Varieties with a difference term and Park's conjecture

Keith Kearnes Ágnes Szendrei Ross Willard*

U. Colorado Boulder, USA U. Waterloo, CAN

GAIA 2013
Melbourne, Australia
July 19, 2013

There is an old gent from Down Under
Who's known as a passionate wonder.
It's scary to see
What he gets naturally
From two contravariant functors.

Finite bases

The variety of all groups is defined by the identities

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

The symmetric group S_3 satisfies these identities and more; e.g.,

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

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

Fact: All identities true in S_3 can be deduced from Σ.

Equivalently, $\mathcal{V}(S_3)$ is axiomatized by Σ.

How does one prove this fact (that Σ is a basis for the identities of S_3)?

Option 1: syntactic. Show how to deduce every identity of S_3 from Σ. (Scary!)

Option 2: semantic. Show that every finitely generated, subdirectly irreducible (SI) model of Σ is in $\mathcal{V}(S_3)$. (In fact, in $\{C_2, C_3, S_3\}$.)

This is a challenging exercise (try it!).

Moral: work must be done.

Finitely based algebras

We say that S_3 is **finitely based**.

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

A certain 6-element semigroup is not finitely based (Perkins, 1969).

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

On the other hand, many finite algebras *are* finitely based, including:

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

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

Baker's Theorem

Recall "every finite lattice is finitely based" (McKenzie, 1970).

Here is a far-reaching, celebrated extension.

Theorem (Baker, 1977)

Every finite algebra generating a congruence distributive (CD) variety is finitely based.

Two ingredients in most proofs:

1. Jónsson's "Maltsev condition" characterizing CD varieties (1967).
2. Jónsson's Lemma (1967): If $\mathbf{A}$ is finite and generates a CD variety, then the SI's in $\mathcal{V}(\mathbf{A})$ are all finite and bounded in size (by $|A|$).

A variety with the underlined property is said to **have a finite residual bound**.

Park's Conjecture

Robert Park was a PhD student of Kirby Baker in the early 1970s.

Informed by Baker's theorem, and having investigated all finite algebras that were known at the time to be not finitely based, Park made the following conjecture in his PhD thesis:

Park's Conjecture (1976)

If $\mathbf{A}$ is a finite algebra and $\mathcal{V}(\mathbf{A})$ has a finite residual bound, then $\mathbf{A}$ is finitely based.

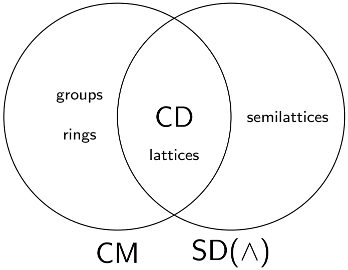
Still unsolved! But confirmed for some broad classes.

Confirmations of Park's conjecture

Park's conjecture is known to be true for finite algebras belonging to ...

1. ... a CD variety (Baker, 1977).
2. ... a CM (congruence modular) variety (McKenzie, 1987).
3. ... an SD($\wedge$) (congruence meet semi-distributive) variety (W, 2000).

Both McKenzie's and my theorem extend Baker's theorem, but in different directions.



How are these theorems proved?

First, an unnecessary but useful device.

Fix a finite algebra **A**.

For $j > 0$ let $\mathcal{V}^{(j)}$ denote the variety axiomatized by all the identities of **A** involving at most j variables.

Facts:

1. $\mathcal{V}^{(1)} \supseteq \mathcal{V}^{(2)} \supseteq \mathcal{V}^{(3)} \supseteq \cdots$.
2. $\bigcap_j \mathcal{V}^{(j)} = \mathcal{V}(\mathbf{A})$.
3. Each $\mathcal{V}^{(j)}$ is finitely axiomatizable.

Thus **A** is finitely based $\Leftrightarrow \mathcal{V}(\mathbf{A}) = \mathcal{V}^{(j)}$ for some (hence all large) j.

Warm-up: DPC

Def: in any algebra $\mathbf{A}$, let $M(x, y, z, w)$ denote the "principal congruence membership" relation:

$$(x, y) \in \mathrm{Cg}^{\mathbf{A}}(z, w).$$

M is characterized by an infinite disjunction of pp-formulas (Maltsev).

In some algebras, M can be defined by a first-order formula.

Def: A variety $\mathcal{V}$ has **definable principal congruences** (DPC) if there is a first-order formula $\pi(x, y, z, w)$ which defines M in every member of $\mathcal{V}$.

Theorem (McKenzie, 1978)

Park's conjecture is true for varieties with DPC.

Proof of McKenzie's DPC theorem

Assume **A** is finite, $\mathcal{V}(\mathbf{A})$ has DPC, and $\mathcal{V}(\mathbf{A})$ has a finite residual bound.

Choose π such that $\mathcal{V}(\mathbf{A}) \models \pi(x, y, z, w) \leftrightarrow$ "$(x, y) \in \mathrm{Cg}(z, w)$".

Let σ be the following sentence:

$$\exists x, y(x \neq y \;\&\; \forall z, w[z \neq w \to \underbrace{\pi(x, y, z, w)}_{\text{“}(x,y)\in \mathrm{Cg}(z,w)\text{”}}]).$$

In $\mathcal{V}(\mathbf{A})$, σ asserts "I am SI."

Next, let $\mathcal{V}(\mathbf{A})_{SI} = \{\mathbf{S}_1, \ldots, \mathbf{S}_k\}$ be the set of SI's in $\mathcal{V}(\mathbf{A})$.

There exists a first-order sentence, τ, which asserts "I am in $\mathcal{V}(\mathbf{A})_{SI}$" (absolutely).

σ: ~~"I am SI"~~ $\exists x, y(x \neq y \;\&\; \forall z, w[z \neq w \to \pi(x, y, z, w)])$.

τ: "I am in $\mathcal{V}(\mathbf{A})_{SI}$"

1. Clearly $\mathcal{V}(\mathbf{A}) \models \sigma \to \tau$.
2. $\therefore \mathcal{V}^{(j)} \models \sigma \to \tau$ for large enough j (compactness theorem).
3. I.e., $\mathcal{V}^{(j)} \models$ ~~"I am SI"~~ $\to$ "I am in $\mathcal{V}(\mathbf{A})_{SI}$".
4. $\therefore$ all SI's in $\mathcal{V}^{(j)}$ are in $\mathcal{V}(\mathbf{A})$.
5. $\therefore \mathcal{V}^{(j)} \subseteq \mathcal{V}(\mathbf{A})$.
6. $\therefore \mathcal{V}^{(j)} = \mathcal{V}(\mathbf{A})$,
7. which proves **A** is finitely based. $\square$

I cheated. Where? σ asserts "I am SI" in $\mathcal{V}(\mathbf{A})$; not necessarily in $\mathcal{V}^{(j)}$.

To fix: need to show $\mathcal{V}^{(j)} \models \pi(x, y, z, w) \leftrightarrow$ "$(x, y) \in \mathrm{Cg}(z, w)$".

I.e., need to "lift" DPC from $\mathcal{V}(\mathbf{A})$ to $\mathcal{V}^{(j)}$. Can do (a trick).

Proof of Baker's CD and my SD($\wedge$) theorems

Suppose **A** is finite and $\mathcal{V}(\mathbf{A})$ is CD. We cannot say that $\mathcal{V}(\mathbf{A})$ has DPC.

However, Baker proved that the "disjointness relation" is definable:

$$D(x,y,z,w) \ : \ \text{“}\mathrm{Cg}(x,y) \cap \mathrm{Cg}(z,w) = 0\text{”}.$$

And he showed how to:

- Lift definability of D from $\mathcal{V}(\mathbf{A})$ to $\mathcal{V}^{(j)}$ (for large j).
- Use definability of D to rule out SI's in $\mathcal{V}^{(j)} \setminus \mathcal{V}(\mathbf{A})$.

My proof for SD($\wedge$) shamelessly plagiarizes Baker's proof, using the Maltsev condition for SD($\wedge$) due to Kearnes, Szendrei (1998) and Lipparini (1998).

- I even plagiarized the Ramsey argument from Baker's proof.
- Baker, McNulty, Wang (2004) gave a nice simplification.

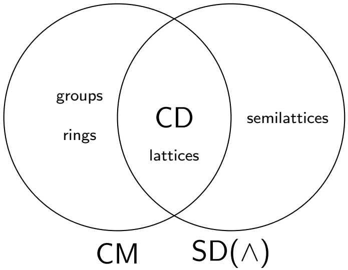
Proof of McKenzie's CM theorem

McKenzie's proof of Park's conjecture for CM varieties is (much) harder.

- CM varieties permit abelianness; witnessed by the **commutator operation** $[-,-]$ defined on $\mathrm{Con}\,\mathbf{A}$.
- $[\alpha,\beta] \le \alpha \wedge \beta$ generally.
- $[\alpha,\beta] < \alpha \wedge \beta$ implies abelianness.
- In CD (or SD($\wedge$)) varieties, $[\alpha,\beta] = \alpha \wedge \beta$.
- Let $C(x,y,z,w)$ denote the relation "$[\mathrm{Cg}(x,y),\mathrm{Cg}(z,w)] = 0$". This is an analogue to D.
- If $\mathcal{V}(\mathbf{A})$ is CM and with a finite residual bound, McKenzie proves that C is first-order definable in $\mathcal{V}(\mathbf{A})$.
- From this point, McKenzie's proof ends resemblance to CD case. Many rich, new ideas used to ultimately get $\mathcal{V}(\mathbf{A}) = \mathcal{V}^{(j)}$.

In search of a common generalization

Recall: Park's conjecture has been proved for algebras in



It would be nice to have a finite basis theorem that covers both CM and SD(∧) varieties.

A candidate setting for the generalization

Definition

A 3-ary term $p(x, y, z)$ is a **difference term** for a variety $\mathcal{V}$ if:

1. $\mathcal{V} \models p(x, x, y) \approx y$.
2. For all $\mathbf{A} \in \mathcal{V}$, $p(a, b, b) \overset{\theta}{\equiv} a$ where $\theta = [\mathrm{Cg}(a, b), \mathrm{Cg}(a, b)]$.

Every CM variety has a difference term (Herrmann, 1979; Gumm 1981).

Every SD($\wedge$) variety has a difference term: $p(x, y, z) = z$.

Properties of DT varieties

Varieties with a difference term are nice.

- There is a natural Maltsev condition (Kearnes, Szendrei 1998): SD($\wedge$) + CP.
- There is a TCT characterization (Kearnes 1995): "omit type 1, and no type-2 tails."
- $[-,-]$ is fairly well behaved (Kearnes 1995, Lipparini 1996). In particular, $[\alpha,\beta]=[\beta,\alpha]$.

We have a generalization!

Theorem (Kearnes, Szendrei, W (July 11, 2013))

Park's conjecture is true for varieties with a difference term.

Remarks on the proof.

1. First we show $C(x, y, z, w)$ is first-order definable in $\mathcal{V}(\mathbf{A})$. (8 dense pages; syntactic analysis + tame congruence theory + Baker-McNulty-Wang tricks)
2. 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

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

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

Looking forward

Obvious next challenge: proving Park's conjecture for varieties that omit type 1.

Such varieties have a "weak difference term" (Hobby, McKenzie).

Challenge

Suppose $\mathcal{V}(\mathbf{A})$ omits type 1 and has a finite residual bound. Show that $C(x, y, z, w)$ & $C(z, w, x, y)$ is first-order definable in $\mathcal{V}(\mathbf{A})$.

Thank you!