The finite basis problem revisited

Ross Willard

University of Waterloo, CAN

AAA87
Linz, Austria
07.02.2014

My collaborators

Keith Kearnes
University of Colorado

Ágnes Szendrei
University of Colorado
Bolyai Institute, Szeged

Finite bases

The variety of all groups can be defined by the identities

$$x(yz) \approx (xy)z, \quad x1 \approx x \approx 1x, \quad \text{and} \quad xx^{-1} \approx 1.$$

The symmetric group $\mathbf{S}_3$ satisfies these identities and more; e.g.,

$$x^6 \approx 1, \quad (x^{-1}y^{-1}xy)^3 \approx 1, \quad x^2y^2 \approx y^2x^2.$$

Let $\Sigma = \{\text{these seven identities}\}$.

Fact: All identities true in $\mathbf{S}_3$ can be deduced from Σ.

Equivalently, $\mathcal{V}(\mathbf{S}_3)$ is **axiomatized** by Σ.

We say Σ a **basis** (for $\mathbf{S}_3$ or $\mathcal{V}(\mathbf{S}_3)$).

Finitely based algebras

Definition

An algebra **A** is **finitely based** if $\mathcal{V}(\mathbf{A})$ is finitely axiomatizable.

Examples of finitely based algebras:

- Every 2-element algebra in a finite signature (Lyndon, 1951)

(From now on, all algebras are assumed to be in a finite signature.)

- Every finite group (Oates and Powell, 1965)
- Every finite ring (Kruse, L'vov, 1973)
- Every finite commutative semigroup (Perkins, 1969)
- Every finite lattice (McKenzie, 1970)
- Every finite **A** such that $\mathcal{V}(\mathbf{A})$ is congruence distributive (Baker, 1972)

Non-finitely based algebras

Not every finite algebra is finitely based (Lyndon, 1954).

The following 3-element groupoid is **not** finitely based (Murskii, 1965):

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

The following 6-element semigroup is **not** finitely based (Perkins, 1969):

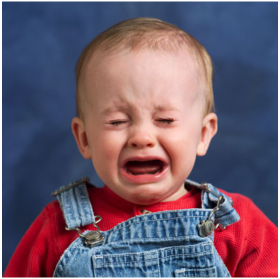
$$\mathbf{B}_2^1 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

The finite basis problem

Which finite algebras are finitely based?

We'll never know.

Theorem (McKenzie, 1996). There is no algorithm which decides, given a finite algebra **A**, whether **A** is finitely based.



However, this is no reason to cry.

Jónsson's Speculation/Park's Conjecture

Baker's Theorem (1972)

$\mathbf{A}$ finite and $\mathcal{V}(\mathbf{A})$ congruence distributive $\Longrightarrow$ $\mathbf{A}$ is finitely based.

$\Downarrow$ key step

$\exists N < \omega$ such that every subdirectly irreducible $\mathbf{S} \in \mathcal{V}(\mathbf{A})$ has $|S| \leq N$.

Def. We say $\mathcal{V}(\mathbf{A})$ "has a finite residual bound" if it satisfies ↗.

Bjarni Jónsson's Question (early 1970s):

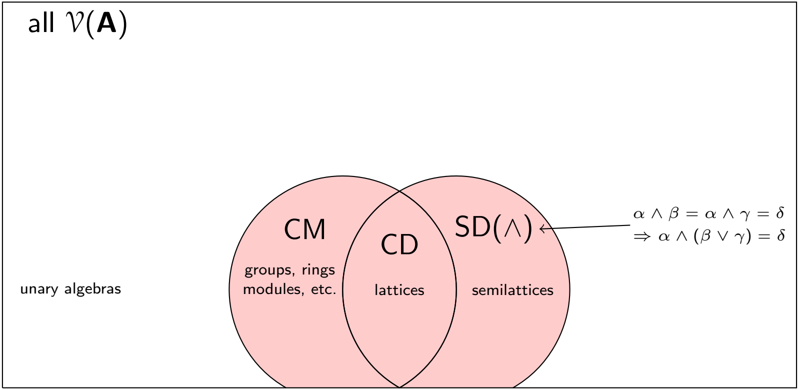
$\mathbf{A}$ finite & $\mathcal{V}(\mathbf{A})$ has a finite residual bound $\overset{?}{\Longrightarrow}$ $\mathbf{A}$ is finitely based.

(Robert Park's conjecture (1976): "YES." Still open!)

Confirmations of Jónsson's Problem/Park's conjecture

The answer for **A** is known to be "YES" if $\mathcal{V}(\mathbf{A})$ is ...

1. ... Congruence distributive (CD) – (Baker, 1972).
2. ... Congruence modular (CM) – (McKenzie, 1987).
3. ... Congruence meet semi-distributive (SD($\wedge$)) – (W, 2000).



How are these theorems proved?

Fix a finite algebra $\mathbf{A}$.

Let $\mathcal{V}^{(n)} :=$ the variety axiomatized by all the $\leq n$-variable identities of $\mathbf{A}$.

Facts:

1. $\mathcal{V}^{(1)} \supseteq \mathcal{V}^{(2)} \supseteq \mathcal{V}^{(3)} \supseteq \cdots \supseteq \mathcal{V}^{(n)} \supseteq \cdots$ and $\bigcap_{n=1}^{\infty} \mathcal{V}^{(n)} = \mathcal{V}(\mathbf{A})$.
2. Each $\mathcal{V}^{(n)}$ is finitely axiomatizable.
3. $\mathbf{A}$ is finitely based $\iff$ $\mathcal{V}(\mathbf{A}) = \mathcal{V}^{(n)}$ for some (hence all large) n.

Definable relations

Definition

In any algebra **B**, let $D(x, y, z, w)$ denote the "disjointness relation":

$$D(a, b, c, d) \stackrel{\text{def}}{\iff} \mathrm{Cg}^{\mathbf{B}}(a, b) \cap \mathrm{Cg}^{\mathbf{B}}(c, d) = 0_B.$$

Note that

$$\neg\, D(a, b, c, d) \iff \underbrace{\exists x, y \left[x \neq y \ \& \ \bigvee_{\pi} \pi(x, y, a, b) \ \& \ \bigvee_{\pi'} \pi'(x, y, c, d) \right]}_{(*)}$$

where both $\bigvee$'s are infinite disjunctions over **principal congruence formulas** (in the language of **A**).

$(*)$ is a formula of infinitary logic. In general, it cannot be made first-order.

Ein Gedankenexperiment

Suppose ...

1. $\mathcal{V}(\mathbf{A})$ has a finite residual bound;
2. $D(x,y,z,w)$ is definable in $\mathcal{V}(\mathbf{A})$ by a first-order formula.
3. D is definable in $\mathcal{V}^{(n)}$ by the same formula (for large enough n).

Recall that an algebra **B** is **finitely subdirectly irreducible** (**FSI**) if 0_B is meet-irreducible in $\mathrm{Con}\,\mathbf{B}$; equivalently, if

$$\forall x,y,z,w[\,D(x,y,z,w) \to (x=y \ \text{ or } \ z=w)\,].$$

The assumptions imply that

"I am FSI"

is first-order definable in $\mathcal{V}^{(n)}$ (for large n).

"I am FSI" is first-order definable in $\mathcal{V}^{(n)}$ (for large n), say by Φ.

Recall: $\mathcal{V}(\mathbf{A})$ has a finite residual bound. This means:

- $\mathcal{V}(\mathbf{A})_{SI} = \{\mathbf{S}_1, \ldots, \mathbf{S}_k\}$ for some **finite** algebras $\mathbf{S}_1, \ldots, \mathbf{S}_k$ (up to $\cong$).
- $\mathcal{V}(\mathbf{A})_{FSI} = \mathcal{V}(\mathbf{A})_{SI}$.

Then:

- "I am in $\{\mathbf{S}_1, \ldots, \mathbf{S}_k\}$" is first-order definable (absolutely), say by Ψ.
- $\mathcal{V}(\mathbf{A}) \models \Phi \to \Psi$.
- Hence $\mathcal{V}^{(n)} \models \Phi \to \Psi$ for large enough n (Compactness Theorem).
- I.e., $(\mathcal{V}^{(n)})_{FSI} \subseteq \{\mathbf{S}_1, \ldots, \mathbf{S}_k\}$.
- Hence $(\mathcal{V}^{(n)})_{SI} \subseteq (\mathcal{V}^{(n)})_{FSI} \subseteq \mathcal{V}(\mathbf{A})_{SI}$.
- Hence $\mathcal{V}^{(n)} \subseteq \mathcal{V}(\mathbf{A})$.
- Hence $\mathcal{V}(\mathbf{A}) = \mathcal{V}^{(n)}$, so $\mathcal{V}(\mathbf{A})$ is finitely axiomatizable! □

Baker's CD theorem and my extension to SD($\wedge$)

In summary, if

1. $\mathcal{V}(\mathbf{A})$ has a finite residual bound;
2. $D(x, y, z, w)$ is first-order definable in $\mathcal{V}(\mathbf{A})$;
3. The same formula defines D in $\mathcal{V}^{(n)}$ (for large n);

then $\mathbf{A}$ is finitely based.

Baker proved that (2), (3) hold if $\mathcal{V}(\mathbf{A})$ is CD.

- Via a combinatorial analysis of failures of $D(x, y, z, w)$, using Jónsson operations and their identities.

My extension to SD($\wedge$) varieties shamelessly plagiarizes Baker's proof.

- Jónsson operations/identities are replaced by operations/identities characterizing SD($\wedge$) due to Kearnes, Szendrei (1998) and Lipparini (1998), improving Hobby, McKenzie (1988) and Czédli (1983).

Prologue to McKenzie's CM theorem: the commutator

All algebras admit a **commutator operation** $[-,-]$ defined on congruences.

Properties:

- $[\alpha, \beta] \leq \alpha \wedge \beta$.
- $[\alpha, \beta] = \alpha \wedge \beta$ in CD (or SD($\wedge$)) varieties.
- $[\alpha, \beta] = 0_B \iff \alpha, \beta$ are "independent" (in some sense).
- $[\alpha, \alpha] = 0_B \iff \alpha$ is "abelian."

Definition

Let $C(x, y, z, w)$ denote the "**commutator disjointness relation**":

$$C(a, b, c, d) \stackrel{\text{def}}{\iff} [\mathrm{Cg}(x, y), \mathrm{Cg}(z, w)] = 0.$$

C is analoguous to, but weaker than, D.

McKenzie's CM theorem

Theorem (McKenzie, 1987)

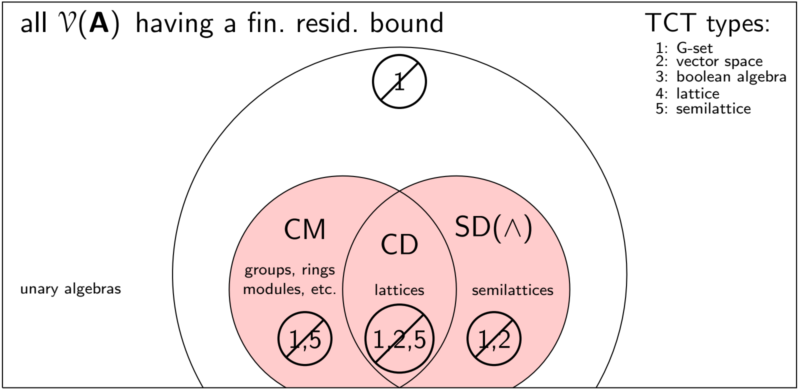
Suppose $\mathcal{V}(\mathbf{A})$ is congruence modular. If $\mathcal{V}(\mathbf{A})$ has a finite residual bound, then $\mathcal{V}(\mathbf{A})$ is finitely axiomatizable.

Remarks on the proof. Assuming $\mathcal{V}(\mathbf{A})$ is CM and has a finite residual bound, McKenzie proved that:

1. **Step 1**: C is first-order definable in $\mathcal{V}(\mathbf{A})$.
2. **Steps 2-10**: Various relations derived from C are first-order definable in $\mathcal{V}^{(n)}$ (for large enough n).
   - Hence certain commutator facts about $\mathcal{V}(\mathbf{A})$ can be lifted to $\mathcal{V}^{(n)}$.
3. **Step 11**: $(\mathcal{V}^{(n)})_{SI} \subseteq \mathcal{V}(\mathbf{A})_{SI}$. Hence $\mathcal{V}(\mathbf{A}) = \mathcal{V}^{(n)}$.

In search of a common generalization

$\mathcal{V}(\mathbf{A})$ for which Jónsson's speculation/Park's conjecture is confirmed:



It would be **very nice** to confirm Jónsson's speculation/Park's conjecture for any $\mathcal{V}(\mathbf{A})$ omitting type 1. Unfortunately, we haven't done that.

Abelian congruences

Let **B** be an algebra and $\theta \in \mathrm{Con}\mathbf{B}$. The **trace** of θ is

$$Tr(\theta) = \mathrm{Sg}^{\mathbf{B}^{2\times 2}}\left(\left(\begin{array}{cc} a & a \\ b & b \end{array}\right), \left(\begin{array}{cc} a & b \\ a & b \end{array}\right) \ : \ a \overset{\theta}{\equiv} b\right) \leq \mathbf{B}^{2\times 2}.$$

Definition

We say θ is **abelian** if for all $\left(\begin{array}{cc} x & y \\ z & w \end{array}\right) \in Tr(\theta)$,

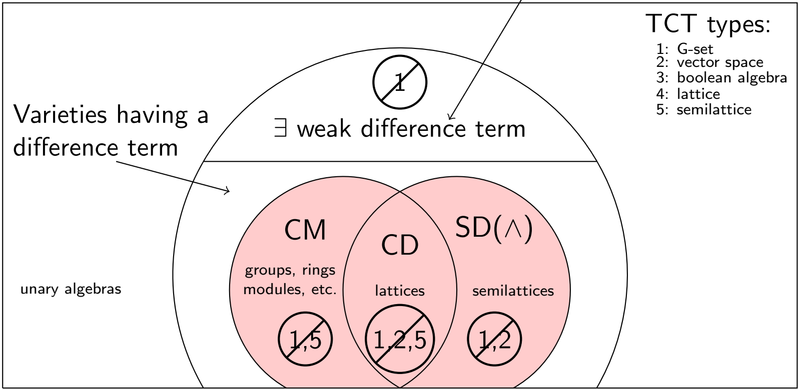
$$x = y \iff z = w.$$

(This is equivalent to $[\theta, \theta] = 0_B$.)

Difference terms

Def: a **weak difference term** (for $\mathcal{V}$) is a term $p(x, y, z)$ satisfying $p(a, a, b) = b = p(b, a, a)$ whenever $(a, b) \in$ an abelian congruence

Def: a **difference term** (for $\mathcal{V}$) is a weak difference term satisfying $p(x, x, y) \approx y$.



Confirmation of Jónsson/Park for DT varieties

Theorem (Kearnes, Szendrei, W)

Suppose $\mathcal{V}(\mathbf{A})$ has a difference term. If $\mathcal{V}(\mathbf{A})$ has a finite residual bound, then $\mathcal{V}(\mathbf{A})$ is finitely axiomatizable.

Remarks on the proof.

1. **Step 1**: we show $C(x, y, z, w)$ is first-order definable in $\mathcal{V}(\mathbf{A})$. (syntactic analysis + TCT + Baker-McNulty-Wang trick)
2. **Steps 2-10**: We then shamelessly attempt to plagiarize McKenzie's proof in the CM case, as far as possible.
3. At the **very last step** of McKenzie's CM proof, we are stuck: he uses definability of "$\mathrm{Cg}(x, y)$ is a non-abelian atom" which we don't have.

Damn!

Apply the KISS principle

Actually

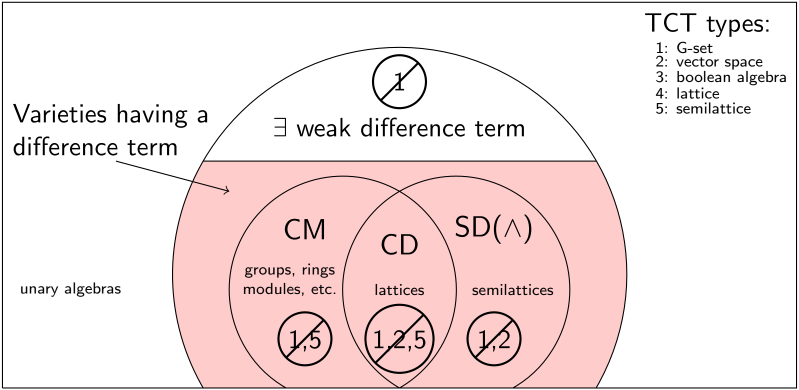
E.W. Kiss, Three remarks on the modular commutator, *AU* **29** (1992).

- Kiss proves that every CM variety has a "4-ary difference term," with interesting properties.
- We prove the same for varieties with a difference term.
- We use this to lift first-order definability of $C(x, y, z, w)$ from $\mathcal{V}(\mathbf{A})$ to $\mathcal{V}^{(j)}$ (something McKenzie wasn't able to do).
- Then some new tricks finish the argument.

Looking backward

At AAA66 in Klagenfurt, in my lecture "The finite basis problem," I posed this challenge:

"**Challenge**. Prove [the Jónsson/Park] conjecture for . . . varieties having a difference term. (Reward: fame and glory.)" ✓



Looking forward

Updated Challenge: Prove the Jónsson/Park conjecture for varieties having a weak difference term (i.e., omitting type 1). (Reward: glory . . .)

Also from my AAA66 lecture:

"**Challenge 2**: Find a counter-example to [the Jónsson/Park conjecture]. (Reward: 50 euros for the first counter-example found.)"

Updated Challenge 2: now 87 euros! 

Thank you!