The finite basis problem, Jónsson's speculation, and weird algebras – Part I

Ross Willard

University of Waterloo

BLAST 2017 – Vanderbilt U.
Aug 15, 2017

An **algebra** is a set with some basic operations. $\mathbf{A} = (A, f_1, f_2, \ldots)$.

- Throughout this tutorial, all algebras have finite signature.

A **law** (in some algebraic signature) is a first-order sentence of the form

$$\forall \mathbf{x}\ s(\mathbf{x}) = t(\mathbf{x}) \qquad (s, t \text{ are terms}). \qquad \text{I'll write } s = t.$$

$\mathrm{Laws}(\mathbf{A}) :=$ the set of laws true in $\mathbf{A}$.

- $\mathrm{var}(\mathbf{A}) := \mathrm{Mod}(\mathrm{Laws}(\mathbf{A})) = \mathrm{HSP}(\mathbf{A})$.
- (var = "variety")

Definition

$\mathbf{A}$ is **finitely based** if there exists $\Sigma \subseteq_{\text{fin}} \mathrm{Laws}(\mathbf{A})$ with $\Sigma \vdash \mathrm{Laws}(\mathbf{A})$.

- (Σ is a **basis** for $\mathrm{Laws}(\mathbf{A})$.)

Example – the group $\mathbf{S}_3$

Some laws satisfied by $\mathbf{S}_3$:

- $x^6 = 1$
- $x^2y^2 = y^2x^2$
- $[x, y]^3 = 1$.

(The 3rd is a consequence of the first two.)

Proposition

The group axioms plus $x^6 = 1$ and $x^2y^2 = y^2x^2$ form a basis for Laws($\mathbf{S}_3$).

- Hence $\mathbf{S}_3$ is finitely based.

Proof sketch. Let $\Sigma = \{\text{group axioms}\} \cup \{\, x^6 = 1,\ x^2y^2 = y^2x^2 \,\}$.

Let $\mathbf{G}$ be an arbitrary model of Σ.

- Aim: to prove that $\mathbf{G}$ satisfies <u>all</u> the laws of $\mathbf{S}_3$.

Can assume $\mathbf{G}$ is finitely generated.

Let $\mathbf{H} = \langle a^2 : a \in G \rangle$.

$\mathbf{H} \lhd \mathbf{G}$, and $\mathbf{G}/\mathbf{H}$ is finitely generated and satisfies $x^2 = 1$.

So $\mathbf{G}/\mathbf{H} \ \cong\ (\mathbb{Z}_2)^m$.

So $\mathbf{H}$ has finite index.

By Schreier's Lemma, $\mathbf{H}$ is also finitely generated.

$\mathbf{H}$ is abelian (since generators commute), thus of exponent 3.

So $\mathbf{H} \ \cong\ (\mathbb{Z}_3)^n$, and we've proved <u>$\mathbf{G}$ is finite</u>.

$\mathbf{G}/\mathbf{H} \;\cong\; (\mathbb{Z}_2)^m, \quad \mathbf{H} \;\cong\; (\mathbb{Z}_3)^n, \qquad \text{so } |G| = 2^m\,3^n.$

Let $\mathbf{P}$ be a Sylow 2-subgroup of $\mathbf{G}$. $\quad |P| = 2^m$.

$\mathbf{G}$ is a semidirect product of $\mathbf{H}$ and $\mathbf{P}$:

$$\boxed{\mathbf{G} \;=\; \mathbf{H} \rtimes \mathbf{P} \qquad \mathrm{conj} : \mathbf{P} \to \mathrm{Aut}(\mathbf{H}).}$$

Thus $\mathbf{P} \;\cong\; \mathbf{G}/\mathbf{H} \;\cong\; (\mathbb{Z}_2)^m$.

So $\mathbf{P} \;=\; \ker(\mathrm{conj}) \oplus \mathbf{Q} \quad$ with $\quad \mathrm{conj}{\restriction_Q} : \mathbf{Q} \hookrightarrow \mathrm{Aut}(\mathbf{H})$.

Hence

$$\begin{aligned} \mathbf{G} \;=\; \mathbf{H} \rtimes \mathbf{P} \;&\cong\; \big(\mathbf{H} \rtimes \mathbf{Q}\big) \times \ker(\mathrm{conj}) \\ &\cong\; \big((\mathbb{Z}_3)^n \rtimes \overline{\mathbf{Q}}\big) \times (\mathbb{Z}_2)^{m_0} \end{aligned}$$

for some $\quad \overline{\mathbf{Q}} \;\leq\; GL_n(\mathbb{Z}_3) \quad$ with $\quad \overline{\mathbf{Q}} \;\cong\; (\mathbb{Z}_2)^{m_1}$.

$$\mathbf{G} \;\cong\; ((\mathbb{Z}_3)^n \rtimes \overline{\mathbf{Q}}) \times (\mathbb{Z}_2)^{m_0}, \quad \overline{\mathbf{Q}} \leq GL_n(\mathbb{Z}_3), \quad \overline{\mathbf{Q}} \cong (\mathbb{Z}_2)^{m_1}.$$

Now some linear algebra:

- $(\mathbb{Z}_3)^n$ is a vector space over GF(3).
- $\overline{\mathbf{Q}}$ is a group of commuting linear operators on $(\mathbb{Z}_3)^n$.
- The minimal polynomial of each $L \in \overline{\mathbf{Q}}$ divides $x^2 - 1$.
- Hence $\overline{\mathbf{Q}}$ is simultaneously diagonalizable (over GF(3)).

A basis for $(\mathbb{Z}_3)^n$ diagonalizing $\overline{\mathbf{Q}}$ gives an embedding

$$\begin{aligned}(\mathbb{Z}_3)^n \rtimes \overline{\mathbf{Q}} &\hookrightarrow (\mathbb{Z}_3)^n \rtimes DiagGL_n(\mathbb{Z}_3)\\ &\cong (\mathbb{Z}_3)^n \rtimes \{1,-1\}^n \;\cong\; (\mathbb{Z}_3 \rtimes \{1,-1\})^n \;\cong\; (\mathbf{S}_3)^n.\end{aligned}$$

Hence

$$\mathbf{G} \;\hookrightarrow\; (\mathbf{S}_3)^n \times (\mathbb{Z}_2)^{m_0} \;\hookrightarrow\; (\mathbf{S}_3)^{n+m_0}.$$

Hence $\mathbf{G} \models \mathrm{Laws}(\mathbf{S}_3)$. □

Summary

For a well-chosen finite set $\Sigma \subseteq \text{Laws}(\mathbf{S}_3)$ we:

1. Proved that every finitely generated model of Σ is finite.
   - I.e., $\text{Mod}(\Sigma)$ is **locally finite**.
2. Proved that every finite model of Σ embeds in a power of $\mathbf{S}_3$.
   - I.e., $\text{Mod}_{\text{fin}}(\Sigma) \subseteq \text{SP}(\mathbf{S}_3) \subseteq \text{HSP}(\mathbf{S}_3) = \text{var}(\mathbf{S}_3)$.

This is typical. To prove a finite set $\Sigma \subseteq \text{Laws}(\mathbf{A})$ is a basis:

1. Deduce local finiteness.
2. Use structure theory to put finite models in $\text{HSP}(\mathbf{A})$.

Moral

Finite basis proofs test our structural knowledge of finite algebras.

Which finite algebras are finitely based?

The following are:

1. The 2-element Boolean algebra. (Huntington 1904)
2. Every 2-element algebra. (Lyndon 1951)
3. The group $\mathbf{S}_3$. (B.H. Neumann 1937)
4. Every finite group. (Oates, Powell 1964)
5. Every finite ring. (Kruse 1973; L'vov 1973)
6. Every finite lattice $(L, \wedge, \vee)$. (McKenzie 1972)
7. Every finite lattice expansion $(L, \wedge, \vee, \ldots)$. (Baker 1972–77)
8. Almost every finite algebra. (Murskiĭ 1979)

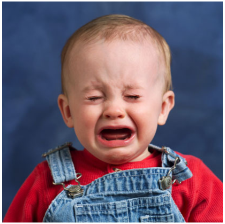
But …

6. Not every finite algebra. (Lyndon 1954)

Problem (Tarski, 1960s)

Is there an algorithm that decides which finite algebras are finitely based?

Answer (McKenzie 1996). No.



Our aim is to find broad classes of finite algebras which we can prove are finitely based.

Bjarni Jónsson, 1920 – 2016

Residual sets

Recall that in proving that $\mathbf{S}_3$ is finitely based, we also proved:

Every member of $\mathrm{var}(\mathbf{S}_3)$ embeds in a power of $\mathbf{S}_3$.

We say that $\mathrm{var}(\mathbf{S}_3)$ is "residually in" $\{\mathbf{S}_3\}$.

Definition

Given an algebra $\mathbf{A}$ and a set $\mathcal{K}$ of algebras, we say that

$$\mathrm{var}(\mathbf{A}) \text{ is } \textbf{residually in } \mathcal{K}$$

if every member of $\mathrm{var}(\mathbf{A})$ embeds in a product of members of $\mathcal{K}$.

The residual bound of $\mathbf{A}$

Definition

Given a finite algebra $\mathbf{A}$,

$\rho(\mathbf{A})$:= the least cardinal λ such that $\exists$ set $\mathcal{K}$ where

1. $\mathrm{var}(\mathbf{A})$ is residually in $\mathcal{K}$, and
2. each $\mathbf{B} \in \mathcal{K}$ has cardinality $< \lambda$.

If no such λ exists, we write $\rho(\mathbf{A}) = \infty$.

Examples

1. $\rho(\mathbf{S}_3) = 7$.
2. $\rho(\mathbf{Q}_8) = \infty$. ($\mathbf{Q}_8$ = the quaternion group.)
3. (Ol'šanskiĭ 1969) If $\mathbf{G}$ is a finite group, then

$$\rho(\mathbf{G}) \text{ is } \begin{cases} < \omega & \text{if every Sylow subgroup of } \mathbf{G} \text{ is abelian} \\ = \infty & \text{otherwise.} \end{cases}$$

Baker's finite basis theorem (1972–77):

> If **A** is a finite lattice expansion $(A, \wedge, \vee, \ldots)$ (or more generally, has "Jónsson terms"), then **A** is finitely based.

Key step (via Jónsson's Lemma):

> $\rho(\mathbf{A}) < \omega$. (Under the same hypothesis)

Jónsson's Speculation (1970s)

Might it generally be true that

$$\rho(\mathbf{A}) < \omega \quad \Rightarrow \quad \mathbf{A} \text{ is finitely based?}$$

Has been confirmed in many cases. But still open!

Tame Congruence Theory (baby version)

Fix a finite algebra **B**, and a minimal congruence relation α on **B**.

The nontrivial α-classes are filled with “babies” (certain small subsets).

These “babies” can come in five “flavors”:

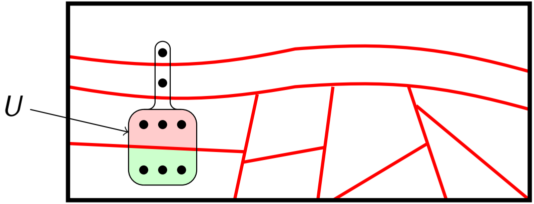
1. trivial
2. vector space
3. boolean algebra
4. lattice order
5. semilattice order

Flavors 2 and 3 are the best.
1 is the worst, followed by 5.

Tails

Also bad: babies with "tails."

B a finite algebra, α a minimal congruence relation.



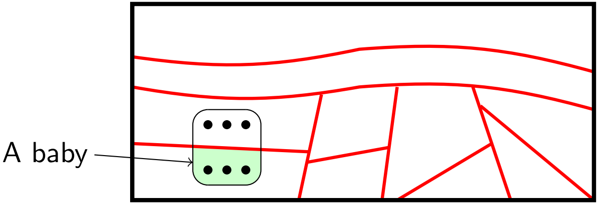
Consider all maps $r : B \to B$ defined by 1-variable **polynomials** (terms with parameters from **B**) which additionally satisfy

- $r(r(x)) = r(x)$ for all $x \in B$.
- $\mathrm{im}(r)$ intersects some α-class nontrivially.

Let r be such a map whose image U is minimal w.r.t. $\subseteq$.

U is not a baby.

- A **baby** (or α-**trace**) is a nontrivial intersection of U with an α-class.
- The trivial intersection(s) form a **tail**.



A baby inherits **flavor** (algebraic structure) from binary polynomials of **B**.

- Palfy's Theorem: there are only 5 flavors.

Example: If **N** is a minimal normal subgroup of a finite group **G**, then

- The babies in the cosets-of-**N** congruence are:

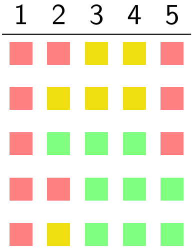
  2. vector spaces (if **N** is abelian)
  3. boolean algebras (if **N** is nonabelian).

- The babies never have tails.

(Groups have "beautiful babies.")

Progress towards proving Jónsson's speculation

The implication $\boxed{\rho(\mathbf{A}) < \omega \Rightarrow \mathbf{A} \text{ is finitely based}}$ is confirmed when:



Baker (1972–77)

McKenzie (1987)

Hobby & McKenzie (1988)

W (2000)

Kearnes, Szendrei & W (2016)

Babies in var($\mathbf{A}$) of a given flavor:

= no babies

= tail-less babies only

= no restriction

TCT flavors:

1: trivial
2: vector space
3: boolean algebra
4: lattice
5: semilattice

A few words on the proofs

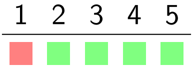
"Extremely intricate" ... "Astonishing" ... "Interesting" ... "This article"

(From the MR of the last result):

> "The proof ... involves analysis of the definability of the 4-ary principal centralizer relation and its repercussions concerning definability in the finite residual bound setting."

What next?

The next obvious goal: the case



Kearnes, Szendrei and I suspect that Jónsson's Speculation has a negative answer in this case.

Cash prize: €87 for the first counter-example!

Thank you