THE FINITE BASIS PROBLEM

ROSS WILLARD

Abstract. A finite algebra of finite type (i.e., having just finitely many fundamental operations) is *finitely based* if the variety it generates can be axiomatized by just finitely many equations. The *finite basis problem* asks for an explicit characterization of the finite algebras of finite type which are finitely based. This is a ridiculously impossible problem, but an intriguing subproblem is the task of proving a conjecture of R. Park from 1976. Park's conjecture, motivated by K. Baker's celebrated finite basis theorem (for finite algebras in congruence distributive varieties) states that if a finite algebra of finite type generates a variety in which all subdirectly irreducible members are finite and of bounded size, then the algebra is finitely based. In this lecture I survey the current state of knowledge of Park's conjecture and related problems, and describe an extension of Baker's theorem I wish I could prove.

1. Finitely Based Algebras

A *finite algebra of finite type* is a structure $\mathbb{A} = \langle A; f_1, f_2, \ldots, f_n \rangle$ where A is finite nonempty set and each f_i is a *finitary operation* on A, i.e., a function $f_i : A^{n_i} \to A$ for a suitable nonnegative integer n_i. An *identity of* $\mathbb{A}$ is a formal equation $s \approx t$ where each of s, t is an expression or word, built from variables and symbols representing the operations $f_1, \ldots, f_n$, which is identically true in $\mathbb{A}$ under all possible assignments of values in A to the variables occurring in s or t. $\mathbb{A}$ is said to be *finitely based* if there exists a finite list of identities of $\mathbb{A}$ from which all the identities of $\mathbb{A}$ can be formally deduced.

That is the definition. A more useful characterization is the following. We consider arbitrary algebras $\mathbb{B} = \langle B; g_1, \ldots, g_n \rangle$ of the same "type" as $\mathbb{A}$, i.e., whose operations $g_1, \ldots, g_n$ are the same in number as those of $\mathbb{A}$ and take the same number of arguments as their counterparts in $\mathbb{A}$. Then as is customary we let $\mathbf{HSP}(\mathbb{A})$ denote the *variety generated by* $\mathbb{A}$ – that is, the smallest class of structures of the same

1991 *Mathematics Subject Classification.* Primary 08B05; Secondary 03C05.

Key words and phrases. equational theory, finitely based, variety, Park's conjecture.

Work supported by the NSERC of Canada.

type as $\mathbb{A}$ which contains $\mathbb{A}$ and is closed under the formation of arbitrary Cartesian products, subalgebras and homomorphic images and containing $\mathbb{A}$. Then $\mathbb{A}$ is finitely based iff $\mathbf{HSP}(\mathbb{A})$ can be axiomatized by some finite list of identities. This in turn is equivalent to saying that $\mathbf{HSP}(\mathbb{A})$ can be axiomatized by a single sentence of first-order logic.

Now an axiomatization of $\mathbf{HSP}(\mathbb{A})$ can be thought of as a *test for membership* in $\mathbf{HSP}(\mathbb{A})$. That is, satisfaction of the axioms provides a "test condition," and an arbitrary algebra (of the same type as $\mathbb{A}$) belongs to $\mathbf{HSP}(\mathbb{A})$ iff it satisfies this test condition. Thus another way to express the property of being finitely based is the following: $\mathbb{A}$ is finitely based iff there is a *first-order* test for membership in $\mathbf{HSP}(\mathbb{A})$.

To illustrate, let's look at the example where $\mathbb{A}$ is the 6-element group S_3. Here are three (correct) tests for membership in $\mathbf{HSP}(S_3)$:

(1) $G \in \mathbf{HSP}(S_3)$ iff G is a quotient group of a subgroup of a power of S_3.
(2) $G \in \mathbf{HSP}(S_3)$ iff G is a group having a normal subgroup N such that (i) N is an elementary abelian 3-group and (ii) G/N is an elementary abelian 2-group.
(3) $G \in \mathbf{HSP}(S_3)$ iff G is a group in which the order of every element is a divisor of 6, squares commute with each other, and every commutator $x^{-1}y^{-1}xy$ has order 3 or 1.

The first characterization, while true, offers little information beyond the definition of $\mathbf{HSP}(\mathbb{A})$ itself. The second characterization is more informative, and of the three is perhaps the most appealing to a group theorist. From our point of view, however, it is not decisive since the existence of a normal subgroup with certain properties can only be stated in the context of second-order logic, not first-order logic (which permits discussion of elements but not of subsets). The third characterization, by contrast, shows that S_3 is finitely based since the test condition it gives can be formulated as a first-order sentence.

2. The Finite Basis Problem

Which finite algebras of finite type are finitely based? This is the *Finite Basis Problem*. The answer is far from known and will likely never be fully known. But to get a sense of what an approximate answer might look like, here are some data.

In some sense all "well-behaved" finite algebras *are* finitely based. In particular, the class of finitely based algebras includes all finite groups [14], all finite rings [6, 7], all finite lattices [10] or algebras whose operations include lattice operations or, more generally, which belong to a congruence distributive variety [1]. This last fact is known as Baker's

Finite Basis Theorem; it was proved by K. Baker in the early 1970s and is sufficiently celebrated to have been reproved many times since then.

Yet, perhaps surprisingly, not every finite algebra of finite type is finitely based. The first known examples of this type were artificially constructed for this purpose [8]; since then, other more natural examples were found, including certain semigroups [16] and nonassociative rings [17].

Finally, we will never be able to *decide* which algebras are finitely based, at least not in the strict sense of the term, since R McKenzie showed, in a monumental paper [13], that the Halting Problem ("which Turing machines will halt if started on the empty input?") can be effectively reduced to the Finite Basis Problem.

3. Park's Conjecture

An elementary result in the theory of universal algebra states that every variety $\mathcal{V}$ contains a class $\mathcal{V}_{si}$ of algebras with the property that

(1) every member $\mathbb{B} \in \mathcal{V}$ is residually in $\mathcal{V}_{si}$ (that is, every pair of distinct elements of B can be separated by a homomorphism from $\mathbb{B}$ into some member of $\mathcal{V}_{si}$); and
(2) every member $\mathbb{C} \in \mathcal{V}_{si}$ is "irreducible" in the sense that it has a pair of elements $a \neq b \in C$ such that no noninjective homomorphism with domain $\mathbb{C}$ separates a from b.

The class $\mathcal{V}_{si}$ is uniquely defined by conditions (1) and (2); the members of $\mathcal{K}_{si}$ are called *subdirectly irreducible*. Every variety is determined by its subdirectly irreducible members, and these algebras are particularly important in the general study of varieties.

In the mid-1970s it was noted that for all examples of finite algebras $\mathbb{A}$ of finite type known at that time to be *not* finitely based, $\mathbf{HSP}(\mathbb{A})$ contained subdirectly irreducible members of arbitrarily large finite cardinalities and all infinite cardinalities. In 1976, in his Ph.D. thesis, R. Park therefore made the following conjecture [15]:

> **Park's Conjecture**: Let $\mathbb{A}$ be a finite algebra of finite type. If there exists a finite bound to the size of all the subdirectly irreducible members of $\mathbf{HSP}(\mathbb{A})$ (or as we say, if $\mathbf{HSP}(\mathbb{A})$ "has a finite residual bound"), then $\mathbb{A}$ is finitely based.

This conjecture is still open. It has been validated in many special cases and it remains of central interest in the field. My chief goal in this lecture is to discuss the status of Park's conjecture; a subgoal is to illustrate the importance of the perspective of first-order logic.

4. The Importance of Principal Congruences

When $\mathbb{A}$ is an algebra and $a, b \in A$, $\mathrm{Cg}(a, b)$ denotes the smallest equivalence relation on the set A which (i) is compatible with the operations of $\mathbb{A}$ so that a quotient algebra may be naturally constructed on the set of its classes, and (ii) identifies a with b. $\mathrm{Cg}(a, b)$ is called the *principal congruence* of $\mathbb{A}$ generated by the pair (a, b).

A class $\mathcal{K}$ of algebras is said to have *definable principal congruences*, or DPC, if there is a first-order formula $\pi(x, y, u, v)$ which defines the relation "$(x, y) \in \mathrm{Cg}(u, v)$" in every member of $\mathcal{K}$. An example of a class $\mathcal{K}$ having DPC is the variety of commutative rings with unit element 1. If R is any such ring and $a, b \in R$, the principal congruence generated by (a, b) is the equivalence relation induced on R by the ideal generated by $a - b$. It follows that the class of all such rings has DPC, as is witnessed by the first-order formula $\pi(x, y, z, w)$ given by

$$\exists r(r(u - v) = x - y).$$

Finite algebras belonging to varieties having DPC satisfy Park's conjecture, because of the following theorem of McKenzie [11].

Theorem 4.1. *Suppose $\mathbb{A}$ is a finite algebra of finite type, and $\mathbf{HSP}(\mathbb{A})$ has a finite residual bound. If $\mathbf{HSP}(\mathbb{A})$ has DPC, then $\mathbb{A}$ is finitely based.*

Theorem 4.1 can be proved by reducing it to the following lemma, which is a special case of a result due to B. Jónsson [4, Theorem 1].

Lemma 4.2. *Suppose $\mathcal{V}$ is a variety of finite type and having a finite residual bound. If there exist classes $\mathcal{S} \subseteq \mathcal{K}$ satisfying:*

1. *$\mathcal{V} \subseteq \mathcal{K}$*
2. *$\mathcal{K}$ is finitely axiomatizable (in first-order logic)*
3. *$\mathcal{S}$ is finitely axiomatizable*
4. *$\mathcal{K}_{si}$, the class of all subdirectly irreducible algebras in $\mathcal{K}$, is contained in S: $\mathcal{K}_{si} \subseteq \mathcal{S}$.*
5. *$\mathcal{V}_{si}$, the class of all subdirectly irreducible algebras in $\mathcal{V}$, is exactly the intersection of $\mathcal{V}$ with $\mathcal{S}$: $\mathcal{V}_{si} = \mathcal{V} \cap \mathcal{S}$.*

Then $\mathcal{V}$ is finitely axiomatizable.

Proof. Because $\mathcal{V}$ has a finite residual bound, $\mathcal{V}_{si}$ consists up to isomorphism of only finitely many finite algebras. Hence membership in $\mathcal{V}_{si}$ can be characterized by a first-order sentence. Thus every member of $\mathcal{V}$ satisfies

(1) "I'm in $\mathcal{K}$" and (if "I'm in $\mathcal{S}$" then "I'm in $\mathcal{V}_{si}$").

As (1) can be formulated by a single first-order sentence, the compactness theorem of first-order logic guarantees the existence of a finitely axiomatizable variety $\mathcal{W} \supseteq \mathcal{V}$ which also models (1). In other words, $\mathcal{W} \subseteq \mathcal{K}$ and $\mathcal{W} \cap \mathcal{S} \subseteq \mathcal{V}_{si}$. It then follows that

$$\mathcal{W} \cap \mathcal{S} = \mathcal{V} \cap \mathcal{S}$$

and hence

$$\mathcal{W}_{si} = \mathcal{V}_{si}$$

because $\mathcal{W}_{si} \subseteq \mathcal{K}_{si} \subseteq \mathcal{S}$ and so $\mathcal{W}_{si} = (\mathcal{W} \cap \mathcal{S})_{si} = (\mathcal{V} \cap \mathcal{S})_{si} = \mathcal{V}_{si}$. Since varieties are determined by their subdirectly irreducible members, it follows that $\mathcal{W} = \mathcal{V}$, proving that $\mathcal{V}$ is finitely axiomatizable. □

We are almost ready to prove Theorem 4.1. Generalizing the notion of being subdirectly irreducible, we say that an algebra $\mathbb{C}$ is *finitely subdirectly irreducible* if for any two noninjective homomorphisms h_1, h_2 with domain $\mathbb{C}$ there exists $a \neq b \in C$ which are separated by neither h_1 nor h_2. Equivalently (letting 0 denote the trivial equivalence relation), $\mathbb{C}$ is finitely subdirectly irreducible if for all $x, y, z, w \in C$, if $\mathrm{Cg}(x, y) \cap \mathrm{Cg}(z, w) = 0$ then $x = y$ or $z = w$.

Proof of Theorem 4.1. It can be shown that there exists a finitely axiomatizable class $\mathcal{K} \supseteq \mathcal{V}$ which also has DPC (exercise). Of course $\mathcal{K}_{fsi}$, the class of finitely subdirectly irreducible members of $\mathcal{K}$, is defined by the condition

> "I'm in $\mathcal{K}$" and $\forall xyzw[$ if "$\mathrm{Cg}(x, y) \cap \mathrm{Cg}(z, w) = 0$" then $x = y$ or $z = w$ $]$.

Because $\mathcal{K}$ has DPC, the relation $\mathrm{Cg}(x, y) \cap \mathrm{Cg}(z, w) = 0$ is definable by a first-order formula within $\mathcal{K}$, so the entire condition above can be formulated as a first-order sentence, proving $\mathcal{K}_{fsi}$ is finitely axiomatizable. Now we apply Lemma 4.2 with $\mathcal{S} = \mathcal{K}_{fsi}$. □

The proof just given shows that the hypothesis of having DPC in the statement of Theorem 4.1 can be weakened.

Corollary 4.3. *Suppose $\mathbb{A}$ is a finite algebra of finite type, and $\mathbf{HSP}(\mathbb{A})$ has a finite residual bound. If there exists a finitely axiomatizable class $\mathcal{K} \supseteq \mathcal{V}$ in which the relation "$\mathrm{Cg}(x, y) \cap \mathrm{Cg}(z, w) = 0$" is definable by a first-order formula, then $\mathbb{A}$ is finitely based.*

5. Baker's Theorem and Extensions

The most significant motivator for Park's conjecture was K. Baker's celebrated finite basis theorem [1].

Theorem 5.1. *Suppose* $\mathbb{A}$ *is a finite algebra of finite type, and* $\mathbf{HSP}(\mathbb{A})$ *is congruence distributive (and hence has a finite residual bound). Then* $\mathbb{A}$ *is finitely based.*

Several proofs of Theorem 5.1 are known. Many of these proofs show, directly or indirectly, that the relation "$\mathrm{Cg}(x, y) \cap \mathrm{Cg}(z, w) = 0$" is definable by a first-order formula (i) in $\mathbf{HSP}(\mathbb{A})$, and then (ii) in a finitely axiomatizable class $\mathcal{K} \supseteq \mathbf{HSP}(\mathbb{A})$. Hence Corollary 1 can be applied.

Building on these ideas, I extended Baker's original proof of Theorem 5.1 to algebras belonging to *congruence meet-semidistributive* varieties (these include for example any algebra whose operations include a semilattice operation).

Theorem 5.2. [18] *Suppose* $\mathbb{A}$ *is a finite algebra of finite type, and* $\mathbf{HSP}(\mathbb{A})$ *has a finite residual bound. If* $\mathbf{HSP}(\mathbb{A})$ *is congruence meet-semidistributive, then* $\mathbb{A}$ *is finitely based.*

The proof follows Baker's original proof of his theorem and is rather complicated. The strategy, like the one outlined above for Baker's theorem, is simply to show that the relation "$\mathrm{Cg}(x, y) \cap \mathrm{Cg}(z, w) = 0$" is definable by a first-order formula in a finitely axiomatizable class $\mathcal{K} \supseteq \mathbf{HSP}(\mathbb{A})$. Do there exist simpler proofs of Theorem 5.2? One possible approach, due to Baker and J. Wang [3], involves a weakening of the concept of DPC which Baker and Wang call *definable principal subcongruences* or DPSC. Baker and Wang proved the analogue of McKenzie's Theorem 4.1 with DPC replaced by DPSC, and also proved that $\mathbf{HSP}(\mathbb{A})$ has DSPC whenever $\mathbb{A}$ is a finite algebra of finite type and $\mathbf{HSP}(\mathbb{A})$ is congruence distributive. This gives a particularly simple proof of Baker's theorem, and it is reasonable to ask if an equally simple proof of Theorem 5.2 can be obtained by the same method.[1] The answer is still not known:

Open Problem. If $\mathbb{A}$ is a finite algebra of finite type, $\mathbf{HSP}(\mathbb{A})$ is congruence meet-semidistributive, and $\mathbf{HSP}(\mathbb{A})$ has a finite residual bound, does it follow that $\mathbf{HSP}(\mathbb{A})$ has DSCP?

An earlier extension of Baker's Theorem 5.1 is the following theorem of McKenzie [12].

[1]Very recently, two relatively straightforward proofs of Theorem 5.2 by other methods have been announced. The first, due to M. Maróti and R. McKenzie [9], also extends the result under certain conditions to the quasivariety $\mathbf{SP}(\mathbb{A})$ generated by $\mathbb{A}$. The second, due to Baker, G. McNulty and Wang [2], weakens the requirement that $\mathbf{HSP}(\mathbb{A})$ have a finite residual bound.

Theorem 5.3. *Suppose* $\mathbb{A}$ *is a finite algebra of finite type, and* $\mathbf{HSP}(\mathbb{A})$ *has a finite residual bound. If* $\mathbf{HSP}(\mathbb{A})$ *is congruence modular, then* $\mathbb{A}$ *is finitely based.*

The remarkable thing about McKenzie's proof of this theorem is that, although it is not possible in this context to show the definability of "$\mathrm{Cg}(x, y) \cap \mathrm{Cg}(z, w) = 0$," the proof makes essential use of the definability of the relation "$[\mathrm{Cg}(x, y), \mathrm{Cg}(z, w)] = 0$" in a finitely axiomatizable class $\mathcal{K} \supseteq \mathbf{HSP}(\mathbb{A})$. Here we see something new: the *commutator operation* $[-, -]$ of commutator theory. Since the commutator operation trivializes to intersection in congruence distributive varieties, McKenzie's proof of Theorem 5.3 can be seen to have some of the same elements of the proofs of Theorems 4.1, 5.1 and 5.2.

6. Future Directions

Park's conjecture has been verified for algebras belonging to varieties which are either

(1) congruence distributive,
(2) congruence modular, or
(3) congruence meet-semidistributive.

Both congruence modularity and congruence meet-semidistributivity generalize congruence distributivity, though in different directions. It is natural to seek a common generalization of congruence modularity and congruence meet-semidistributivity. One natural candidate is the property of having difference term.

Definition 6.1. Let $\mathcal{K}$ be a class of algebras. A term $p(x, y, z)$ is a *difference term for* $\mathcal{K}$ if for all $\mathbb{A} \in \mathcal{K}$, all $\theta \in \mathrm{Con}\,\mathbb{A}$ and all $(a, b) \in \theta$,

$$\begin{aligned} p(a, b, b) &= a, \text{ and} \\ (p(a, a, b), b) &\in [\theta, \theta]. \end{aligned}$$

Every congruence modular variety or congruence meet-semidistributive variety has a difference term. Moreover, the commutator operation is well-behaved in varieties having a difference term. Finally, there is a natural tame congruence-theoretic characterization of (locally finite) varieties having a difference term [5]. For all of these reasons, I suggest that the next challenge is:

Challenge. Prove Park's conjecture for finite algebras belonging to varieties having a difference term. (Reward: fame and glory.)

But is Park's conjecture true in complete generality? I suggest that perhaps the answer is "no." Therefore, if ever you are studying a

particularly strange finite algebra whose operations are sufficiently impoverished that it does not have a difference term, but are not so impoverished that the algebra generates an abelian variety, try to determine if the variety it generates has a finite residual bound. If it does, then attempt to determine if the variety is finitely axiomatizable. You might find a counter-example to Park's conjecture. Counter-examples often do not earn the same fame and glory as do difficult theorems, so to make this activity worth your while I make the following offer:

Challenge 2. Find a counter-example to Park's conjecture. (Reward: 50 euros for the first counter-example found.)

References

[1] K. Baker, Finite equational bases for finite algebras in a congruence-distributive equational class, *Adv. Math.* **24** (1977), 207–243.

[2] K. A. Baker, G. F. McNulty, and J. Wang, An extension of Willard's finite basis theorem: congruence meet-semidistributive varieties of finite critical depth (preprint, 2004).

[3] K. A. Baker and J. Wang, Definable principal subcongruences, *Algebra Universalis* **47** (2002), 145–151.

[4] B. Jónsson, Congruence varieties, Appendix 3 in G. Grätzer, *Universal Algebra*, Second Edition, Springer-Verlag, 1979.

[5] K. A. Kearnes, Varieties with a difference term, *J. Algebra* **177** (1995), 926–960.

[6] R. Kruse, Identities satisfied by a finite ring, *J. Algebra* **26** (1973), 298–318.

[7] I. V. L'vov, Varieties of associative rings, I, *Algebra i Logika* **12** (1973), 269–297; II, *Algebra i Logika* **12** (1973), 667-688, 735.

[8] R. Lyndon, Identities in finite algebras, *Proc. Amer. Math. Soc. 5* (1954), 8–9.

[9] M. Maróti and R. McKenzie, Finite basis problems and results for quasivarieties (preprint, 2003).

[10] R. McKenzie, Equational bases for lattice theories, *Math. Scand.* **27** (1970), 24–38.

[11] R. McKenzie, Para-primal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties, *Algebra Universalis* **8** (1978), 336–348.

[12] R. McKenzie, Finite equational bases for congruence modular varieties, *Algebra Universalis* **24** (1987), 224–250.

[13] R. McKenzie, Tarski's finite basis problem is undecidable, *Internat. J. Algebra and Computat.* **6** (1996), 49–104.

[14] S. Oates and M. B. Powell, Identical relations in finite groups, *J. Algebra* **1** (1965), 11–39.

[15] R. Park, *Equational classes of non-associative ordered systems*, Ph.D. dissertation, UCLA, 1976.

[16] P. Perkins, Bases for equational theories of semigroups, *J. Algebra* **11** (1968), 293–314.

[17] S. V. Polin, On the identities of finite algebras, *Sib. Math. J.* **17** (1976), 1356-1366.

[18] R. Willard, A finite basis theorem for residually finite, congruence meet-semidistributive varieties, *J. Symbolic Logic* **65** (2000), 187–200.

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
E-mail address: rdwillar@uwaterloo.ca