b, c) \overset{\theta}{\sim} m(a, a, c) = c$$

witnessing $(a, c) \in \varphi \circ \theta$.

Key: $m(x, y, z)$ gives a **uniform witness** to $\theta \circ \varphi \subseteq \varphi \circ \theta$.

($\Leftarrow$). We construct a generic instance of $\theta \circ \varphi \overset{?}{\subseteq} \varphi \circ \theta$ in $\mathrm{var}(\mathbf{A})$.

Let $\mathbf{B} = \mathbb{F}_{\mathrm{var}(\mathbf{A})}(x, y, z) \in \mathrm{var}(\mathbf{A})$, the free $\mathrm{var}(\mathbf{A})$-algebra of rank 3
$\theta =$ the smallest congruence of $\mathbf{B}$ containing (x, y)
$\varphi =$ the smallest congruence of $\mathbf{B}$ containing (y, z).

Clearly $x \overset{\theta}{\sim} y \overset{\varphi}{\sim} z$, so $(x, z) \in \theta \circ \varphi$.

Assuming $\mathrm{var}(\mathbf{A})$ is CP, then $(x, z) \in \varphi \circ \theta$.

Choose a witness $m \in B$, so $x \overset{\varphi}{\sim} m \overset{\theta}{\sim} z$.

m "is" a term.

$(x, m) \in \varphi$ implies $\mathrm{var}(\mathbf{A}) \models x \approx m(x, z, z)$

$(m, z) \in \theta$ implies $\mathrm{var}(\mathbf{A}) \models m(x, x, z) \approx z$.

Commentary on 1st item (3-NU term $\Rightarrow$ every $\mathrm{var}(\mathbf{A})$ is CD).

Theorem (B. Jónsson)

Given **A**, TFAE:

- $\mathrm{var}(\mathbf{A})$ is CD.
- Every $\mathrm{Con}(\mathbf{B}) \models \alpha \cap (\beta \circ \gamma) \subseteq (\alpha \cap \beta) \vee (\alpha \cap \gamma)$
- $\exists k$ such that every $\mathrm{Con}(\mathbf{B}) \models$

$$\alpha \cap (\beta \circ \gamma) \subseteq \underbrace{(\alpha \cap \beta) \circ (\alpha \cap \gamma) \circ (\alpha \cap \beta) \circ \cdots \circ (\alpha \cap [\beta|\gamma])}_{k}$$

Call the displayed condition $\mathrm{CD}(k)$.

Exercise

$\mathrm{var}(\mathbf{A}) \models \mathrm{CD}(2) \Leftrightarrow$ **A** has a 3-NU term.

Remark: $\mathrm{CD}(3)$ is witnessed by a pair of 3-ary terms, etc. (Called *Jónsson* terms)

4. The abelian/nonabelian dichotomy

Definition

An algebra $\mathbf{A}$ is **abelian** if the diagonal $0_A := \{(a, a) : a \in A\}$ is a block of some congruence of $\mathbf{A}^2$.

Equivalently, if for all term operations $f(\bar{x}, \bar{y})$,

$$\forall \bar{a}, \bar{b}, \bar{c}, \bar{d} : f(\bar{a}, \bar{c}) = f(\bar{a}, \bar{d}) \rightarrow f(\bar{b}, \bar{c}) = f(\bar{b}, \bar{d}). \qquad (*)$$

Examples: abelian groups; R-modules; G-sets.

Non-examples: nonabelian groups; anything with a semilattice operation.

By restricting the quantifiers in $(*)$, can define notion of a *congruence* being abelian; or of one congruence **centralizing** another. Leads to notions of solvability, nilpotency.

Nicest setting: in CM varieties.

- Abelian algebras (and congruences) are *affine* (see below).

Definition

A is **affine** if (i) **A** has a Mal'tsev term $m(x, y, z)$, and (ii) all fundamental operations commute with $m(x, y, z)$.

Equivalently, if there is a ring R, an R-module ${}_RM$ with universe A, and a submodule $U \leq {}_RR \times {}_RM$ such that

$$\text{Clo}\,\mathbf{A} = \text{all} \sum_{i=1}^{n} r_i x_i + a \quad (r_i \in R,\ a \in A)$$

$$\text{for which } \left(1 - \sum_{i=1}^{n} r_i,\ a\right) \in U.$$

(In which case $m(x, y, z) = x - y + z$.)
(Idempotent case: $U = \{(0, 0)\}$.)

Still in CM varieties:

- Centralizer relation on congruences is understood.
- Abelian-free intervals in $\mathrm{Con}(\mathbf{A})$ correspond to structure "similar to" that in CD varieties.
- Thus we get positive information on either side of the abelian/nonabelian dichotomy.
- Example (Freese, McKenzie, 1981): Let $\mathbf{A}$ be a finite algebra in a CM variety. Whether or not $\mathrm{var}(\mathbf{A})$ is residually finite can be characterized by centralizer facts in $\mathbf{HS}(\mathbf{A})$.

PART II: Tame Congruence Theory

5. Polynomial subreducts
6. Minimal sets and traces (of a minimal congruence)
7. The 5-fold classification and types
8. Classifying algebras by the types their varieties omit

5. Polynomial subreducts

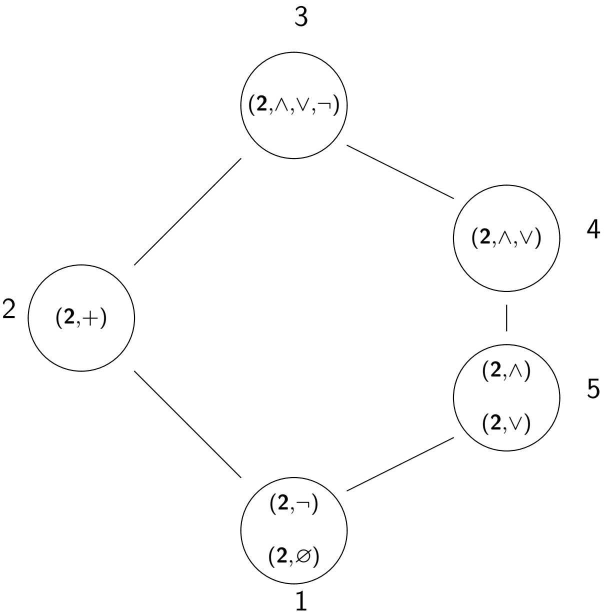
Polynomial operations: like term operations, but allowing parameters.

Definition

Algebras **A**, **B** are **polynomially equivalent** if they have the same universe and the same *polynomial* operations.

- Polynomial equivalence is coarser than term-equivalence.
- Example: on the set $\mathbf{2} := \{0, 1\}$, there are exactly 7 algebras up to polynomial equivalence.

  [picture on next slide]


3
$(\mathbf{2}, \wedge, \vee, \neg)$
4
$(\mathbf{2}, \wedge, \vee)$
2
$(\mathbf{2}, +)$
$(\mathbf{2}, \wedge)$
5
$(\mathbf{2}, \vee)$
$(\mathbf{2}, \neg)$
$(\mathbf{2}, \varnothing)$
1

Strange construction #1.

Definition

Let $\mathbf{A} = (A, \mathcal{F})$ be an algebra and $S \subseteq A$. Form a new algebra with

- universe $= S$
- clone of operations $=$ all $f|_{S^n}$, f an n-ary **polynomial** operation of $\mathbf{A}$ with $f(S^n) \subseteq S$.

This is $\mathbf{A}|_S$, the **polynomial algebra induced on** S (by $\mathbf{A}$).

Toy example

$$\begin{aligned} \mathbf{A} &= \text{1-dimensional vector space over finite field } F = GF(p^n) \\ &= (F;\ \{+,\ (\lambda x)_{\lambda \in F}\}) \end{aligned}$$

Polynomial operations of **A**: all

$$\sum_{i=1}^{n} \lambda_i x_i + a, \quad \lambda_i \in F,\ a \in F$$

Let $S = F^* = F \setminus \{0\}$. Then

Exercise

- Every nonconstant operation of $\mathbf{A}|_S$ depends on exactly one variable.
- $\mathbf{A}|_S$ is term-equivalent to a G-set with all constants, where G is the cyclic group of order $p^n - 1$.

Another toy example

$$\mathbf{A} = (A_4, \cdot), \text{ the alternating group on 4 letters.}$$

Recall: $|A_4| = 12$, and the elements include the 8 permutations of $\{1, 2, 3, 4\}$ which cycle 3 elements, the 3 permutations which match each element with a partner and switch partners, and the identity permutation.

Polynomial operations of $\mathbf{A}$: rather more complicated.

Let $N =$ its 4-element normal subgroup.

Group Theory Exercise

$\mathbf{A}|_N$ is term-equivalent to a 1-dimensional vector space over $GF(4)$ with all constants.

In both examples, the point is that $\mathbf{A}|_S$ is **not** a subalgebra of $\mathbf{A}$, or even of the same type of algebra as $\mathbf{A}$.

6. Minimal sets and traces (of a minimal congruence)

Strange construction #2. Let **A** be a finite algebra.

Definition

- $E(\mathbf{A}) = \{$all unary polynomials $e(x)$ of **A** satisfying $e(e(x)) = e(x)\}$.
- **Neighborhood**: any $e(A)$, $e \in E(\mathbf{A})$.

Let $\alpha \in \mathrm{Con}(\mathbf{A})$ be a **minimal** (nonzero) congruence.

Definition

- $\mathcal{N}_{\mathbf{A}}(\alpha) = \{$those neighborhoods which intersect at least one α-block in ≥ 2 points$\}$.
- α-**minimal set**: any *minimal* member of $\mathcal{N}_{\mathbf{A}}(\alpha)$ (with respect to $\subseteq$).
- α-**trace**: any intersection of an α-minimal set with an α-block, provided the intersection has ≥ 2 points.
- α-**body**: the union of all α-traces in one α-minimal set.

Example: the group A_4. [Picture]

Let N be the 4-element normal subgroup and $\alpha = \theta_N$ the congruence whose classes are the three cosets of N.

Fix an element a of order 3. (So the cosets of N are N, aN, a^2N.)

Consider the following unary polynomials of A_4.

$$e_1(x) = x^4 \qquad U_1 = e_1(A_4)$$
$$e_2(x) = a(a(ax^4)^4)^4 \qquad U_2 = e_2(A_4)$$
$$e_3(x) = a(a^{-1}x)^3 \qquad U_3 = e_3(A_4).$$

$e_1(x) = x$ for all $x \in aN \cup a^2N$ while $e_1(x) = 1$ for $x \in N$. Hence $e_1(e_1(x)) = e_1(x)$ and $U_1 = \{1\} \cup aN \cup a^2N$ is a neighborhood.

e_2 maps N to 1, aN to a and a^2N to a^2. Hence $e_2(e_2(x)) = e_2(x)$ and $U_2 = \{1, a, a^2\}$ is a neighborhood. (In fact, every transversal of the cosets of N is a neighborhood.)

Example (continued)

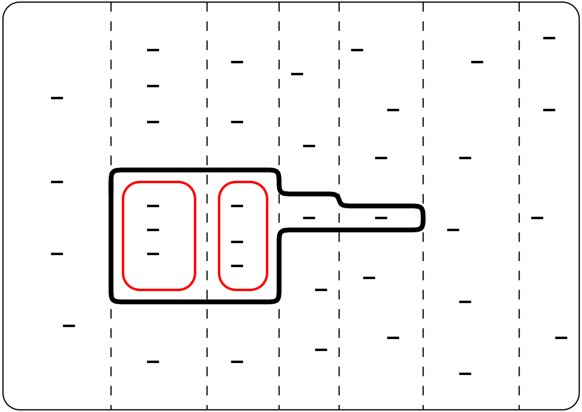
$e_3(x) = x$ for $x \in aN$ while $e_3(x) = a$ for $x \in N \cup a^2N$. Hence $e_3(e_3(x)) = e_3(x)$ and $U_3 = aN$ is a neighborhood.

$U_2 \notin \mathcal{N}_{\mathbf{A}}(\alpha)$ since U_2 does not meet any α-class nontrivially. $U_1 \in \mathcal{N}_{\mathbf{A}}(\alpha)$ but U_1 is not an α-minimal set because $U_3 \in \mathcal{N}_{\mathbf{A}}(\alpha)$ and $U_3 \subset U_1$. A computer can show that U_3 **is** an α-minimal set. In fact, the cosets of N are precisely the α-minimal sets.

Since each α-minimal set in this example is contained entirely inside an α-class, the α-traces and α-bodies are identical to the α-minimal sets, i.e., the cosets of N.

Warning: this is not the typical picture!!

[Typical picture on next page]



This portrays the classes of a minimal congruence α (dashed lines), one α-minimal set (dark black line), and an α-body consisting of two α-traces (red lines). The two points not in the body comprise the **tail**.

7. The 5-fold classification and types

Key step: focus on polynomial algebras induced on α-minimal sets and α-traces.

The latter are catalogued up to polynomial equivalence.

Theorem 1 (P. P. Pálfy)

Let $\mathbf{A}$ be a finite algebra, α a minimal congruence, and N an α-trace. Then the induced polynomial algebra $\mathbf{A}|_N$ is polynomially equivalent to one of:

1. a G-set.
2. a 1-dimensional vector space over a finite field.
3. a 2-element boolean algebra.
4. a 2-element lattice $(L, \{\wedge, \vee\})$.
5. a 2-element semilattice $(S, \vee)$.

Theorem 2

Let **A** be a finite algebra and α a minimal congruence. If N_1, N_2 are any two α-traces, then $\mathbf{A}|_{N_1} \cong \mathbf{A}|_{N_2}$.

Thus we get a 5-fold classification of minimal congruences.

Definition

For α a minimal congruence of **A**, the **type** of α is the common type

- Type 1 (**unary**)
- Type 2 (**vector space**)
- Type 3 (**boolean**)
- Type 4 (**lattice**)
- Type 5 (**semilattice**)

of the polynomial algebras induced on the α-traces of **A**.

Example: The minimal congruence of the group A_4 has "Type 2."

The 5 types reflect 5 distinct "local" structures in an algebra **A**.

In turn, the local structure reflects and is reflected by the global structure of **A**.

The lowest-order tool is:

Theorem 3

Let α be a minimal congruence of **A**.

(Connectedness) Each nontrivial α-block is the union of connected α-traces.

Moreover, **A** has enough unary polynomials to:

(Isomorphism) …map any α-trace isomorphically to any other.

(Density) …map any two distinct elements in an α-block to distinct elements of an α-trace.

Connecting local and global structure

Example:

Theorem

Let α be a minimal congruence of finite $\mathbf{A}$.

- α is abelian $\Leftrightarrow$ the type of α is 1 or 2.
- If α is abelian and $\mathbf{A}$ is idempotent, then each block of α (as a subalgebra of $\mathbf{A}$) is **quasi-affine** (i.e., is a subalgebra of a reduct of a module).

Typing $\mathrm{Con}(\mathbf{A})$

Suppose $\alpha \in \mathrm{Con}(\mathbf{A})$ is **not** minimal. Choose $\delta < \alpha$ so that α is minimal over δ.

[Picture]

Passing to $\mathbf{A}/\delta$, we can assign a type (1–5) to the pair (δ, α).

In this way, a type (1–5) is assigned to each edge of the graph of $\mathrm{Con}(\mathbf{A})$. Much is known.

In applications, one often needs local information about (δ, α) in **A** (not just in $\mathbf{A}/\delta$).

Leads to a refined def. of (δ, α)-minimal sets, traces and bodies ($\subseteq A$).

Polynomial algebras induced on (δ, α)-traces are completely understood in types 3 and 4, largely understood in cases 1, 2 and 5.

Classifying algebras by the types their varieties omit

Definition

Let $\mathbf{A}$ be a finite algebra and $i \in \{1, 2, 3, 4, 5\}$. We say that $\mathrm{var}(\mathbf{A})$

- **admits** type i if type i occurs in $\mathrm{Con}(\mathbf{B})$ for some (finite) $\mathbf{B} \in \mathrm{var}(\mathbf{A})$. (WLOG, $\mathbf{B} \leq \mathbf{A}^n$.)
- **omits** type i otherwise.

Omitting types gives us another way to classify $\mathrm{var}(\mathbf{A})$. For example:

Theorem

For $\mathbf{A}$ finite, TFAE:

- $\mathbf{A}$ has a Taylor term (equivalently, a weak NU-term).
- $\mathrm{var}(\mathbf{A})$ omits type 1.

Similar characterizations (via terms satisfying equations) exist for $\mathrm{var}(\mathbf{A})$ omitting any "down-set" of types (e.g., $\{1, 2\}$, $\{1, 5\}$, etc).

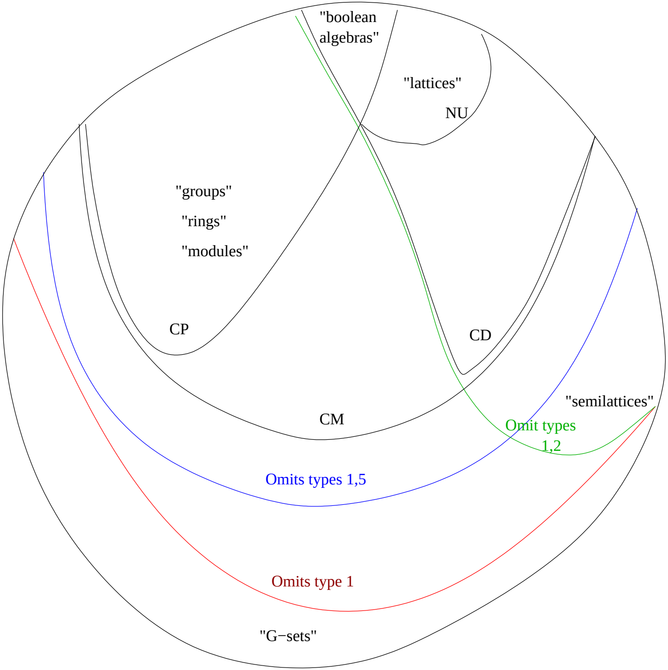
Fitting in the congruence classifications

Theorem

- $\mathrm{var}(\mathbf{A})$ is CM iff $\mathrm{var}(\mathbf{A})$ omits type 1 and 5 and has no tails.
- $\mathrm{var}(\mathbf{A})$ is CD iff $\mathrm{var}(\mathbf{A})$ omits type 1, 2 and 5 and has no tails.

Another relevant class is the class of $\mathbf{A}$ for which $\mathrm{var}(\mathbf{A})$ omits the abelian types 1,2. This class is characterized as those $\mathbf{A}$ for which every $\mathrm{Con}(\mathbf{B})$ satisfies a certain implicational law called SD($\wedge$).

[Big picture on next page]


"boolean
algebras"
"lattices"
NU
"groups"
"rings"
"modules"
CP
CD
CM
"semilattices"
Omit types
1,2
Omits types 1,5
Omits type 1
"G−sets"

Postscript (not included in lecture):

Tame congruence theory reveals how far is the gap between those idempotent **A** for which CSP(**A**) is known to be NP-complete (var(**A**) admits type 1), and those for which CSP(**A**) is known to be in P (CP, NU, bounded width, varieties generated by a finite conservative algebra).

Tame congruence theory suggests intermediate classes of algebras to be explore.

Under weak assumptions (e.g., that var(**A**) omits type 1), the theory yields subtle, positive structural information about all **B** $\in \mathrm{var}$(**A**).

Most importantly, the theory suggests one way to localize, divide and conquer the confusion of "all finite algebras."