Which Finite Algebras Are Finitely Based?

George F. McNulty

Department of Mathematics

University of South Carolina

Some Initial Considerations

Here we will only consider **algebras** to be nonempty sets equipped with a system of only finitely many operations, each of finite rank.

An algebra $\mathbf{A}$ is **finitely based** if and only if there is a finite set Σ of equations true in $\mathbf{A}$ such that every equation true in $\mathbf{A}$ is a logical conseqeunce of Σ—that is, the equational theory of $\mathbf{A}$ is finitely axiomatizable.

Likewise, a variety $\mathcal{V}$ of algebras is **finitely based** if the equational theory of $\mathcal{V}$ is finitely axiomatizable.

In the Beginning

Using a difficult 1941 result of Emil Post, in 1951 Roger Lyndon demonstrated that all 2-element algebras are finitely based.

In the Beginning

Using a difficult 1941 result of Emil Post, in 1951 Roger Lyndon demonstrated that all 2-element algebras are finitely based.

On the other hand, in 1954 he made the surprising discovery of an algebra with seven elements that is not finitely based.

A Central Problem

This led Alfred Tarski to pose the following problem:

Tarski's Finite Basis Problem: *Does there exist a recursive algorithm which when presented with an effective description of a finite algebra will determine if the algebra is finitely based?*

A Central Problem

This led Alfred Tarski to pose the following problem:

Tarski's Finite Basis Problem: *Does there exist a recursive algorithm which when presented with an effective description of a finite algebra will determine if the algebra is finitely based?*

In groundbreaking work published in 1996, Ralph McKenzie has shown that no such algorithm exists.

A Brief History

A certain 3-element groupoid is not finitely based (Murskiĭ 1965);

A Brief History

A certain 3-element groupoid is not finitely based (Murskiĭ 1965);
All finite groups are finitely based (Oates and Powell 1965);

A Brief History

A certain 3-element groupoid is not finitely based (Murskiĭ 1965);
All finite groups are finitely based (Oates and Powell 1965);
All finite rings are finitely based (L'vov and Kruse independently,1973);

A Brief History

A certain 3-element groupoid is not finitely based (Murskiĭ 1965);
All finite groups are finitely based (Oates and Powell 1965);
All finite rings are finitely based (L'vov and Kruse independently,1973);
The semigroup consisting of the following six matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

where the operation is matrix multiplication is not finitely based (Perkins 1968).

A Brief History

A certain 3-element groupoid is not finitely based (Murskiĭ 1965);
All finite groups are finitely based (Oates and Powell 1965);
All finite rings are finitely based (L'vov and Kruse independently,1973);
The semigroup consisting of the following six matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

where the operation is matrix multiplication is not finitely based (Perkins 1968).

All commutative semigroups are finitely based (Perkins 1968);

More of the Story

All finite lattices with operators are finitely based (McKenzie 1970);

More of the Story

All finite lattices with operators are finitely based (McKenzie 1970);

All finite algebras with only finitely many basic operations which belong to congruence distributive varieties are finitely based (Baker 1971);

At this point, most of the finite algebras arising in the classical setting were known to be finitely based. Apart from Perkins example of those six 2×2 matrices, all the nonfinitely based finite algebras seemed to be very ad hoc. While Tarski's Problem seemed out of reach there are two inviting prospects.

Two Inviting Prospects

Surely one could extend Baker's Theorem to the congruence modular case, thus giving a common generalization to to those results about finite groups, rings, and lattices. . .

Two Inviting Prospects

Surely one could extend Baker's Theorem to the congruence modular case, thus giving a common generalization to to those results about finite groups, rings, and lattices. . .

It looks like all the finite algebras which are not finitely based must generate varieties which have infinite subdirectly irreducible algebras. . .

How to Dash Some Hopes

Certain finite nonassociative rings are not finitely based (Polin 1976);

How to Dash Some Hopes

Certain finite nonassociative rings are not finitely based (Polin 1976);

Certain finite groups with an element distinguished by a new constant are not finitely based (Bryant 1982).

A Problem

Call a finite algebra **expandably finitely based** provided every expansion of $\mathbf{A}$ by finitely many additional operations is finitely based. Ralph McKenzie proved that every finite lattice is expandably finitely based, and Baker's Theorem entails the same is true for any finite algebra that generates a congruence distributive variety. On the other hand Bryant's Theorem tells us that not every finite group is expandably finitely based. Which finite algebras generating congruence modular varieties are expandably finitely based?

Subdirectly Irreducible Algebras

A **subdirect respresentation** of an algebra $\mathbf{A}$ is a system $\langle h_i \mid i \in I \rangle$ of homomorphisms with domain A so that the system of homomorphisms separates the elements of A. The homomorphic images $h_i(\mathbf{A})$ are called the **factors** of the representation. A subdirect representation is **trivial** if one of its homomorphism is an isomorphism. An algebra is **subdirectly irreducible** provided all of its subdirect representations are trivial. The subdirectly irreducible algebras are exactly those which have a least nontrivial congruence (called the **monolith**).

According to a classical result of Garrett Birkhoff, every algebra has a subdirect representation for which all the factors are subdirectly irreducible. Consequently, every variety is determined by its class of subdirectly irreducible members. For any class $\mathcal{K}$ of algebras we use $\mathcal{K}_{\mathsf{si}}$ to denote the class of subdirectly irreducible algebras in $\mathcal{K}$. In this talk we will say that $\mathcal{K}$ is **residually very finite** provided there is a finite upper bound on the size of the algebras in $\mathcal{K}_{\mathsf{si}}$.

The Other Inviting Prospect. . .

Around 1974 Bjarni Jónsson offered the speculation that if $\mathbf{A}$ is a finite algebra which generates a residually very finite variety, then $\mathbf{A}$ is finitely based.

The Other Inviting Prospect. . .

Around 1974 Bjarni Jónsson offered the speculation that if $\mathbf{A}$ is a finite algebra which generates a residually very finite variety, then $\mathbf{A}$ is finitely based.

Around the same time, Robert Park analyzed all the known nonfinitely based finite algebra showing that each one generated infinite subdirectly irreducible algebras. He offered as a conjecture the speculation just mentioned. **It has not been settled**, but many more nonfinitely based algebras are now known that deserve the same attention Park gave to those known in the early 1970's.

Two Extensions of Baker's Theorem

All finite algebras with only finitely many basic operations which belong to congruence modular residually very finite varieties are finitely based. (McKenzie 1987);

Two Extensions of Baker's Theorem

All finite algebras with only finitely many basic operations which belong to congruence modular residually very finite varieties are finitely based. (McKenzie 1987);

All finite algebras with only finitely many basic operations which belong to congruence meet semidistributive residually very finite varieties are finitely based (Willard 2000).

Principal Congruences

A variety $\mathcal{V}$ has **definable principal congruences** provided there is an elementary formula $\Gamma(u, v, x, y)$ such that

$$\{\langle c, d\rangle \mid \mathbf{A} \models \Gamma(c, d, a, b)\} = \mathsf{Cg}^{\mathbf{A}}(a, b)$$

for all $\mathbf{A} \in \mathcal{V}$ and all $a, b \in A$. According to some highly useful work of Mal'tsev, the formula $\Gamma(u, v, x, y)$ can be taken to be a certain kind of positive existential formula so that the sentence

$$\forall x, u, v[\Gamma(u, v, x, x) \to u \approx v]$$

holds in every algebra (whether in $\mathcal{V}$ or not). Formulas of this kind are called **congruence formulas**.

Another Theorem of McKenzie (1978)

If $\mathcal{V}$ is a residually very finite variety with definable principal congruences, then $\mathcal{V}$ is finitely based.

Another Theorem of McKenzie (1978)

If $\mathcal{V}$ is a residually very finite variety with definable principal congruences, then $\mathcal{V}$ is finitely based.

If $\mathcal{V}$ is a locally finite variety with definable principal congruences and $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatizable, then $\mathcal{V}$ is finitely based.

A variety $\mathcal{V}$ has **definable principal subcongruence** provided there is a congruence formula $\Gamma(u, v, x, y)$ such that for any $\mathbf{A} \in \mathcal{V}$ and any $a, b \in A$ with $a \neq b$ there are $c, d \in A$ with $c \neq d$ such that

1. $\mathbf{A} \models \Gamma(c, d, a, b)$, and
2. $\Gamma(u, v, c, d)$ defines $\mathrm{Cg}^{\mathbf{A}}(c, d)$.

A Theorem of Baker and Wang (2000)

If $\mathcal{V}$ is a locally finite variety wtih definable principal subcongruences and $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatizable, then $\mathcal{V}$ is finitely based.

A Theorem of McNulty and Wang (2000)

If $\mathcal{V}$ is a variety generated by some finite group, then $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatizable.

Some Infinite Nonfinitely Based Algebras

The natural numbers endowed with addition, multiplication, and exponentiation (Martin 1973);

Some Infinite Nonfinitely Based Algebras

The natural numbers endowed with addition, multiplication, and exponentiation (Martin 1973);

The natural numbers endowed with addition, multiplication, exponentiation, and 1 (Gurevič 1990);

Some Infinite Nonfinitely Based Algebras

The natural numbers endowed with addition, multiplication, and exponentiation (Martin 1973);

The natural numbers endowed with addition, multiplication, exponentiation, and 1 (Gurevič 1990);

Certain infinite groups (Ol'shanskiĭ 1970);

Some Infinite Nonfinitely Based Algebras

The natural numbers endowed with addition, multiplication, and exponentiation (Martin 1973);

The natural numbers endowed with addition, multiplication, exponentiation, and 1 (Gurevič 1990);

Certain infinite groups (Ol'shanskiĭ 1970);

Certain infinite lattices (Baker, Herrmann, McKenzie circa 1970):

Inherently Nonfinitely Based Varieties

A variety $\mathcal{V}$ is said to be **inherently nonfinitely based** provided

- $\mathcal{V}$ is locally finite, and
- $\mathcal{V}$ is included in no finitely based locally finite variety.

Inherently Nonfinitely Based Varieties

A variety $\mathcal{V}$ is said to be **inherently nonfinitely based** provided

- $\mathcal{V}$ is locally finite, and
- $\mathcal{V}$ is included in no finitely based locally finite variety.

A variety $\mathcal{V}$ is inherently nonfinitely based provided

- $\mathcal{V}$ is locally finite, and
- for infinitely many natural numbers n there are finitely generated infinite algebras $\mathbf{B}_n$ such that each n-generated subalgebra of $\mathbf{B}_n$ belongs to $\mathcal{V}$.

Inherently Nonfinitely Based Algebras

Many of the known nonfinitely based finite algebras have turned out to be inherently nonfinitely based, although this does not apply to Lyndon's original example, nor to Bryant's pointed group.

Inherently Nonfinitely Based Algebras

Many of the known nonfinitely based finite algebras have turned out to be inherently nonfinitely based, although this does not apply to Lyndon's original example, nor to Bryant's pointed group.

In 1989 Baker, McNulty, and Werner described a general method for proving that certain finite algebras are inherently nonfinitely based.

In 1987, Mark Sapir gave an algorithm for deciding which finite semigroups are inherently nonfinitely based.

In 1987, Mark Sapir gave an algorithm for deciding which finite semigroups are inherently nonfinitely based.

In 1989, Isaev constructed for each finite field $\mathbf{k}$ a 5 dimensional $\mathbf{k}$ algebra which is inherently nonfinitely based.

Infinite Inherently Nonfinitely Based Algebras

In 2002, Freese McNulty, and Nation gave a general method for contructing inherently nonfinitely based lattices. We also showed that McKenzie's example of a nonfinitely based lattice fails to be inherently nonfinitely based.

Infinite Inherently Nonfinitely Based Algebras

In 2002, Freese McNulty, and Nation gave a general method for contructing inherently nonfinitely based lattices. We also showed that McKenzie's example of a nonfinitely based lattice fails to be inherently nonfinitely based.

Is there an inherently nonfinitely based modular lattice?

Infinite Inherently Nonfinitely Based Algebras

In 2002, Freese McNulty, and Nation gave a general method for contructing inherently nonfinitely based lattices. We also showed that McKenzie's example of a nonfinitely based lattice fails to be inherently nonfinitely based.

Is there an inherently nonfinitely based modular lattice?

Is there an inherently nonfinitely based group?

The Finite Algebra Membership Problem

Given a variety $\mathcal{V}$ every finite algebra $\mathbf{B}$ gives an instance of the Finite Algebra Membership Problem of $\mathcal{V}$:

Does $\mathbf{B}$ belong to $\mathcal{V}$?

We can specify this problem to a finite algebra $\mathbf{A}$ so that the instance of the problem associated with $\mathbf{B}$ becomes:

Does $\mathbf{B}$ belong to the variety generated by $\mathbf{B}$

Computational complexity problems like this were promoted in the wonderful and thorough survey of Kharlampovich and Sapir 1995.

Complexity of the Finite Algebra Membership Problem

For any finitely based finite algebra $\mathbf{A}$, the finite algebra membership problem of $\mathbf{A}$ is of polynomial time complexity.

Complexity of the Finite Algebra Membership Problem

For any finitely based finite algebra $\mathbf{A}$, the finite algebra membership problem of $\mathbf{A}$ is of polynomial time complexity.

In 1998 Zoltan Szekely found a small algebra $\mathbf{A}$ whose finite algebra membership problem is NP-complete.

Complexity of the Finite Algebra Membership Problem

For any finitely based finite algebra $\mathbf{A}$, the finite algebra membership problem of $\mathbf{A}$ is of polynomial time complexity.

In 1998 Zoltan Szekely found a small algebra $\mathbf{A}$ whose finite algebra membership problem is NP-complete.

The niave algorithm for solving finite algebra membership problems displays at least double exponential time complexity.

Is there a finite algebra $\mathbf{A}$ whose finite algebra membership problem is exponentially hard?

The Equational Complexity of a Variety

With every variety $\mathcal{V}$ we associate a function $\beta_{\mathcal{V}}$ on the positive integers so that $\beta_{\mathcal{V}}(n)$ is the least positive integer k such that for every algebra $\mathbf{B}$ with exactly n elements

$$\mathbf{B} \in \mathcal{V}$$

if and only if

every equation of length no more than k which is true in $\mathcal{V}$ is true in $\mathbf{B}$.

The function $\beta_{\mathcal{V}}$ is called the equational bound of $\mathcal{V}$. By the equational bound $\beta_{\mathbf{A}}$ of the algebra $\mathbf{A}$ we mean the equational bound of the variety generated by $\mathbf{A}$.

If $\mathcal{V}$ is finitely based, then $\beta_{\mathcal{V}}$ is dominated by a constant function.

If $\mathcal{V}$ is finitely based, then $\beta_{\mathcal{V}}$ is dominated by a constant function.

Problem 1A: If $\mathbf{A}$ is a finite algebra and $\beta_{\mathbf{A}}$ is dominated by a constant function, then must $\mathbf{A}$ be finitely based?

If $\mathcal{V}$ is finitely based, then $\beta_{\mathcal{V}}$ is dominated by a constant function.

Problem 1A: If $\mathbf{A}$ is a finite algebra and $\beta_{\mathbf{A}}$ is dominated by a constant function, then must $\mathbf{A}$ be finitely based?

If $\mathbf{A}$ is a finite algebra and $\beta_{\mathbf{A}}$ is dominated by a constant function, then either $\mathbf{A}$ is finitely based or else it is inherently nonfinitely based.

In 1998 Zoltan Szekely produced a number of small finite algebras whose equational bounds eventually dominate every sublinear function.

In 1998 Zoltan Szekely produced a number of small finite algebras whose equational bounds eventually dominate every sublinear function.

Is there a finite algebra whose equational bound eventually dominates a linear function? How fast can such functions grow?