How to Spot Polynomial Time Problems for a fixed language $\mathcal{L}$ of algebras

A property $\mathcal{P}$ of $\mathcal{L}$-algebras is **polynomial time** if there is an algorithm and a polynomial $p(x)$ such that, given any $\mathcal{L}$-algebra $\mathbf{A}$, the algorithm determines, within time $p(|A|)$, if $\mathcal{P}$ holds.

First-order properties are polynomial time

Thus testing an algebra for being a

lattice, group, ring, field, etc.

can be done in polynomial time.

(See Freese, Jezek and Nation's **Free Lattices** for a comprehensive discussion of computational aspects of **posets** and **lattices**.)

One can augment the language $\mathcal{L}$ of algebras with relation symbols. This gives polynomial time first-order properties in an expanded language.

<u>S is a **subuniverse** of $\mathbf{A}$</u>
is expressed by:

$$x_1, \ldots, x_n \in S \;\longrightarrow\; f(\vec{x}) \in S \quad \text{for } f \in \mathcal{F}$$

<u>θ is a **congruence** of $\mathbf{A}$</u>
is expressed by:

θ is an equivalence relation on A
$\bigwedge_i (x_i, y_i) \in \theta \;\longrightarrow\; f(\vec{x}, \vec{y}) \in \theta \quad \text{for } f \in \mathcal{F}$

<u>θ, θ' is a **pair of factor congruences** of $\mathbf{A}$</u>
is expressed by:

θ, θ' are congruence relations on A
$\theta \circ \theta' = \nabla$
$\theta \cap \theta' = \Delta$

Polynomial time constructions:

Least Fixpoints of Universal Horn Formulas

A construction that can be expressed as the least fixpoint of a system of Universal Horn formulas can be carried out in polynomial time.

$S = Sg(X)$, the **subuniverse generated by** X is the least fixpoint of

$$\begin{array}{l} x \in X \;\longrightarrow\; x \in S \\ x_1, \ldots, x_n \in S \;\longrightarrow\; f(\vec{x}) \in S \quad \text{for } f \in \mathcal{F} \end{array}$$

$\theta = \Theta(X)$, the **congruence generated by** $X \subseteq A \times A$ is the least fixpoint of

$$\begin{array}{l} (x,y) \in X \;\longrightarrow\; (x,y) \in \theta \\ (x,x) \in \theta \\ (x,y) \in \theta \;\longrightarrow\; (y,x) \in \theta \\ (x,y),(y,z) \in \theta \;\longrightarrow\; (x,z) \in \theta \\ \bigwedge_i (x_i, y_i) \in \theta \;\longrightarrow\; (f\vec{x}, f\vec{y}) \in \theta \quad \text{for } f \in \mathcal{F} \end{array}$$

Fixed point + First-order

The following characterizations are due to Berman and McKenzie

Let $X = \{(a,a,b,b) : a,b \in A\}$
Let $Y = \{(a,b,a,b) : a,b \in A\}$
Let $Z = \{(a,b,c,c) : a,b \in A\}$

$\mathbf{A}$ is **abelian** is expressed by:

$$(x,x,y,z) \in Sg(X \cup Y) \longrightarrow y \approx z$$
$$(x,y,x,z) \in Sg(X \cup Y) \longrightarrow y \approx z$$

$\mathbf{A}$ is **strongly abelian** is expressed by:

$$(x,x,y,z) \in Sg(Y \cup Z) \longrightarrow y \approx z$$

One can find the set of **principal congruences** of $\mathbf{A}$ in polynomial time by applying the previous construction $\binom{|A|}{2}$ times.

One can test an algebra for being **congruence permutable** in polynomial time (by testing the principal congruences).

In 1920 Skolem used simultaneous least fixpoints of universal Horn formulas to give an efficient solution to the **word problem for lattices**.

Finding typesets

Berman, Kiss, Pröhle and Szendrei showed that one can find the **typeset of $\mathbf{A}$** in polynomial time.

McKenzie showed that finding the **typeset of** $V(\mathbf{A})$ is undecidable.

Nondeterministic polynomial time properties

A property $\mathcal{P}$ of $\mathcal{L}$-algebras is NP if there is an algorithm for $\mathcal{P}$ that runs in polynomial time when given a polynomial size (suitable) hint.

Fagin's theorem says that NP properties are precisely those that can be expressed in the form:
$\exists R_1 \cdots \exists R_k \varphi$
where φ is a first-order formula.

θ **is a factor congruence** is NP as one can express this by the $\exists$SO formula

$$\exists \theta' \left(\begin{array}{l} \theta, \theta' \text{ are congruences} \\ \theta \circ \theta' = \nabla \\ \theta \cap \theta' = \Delta \end{array} \right)$$

R. Freese has proved that one can determine if $\mathbf{A}$ is CD in polynomial time.

C. Herrmann has proved that one can determine if $\mathbf{A}$ is CM in polynomial time.

Are the following problems **polynomial time**?

1) θ is a **factor congruence**
2) $\mathbf{A}$ is **directly decomposable**

Are the following problems in **NP**?

3) $\mathbf{A}$ is **directly indecomposable**
4) $V(\mathbf{A})$ is **CP**, **CM**, or **CD**
5) $\mathbf{A}$ is **primal**, or **quasiprimal**

Investigating the power of computers

Everyone knows the **16 groupoids** on the two elements $\{0, 1\}$, namely they are the truth tables for the binary connectives from the propositional logic, e.g.,

$\wedge$	0	1
0	0	0
1	0	1

But not the **19,683 groupoids** on the three elements $\{0, 1, 2\}$.

Actually, there are only **3,330**, up to isomorphism.

A computer study of 3-element groupoids by Berman and Burris in Logic and Algebra, 1996
(Proceedings of the Magari Conference, publ. Marcel Dekker)

A catalog of the 3,330 isomorphism types

Gives the weak isomorphism relation between them (there are 411 equivalence classes)

Analyzes the following 12 properties:

> $\mathbf{A}$ is quasiprimal, affine, strongly abelian,
> abelian, has an invertible binary term,
> has trivial abelian subalgebras,
> is simple, is rigid
> $V(\mathbf{A})$ is decidable, CD, CM, CP

and gives

> typeset($\mathbf{A}$), and $|F(n)|$ for $n \leq 2$.

The future for making catalogs

3-element groupoids with a unary operation $(A, +, f)$

about **90,000 isomorphism types**
This looks tractable.

3-element bi-groupoids $(A, +, \times)$

about **65,000,000 isomorphism types**
This does not look feasible.

3-element ternary algebras (A, t)

about 10^{12} **isomorphism types**
Clearly too many.

4-element groupoids $(A, +)$

about **200,000,000 isomorphism types**
This does not look feasible.

The biggest early threat to the success of our catalog was determining if $V(\mathbf{A})$ was CP, i.e., if $\mathbf{A}$ had a Mal'cev term $p(x,y,z)$.

We know of no good algorithm for this, so we resorted to brute force in many cases:

determine if $m \in Sg(X)$, where

$$X = \left\{ \begin{array}{ccccccccccccccc} (0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 0 & 1 & 2) \\ (0 & 0 & 1 & 2 & 0 & 1 & 1 & 2 & 0 & 1 & 2 & 2 & 0 & 1 & 2) \\ (1 & 2 & 1 & 2 & 0 & 0 & 2 & 2 & 0 & 1 & 0 & 1 & 0 & 1 & 2) \end{array} \right\}$$

and

$$m = \begin{array}{ccccccccccccccc} (1 & 2 & 0 & 0 & 1 & 0 & 2 & 1 & 2 & 2 & 0 & 1 & 0 & 1 & 2) \end{array}$$

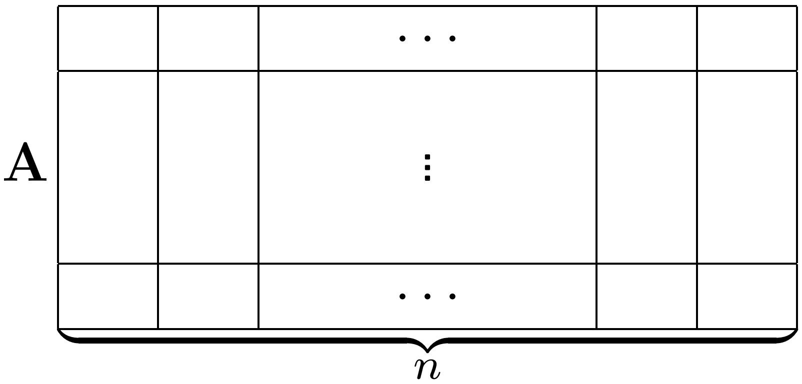
So we needed to generate

$$Sg(X) \subseteq A^{15}$$

This approach falls under the general computational problem studied by Berman and Wolk:

Generate $S(\mathbf{A}, n, X)$

$S(\mathbf{A}, n, X)$ is the subuniverse of $\mathbf{A}^n$ generated by X



In the **worst case** one needs to carry out about

$$n \cdot |A|^{2n}$$

coordinate multiplications to generate $S(\mathbf{A}, n, X)$.

The n **in** $S(\mathbf{A}, n, X)$

for some popular questions

for	n
F(2)	$\lvert A\rvert^2$
Mal'cev term	$2\lvert A\rvert^2 - \lvert A\rvert$
Majority term **CD** **CM**	$3\lvert A\rvert^2 - 2\lvert A\rvert$
F(3)	$\lvert A\rvert^3$

Feasibility Study
Bounds on computational resources

Current Machine	Dream Machine
10^{16} cycles/year	10^{25} cycles/year

Current Machine is single 250 MHz CPU

Dream Machine has 1 million 100 GHz CPU's in parallel

The maximum n in $S(\mathbf{A}, n, X)$
for 1 Year of Computation

	Current	Dream
$\|A\| = 2$	24	38
3	15	24
4	12	19
5	10	17

Analyzing a single groupoid $\mathbf{A}$

Mal'cev term	**size of algebra**	
	3 elements	4 elements
Current	4 mos	10^{20} yrs
Dream	$<$ 1 sec	100 billion years

$V(\mathbf{A})$ **is CD**	**size of algebra**	
	3 elements	4 elements
Current	200,000 years	
Dream	$<$ 1 sec	10^{25} years

size of $\mathbf{F}(3)$	**size of algebra**	
	3 elements	4 elements
Current	100 billion years	
Dream	150 years	

Intractable 4-element Groupoids?

It seems that *there may be* a 4-element groupoid

$\cdot$	0	1	2	3
0	$\star$	$\star$	$\star$	$\star$
1	$\star$	$\star$	$\star$	$\star$
2	$\star$	$\star$	$\star$	$\star$
3	$\star$	$\star$	$\star$	$\star$

with the property that *we have no techniques to determine if it has a Mal'cev term; or a near unanimity term*.

PROBLEM: Is there an **efficient algorithm** to determine if a **4-element groupoid** has a Mal'cev term? a near unanimity term?

The strategy for 3-element groupoids

Brush up on your **C-programming** skills.

Find **isomorphism types**.

Determine some **easy properties**: rigidity, number of 1-element subalgebras, etc.

Find enough tricks to determine which have **Mal'cev terms**.

Determine the **weak isomorphism** relation $\sim$.

Determine the **weak embeding** relation $\leq$.

Determine **other properties**: majority term, Jónsson terms, etc.

Invertible binary terms

A basic tool for simplifying the search for a Mal'cev term is the existence of a
binary term $b(x, y)$, and
two unary terms $u_1(x), u_2(x)$ such that

range(u_i) $\neq A$, and
$b(u_1x, u_2x) \approx x$ holds in $\mathbf{A}$.

Then $\mathbf{A}$ has a Mal'cev term iff each of the ranges of the u_i have a Mal'cev term m_i.

Namely use $m(x, y, z) =$
$b(m_1(u_1x, u_1y, u_1z),\ m_2(u_2x, u_2y, u_2z))$.

This worked for nearly half of the 3 element groupoids.

The properties studied are **invariant under transpose**.

Some known polynomial time properties were quickly analyzed, e.g., rigidity.

Determine which have a Mal'cev term

This was formulated as a question about $S(\mathbf{A}, 15, X)$, namely is $\mathbf{m}$ in the subuniverse generated by $X = \{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ where

$\mathbf{x} =$	0	0	0	0	1	1	1	1	2	2	2	2	0	1	2
$\mathbf{y} =$	0	0	1	2	0	1	1	2	0	1	2	2	0	1	2
$\mathbf{z} =$	1	2	1	2	0	0	2	2	0	1	0	1	0	1	2
$\mathbf{m} =$	1	2	0	0	1	0	2	1	2	2	0	1	0	1	2

Use **projections on few coordinates** to reject many cases

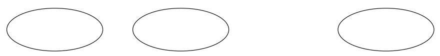
Use **invertible** binary terms to accept many cases

Finally use **full computations** on $S(\mathbf{A}, n, X)$.

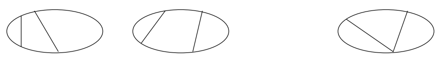
Finding the **weak embedding** preorder $\leq$

First determine when $\mathbf{A} \sim \mathbf{B}$ (weakly isomorphic):

Find an **upper bound** (132 classes) using known properties such as rigidity, Mal'cev, etc.



Find a **lower bound** (440 classes) using time limited attempts with **F(2)**'s



Choose 440 representatives, and use **F(2)**'s to show that

there are 411 equivalence classes

Choose 411 representatives and use **F(2)**'s to determine $\leq$

Applications of $\leq$

Determine all $|F(2)|$ and all $Typeset(\mathbf{A})$

Use the **covers** and **subcovers** of $\leq$

plus **programs** for finding majority terms
Jónsson terms Gumm terms

to analyze the properties

has a **majority term**
$V(\mathbf{A})$ is **congruence distributive**
$V(\mathbf{A})$ is **congruence modular**
has a **near unanimity term**

Conclusions

The partial ordering $\leq$ is a powerful tool to analyze further properties. In particular **Mal'cev conditions** look quite tractable.

The 3-Element Groupoid (#534) has a **4-ary Near Unanimity** term

$\cdot$	0	1	2
0	0	0	1
1	0	2	0
2	1	0	2

$$U(x,y,z,w) = ((x^2y^2)((x^2(x^2y^2))(z^2w^2)^2)) \\ \cdot ((x^3y^3)((x^3(x^3y^3))(z^3w^3)^2))$$

[Paweł Idziak (1994)] A 3-element groupoid has a near unanimity term iff it has a majority term or is equivalent to #534.

Skolem's axioms for the Calculus of Groups

in the relational language $\{J, M, \leq\}$

$x \leq x$

$x \leq y \ , \quad y \leq z \ \longrightarrow \ x \leq z$

$Mxyz \ \longrightarrow \ z \leq x \ , \quad z \leq y$

$Mxyz \ , \quad w \leq x \ , \quad w \leq y \ \longrightarrow \ w \leq z$

$Mxyz \ , \quad x \sim x' \ , \quad y \sim y' \ , \quad z \sim z' \ \longrightarrow \ Mx'y'z'$

$Jxyz \ \longrightarrow \ x \leq z \ , \quad y \leq z$

$Jxyz \ , \quad x \leq w \ , \quad y \leq w \ \longrightarrow \ z \leq w$

$Jxyz \ , \quad x \sim x' \ , \quad y \sim y' \ , \quad z \sim z' \ \longrightarrow \ Jx'y'z'$

$\forall x \forall y \exists z \, Mxyz$

$\forall x \forall y \exists z \, Jxyz$

Let $\mathbf{A} = (A, J, M, \leq)$ be a finite structure.

Let $\leq^\star$ be the **least fixpoint of** $\leq$ under the universal Horn portion of Skolem's axioms.

Then the equivalence relation θ determined by $\leq^\star$ gives the smallest congruence θ such that $\mathbf{A}/\theta$ can be (weakly) embedded in a lattice.

Theorem Let V be a variety of algebras. T.F.A.E.

(a) The uniform word problem for V is solvable in polynomial time.

(b) Given a partial algebra $\mathbf{P}$, one can find the smallest congruence θ such that $\mathbf{P}/\theta$ embeds in a member of V.

Corollary. Skolem had a polynomial time algorithm to solve the word problem for lattices.

How to generalize Skolem's result:

Let V be a variety of algebras.

Let W be the **relational** version of V.

Let $S(W)$ be the class of substructures of W.

Let $S'(W)$ be the class of structures that are **weakly embeddable** in W.

Theorem If K is a finitely axiomatizable universal Horn class with

$$S(W) \subseteq K \subseteq S'(W)$$

then the uniform word problem for V is solvable in polynomial time.