Inherently Nonfinitely Based Solvable Algebras

Keith Kearnes Ross Willard*

Revised September 1993

Abstract

We prove that an inherently nonfinitely based algebra cannot generate an abelian variety. On the other hand, we show by example that it is possible for an inherently nonfinitely based algebra to generate a strongly solvable variety.

1 Introduction

Let \mathbf{A} be an algebra with finitely many basic operations and let $\Sigma(\mathbf{A})$ denote the set of equations true in \mathbf{A} . \mathbf{A} is said to be **finitely based** if there is a finite subset $\Sigma_0 \subseteq \Sigma(\mathbf{A})$ such that Σ_0 and Σ have the same models. Otherwise, \mathbf{A} is said to be **nonfinitely based**. A variety of finite type is said to be **finitely based** or **nonfinitely based** according to whether or not it is the class of models of some finite set of equations. By a result of Birkhoff [3], \mathbf{A} is finitely based if and only if the variety it generates, $\mathcal{V}(\mathbf{A})$, is finitely based.

A is said to be **inherently nonfinitely based** if it is finite but is not a member of any locally finite, finitely based variety. Since $\mathcal{V}(\mathbf{A})$ is locally finite if **A** is finite, an inherently nonfinitely based algebra is always nonfinitely based.

The property of being inherently nonfinitely based is more stable than the property of being merely nonfinitely based. For example, suppose that \mathbf{A} and

^{*}Research supported by a grant from NSERC.

¹AMS subject classification: Primary: 08B05.

²Key words and phrases: algebra, variety, inherently nonfinitely based, Hamiltonian, strongly solvable.

B are finite algebras with $\Sigma(\mathbf{B}) \subseteq \Sigma(\mathbf{A})$. If **A** is inherently nonfinitely based, then **B** is, too. On the other hand, whether **B** is finitely based is independent of whether **A** is finitely based. For another example of the relative stability of the inherent nonfinite basis property we refer the reader to [4]. There it is shown that even when **A** is finitely based, an expansion of **A** obtained by adding one new constant to the language of **A** may be nonfinitely based. But no such expansion can be inherently nonfinitely based.

An algebra \mathbf{A} is said to be **abelian** if there exists an equivalence relation on the set $A \times A$ which (i) is compatible with the fundamental operations of \mathbf{A} (applied coordinatewise), and (ii) has the set $\{(a, a) : a \in A\}$ as a single equivalence class. The results of this paper are motivated by Problem 3 of [5] which asks whether there is a finite abelian algebra which is nonfinitely based. We do not know the answer to this question. What we prove here is that if every member of $\mathcal{V}(\mathbf{A})$ is abelian, then \mathbf{A} cannot be inherently nonfinitely based. On the other hand, we give an example of an inherently nonfinitely based algebra, \mathbf{G}_3^* , such that $\mathcal{V}(\mathbf{G}_3^*)$ is 2-step strongly solvable.

2 Hamiltonian Varieties

An algebra \mathbf{A} is said to be **Hamiltonian** if every nonempty subuniverse of \mathbf{A} is a class of some congruence of \mathbf{A} . A variety is Hamiltonian if every member is. If $\mathbf{A} \times \mathbf{A}$ is Hamiltonian, then clearly \mathbf{A} is abelian; hence every Hamiltonian variety is abelian. Conversely, Kiss and Valeriote [7] have proved that if a variety is abelian and locally finite, then it is Hamiltonian.

Theorem 1 (Klukovits, [8]) A variety \mathcal{V} is Hamiltonian if and only if, for every term $t(x, \bar{z})$ in the language of \mathcal{V} , there is a ternary term g^t such that \mathcal{V} satisfies the equation

$$g^t(t(x,\bar{z}),x,y) = t(y,\bar{z}). \quad \Box$$

The term g^t from the previous theorem is called a **Klukovits term** for t (at x), and also a Klukovits term for \mathcal{V} . Observe that if \mathcal{V} is Hamiltonian, $t(x, y, \bar{z})$ is a term and g^t is a Klukovits term for t at x, then $t(x, y, \bar{z}) =$

 $g^t(t(y, y, \bar{z}), y, x)$ is an equation of \mathcal{V} . From this we get that if t depends on both x and y, then t is \mathcal{V} -equivalent to a term constructible from g^t and a term $t(y, y, \bar{z})$ depending on fewer distinct variables than t depends on. Thus, any term is \mathcal{V} -equivalent to a term composed from a unary term and Klukovits terms.

Lemma 2 If \mathcal{V} is a Hamiltonian variety and $|F_{\mathcal{V}}(3)| = n < \omega$, then for each $\mathbf{A} \in \mathcal{V}$ and each $a, b \in A$ the integer n is a bound on the size of the $\operatorname{Cg}^{A}(a, b)$ -blocks.

Proof: Quasi-order A by \leq where $x \leq y$ if $x \in \text{Sg}^A(a, b, y)$. Define an equivalence relation $\theta = \{(x, y) \in A \times A | x \leq y \text{ and } y \leq x\}$. For each $y \in A$ the set $\{x \in A | x \leq y\}$ has cardinality at most n, so the θ -equivalence classes have at most n-elements each. We now proceed to show that $\text{Cg}^A(a, b) \subseteq \theta$ which will finish the proof.

Choose $(c, d) \in \operatorname{Cg}^A(a, b)$. Since the universe of $\mathbf{S} = \operatorname{Sg}^A(a, b, c)$ is a block of a congruence γ on \mathbf{A} and $a, b \in S$, it follows that $(c, d) \in \operatorname{Cg}^A(a, b) \subseteq \gamma$. Hence d belongs to the γ -class containing c and that class is just S. Therefore $d \in \operatorname{Sg}^A(a, b, c)$ and $d \leq c$. Similarly, $c \leq d$ and so $(c, d) \in \theta$. Since $(c, d) \in \operatorname{Cg}^A(a, b)$ was chosen arbitrarily, $\operatorname{Cg}^A(a, b) \subseteq \theta$. \Box

Theorem 3 (Berman, [2]) A Hamiltonian variety whose 3-generated free algebra is finite is locally finite.

Proof: A Hamiltonian variety is equivalent to a variety whose basic operations have arity ≤ 3 since the clone of a Hamiltonian variety is generated by its unary terms and its 3-variable Klukovits terms. Therefore, without loss of generality, we may assume that our variety has finitely many basic operations.

Assume now that \mathcal{V} is a 3-finite, Hamiltonian variety with finitely many basic operations which is not locally finite. We will show that this assumption leads to a contradiction. \mathcal{V} contains a finitely generated, infinite algebra **B**. Any congruence on **B** of finite index is compact, because it is the kernel of a homomorphism from a finitely generated algebra onto a finitely presentable algebra. Hence the set of congruences on **B** of infinite index is closed under unions of chains. Now we use Zorn's Lemma to find a maximal congruence $\theta \in \text{Con } \mathbf{B}$ of infinite index. Then $\mathbf{A} = \mathbf{B}/\theta$ is a finitely generated, infinite member of \mathcal{V} with the property that \mathbf{A}/α is finite whenever $\alpha > 0$. Choose distinct $a, b \in A$. Since $\mathbf{A}/\text{Cg}^A(a, b)$ is finite, $\text{Cg}^A(a, b)$ has only finitely many congruence classes. Each class has $\leq |F_{\mathcal{V}}(3)|$ elements. But this is impossible if A is infinite. The assumption on which the construction of \mathbf{A} was based was the assumption that \mathcal{V} is not locally finite and so we have proved the theorem. \Box

Remark: In fact, Berman shows that $|F_{\mathcal{V}}(n)| \leq (|F_{\mathcal{V}}(3)|)^{n-2}$ for $n \geq 3$.

Lemma 4 A Hamiltonian variety of finite type with definable principal congruences is contained in a finitely based Hamiltonian variety.

Proof: Let \mathcal{V} be a Hamiltonian variety with definable principal congruences. This means there is a finite set of formulas $\Pi = \{\pi_i(x, y; u, v) | i \in I\}$ each of the form

$$\exists \bar{z} \left[(x = p_1(r_1, \bar{z})) \land \left(\bigwedge_{j=1}^{n-1} (p_j(r'_j, \bar{z}) = p_{j+1}(r_{j+1}, \bar{z})) \right) \land (p_n(r'_n, \bar{z}) = y) \right]$$

where $\{r_j, r'_j\} = \{u, v\}$ for all j, such that for each $\mathbf{A} \in \mathcal{V}$ we have $(a, b) \in \operatorname{Cg}^A(c, d)$ iff $\pi_i(a, b; c, d)$ for some $i \in I$. Define ϕ to be the formula $\bigvee_{i \in I} \pi_i$. Let Ψ be a sentence asserting that for all c and d, $\{(a, b) | \phi(a, b; c, d)\}$ is a congruence containing (c, d). (There is such a sentence since \mathcal{V} is of finite type.) By compactness, there is a finitely based supervariety $\mathcal{W} \supseteq \mathcal{V}$ where Ψ holds. \mathcal{W} has definable principal congruences and, in fact, ϕ is a formula which defines principal congruences in \mathcal{W} .

For each $i \in I$ and each p_j occuring in π_i there is a Klukovits term g_{ij} for p_j . \mathcal{V} satisfies the equation

$$g_{ij}(p_i(x,\bar{z}),x,y) = p_i(y,\bar{z}).$$

Let \mathcal{U} be the subvariety of \mathcal{W} which is axiomatized by these equations and the equations of \mathcal{W} . \mathcal{U} is finitely based, has ϕ as a formula which defines principal congruences and contains \mathcal{V} . We proceed to show that \mathcal{U} is Hamiltonian.

Suppose that $\mathbf{A} \in \mathcal{U}$ and that *B* is a nonempty subuniverse of \mathbf{A} . Let $\beta = \operatorname{Cg}^{A}(B \times B)$. If *B* is the union of all the $\operatorname{Cg}^{A}(c, d)$ -blocks for $c, d \in B$, then *B*

is a β -block. Therefore, if B is not a β -block, then we can find $c, d \in B$ and $(a, b) \in \operatorname{Cg}^A(c, d)$ with $a \in B$ and $b \in A - B$. Since $\phi(a, b; c, d)$ holds there must exist an $i \in I$, a p_j occurring in π_i and a $\overline{z} \in A^m$ such that $p_j(c, \overline{z}) \in B$ and $p_j(d, \overline{z}) \notin B$ (or else the same condition with c and d switched). But $p_j(d, \overline{z}) = g_{ij}(p_j(c, \overline{z}), c, d)$, which is in B since B is a subuniverse containing $p_j(c, \overline{z}), c$ and d. This contradiction shows that B is a congruence block and, since \mathbf{A} and B were arbitrary, that \mathcal{U} is Hamiltonian. \Box

Theorem 5 Every locally finite, abelian variety with finitely many basic operations is contained in a finitely based, locally finite, abelian variety.

Proof: If \mathcal{V} is locally finite and abelian, then it is Hamiltonian by the principal result of [7]. [6] proves that \mathcal{V} has the congruence extension property. Therefore, by the results in [1], \mathcal{V} has definable principal congruences. Now we are in a position to apply Lemma 4. We may conclude that \mathcal{V} is contained in a finitely based Hamiltonian variety \mathcal{U} . \mathcal{U} has a finitely based subvariety, \mathcal{W} , containing \mathcal{V} and such that $\mathbf{F}_{\mathcal{W}}(3)$ is finite. \mathcal{W} is finitely based, Hamiltonian (therefore abelian), and locally finite by Theorem 3. \Box

Corollary 6 An abelian variety contains no inherently nonfinitely based members. \Box

3 An Inherently Nonfinitely Based Strongly Solvable Algebra

If **A** is an algebra with congruences α, β satisfying $\alpha < \beta$, then β is said to be **strongly abelian over** α if for all (n + 1)-ary polynomial operations p of **A** and all $a \stackrel{\beta}{\equiv} b$ and $c_i \stackrel{\beta}{\equiv} d_i \stackrel{\beta}{\equiv} e_i$, $1 \le i \le n$,

$$p(a, \bar{c}) \stackrel{\alpha}{\equiv} p(b, \bar{d})$$
 implies $p(a, \bar{e}) \stackrel{\alpha}{\equiv} p(b, \bar{e})$.

If the implication is replaced by $p(a, \bar{c}) \stackrel{\alpha}{\equiv} p(a, \bar{d})$ implying $p(b, \bar{c}) \stackrel{\alpha}{\equiv} p(b, \bar{d})$, then β is said to be **abelian** over α . It is known that the strongly abelian property implies the abelian property but not conversely, and that \mathbf{A} is abelian (as defined in the Introduction) if and only if 1_A is abelian over 0_A (for more details, see [5]).

A is said to be *m*-step strongly solvable if there exist congruences $0_A = \alpha_0 < \alpha_1 < \cdots < \alpha_m = 1_A$ with α_{i+1} strongly abelian over α_i for all i < m. By a groupoid we mean an algebra consisting of a set with one binary operation. In this section we shall construct a finite 2-step strongly solvable groupoid which is inherently nonfinitely based.

Lemma 7 Any groupoid satisfying (xy)z = (uv)w is 2-step strongly solvable.

Proof: Let **A** be a groupoid satisfying (xy)z = (uv)w. Let $C = \{ab : a, b \in A\}$ and $\mu = C^2 \cup 0_A$. Clearly μ is a congruence of **A** and 1_A is strongly abelian over μ , because multiplication in **A** is constant modulo μ .

Next, suppose that $s(\bar{x}, \bar{y})$ and $t(\bar{x}, \bar{y})$ are (n+m)-ary groupoid terms and $\bar{a} \in A^m$. Let $f(\bar{x})$ and $g(\bar{x})$ denote the restrictions to C^n of the polynomial operations $s^{\mathbf{A}}(\bar{x}, \bar{a})$ and $t^{\mathbf{A}}(\bar{x}, \bar{a})$ respectively, and let $h(\bar{x}) = f(\bar{x}) \cdot g(\bar{x})$. Observe that if h is nonconstant (as a function $C^n \to C$), then necessarily g is also nonconstant, s is a variable y_i , and $a_i \in A \setminus C$. Therefore, an n-ary polynomial operation of \mathbf{A} whose restriction to C^n is nonconstant must have the form $a_1(a_2(\cdots a_{r-1}(a_rx_j)\cdots))$ with $a_i \in A \setminus C$.

We now prove that μ is strongly abelian over 0_A . Suppose p is an (n+1)ary polynomial operation of \mathbf{A} , that $a \stackrel{\mu}{\equiv} b$ and $c_i \stackrel{\mu}{\equiv} d_i \stackrel{\mu}{\equiv} e_i$ for $1 \leq i \leq n$, and that $p(a, \bar{c}) = p(b, \bar{d})$ while $p(a, \bar{e}) \neq p(b, \bar{e})$. Obviously $a \neq b$ and hence $a, b \in C$ (as $a \stackrel{\mu}{\equiv} b$). Since we are allowing p to be a polynomial operation, we can assume that $|\{c_i, d_i, e_i\}| \geq 2$ and hence $c_i, d_i, e_i \in C$ for each i. Therefore, the restriction of p to C^{n+1} is nonconstant. But then p can depend on only one variable, contradicting the above assumptions. \Box

We next define a nice class of groupoids satisfying (xy)z = (uv)w. Suppose V is a nonempty set, S is a set of partial maps $V \to V$, W^* is a set disjoint from V, and $f : W^* \to S$ is a surjective map, written $x \mapsto f_x$. Choose $\infty \notin V \cup W^*$. Define a groupoid $\mathbf{A} = \langle A, \cdot \rangle$ as follows.

$$A = V \cup W^* \cup \{\infty\}$$

$$x \cdot y = \begin{cases} f_x(y) & \text{if } x \in W^* \text{ and } y \in \text{dom}(f_x) \\ \infty & \text{otherwise.} \end{cases}$$

Clearly $\mathbf{A} \models (xy)z = (uv)w$. Moreover, the equational theory of \mathbf{A} is tractable. Let us say that a groupoid term is **nontrivial** if it is a variable or a rightassociated product of variables in which the right-most variable occurs only once, and is **trivial** otherwise. If x_1, x_2, \ldots, x_n $(n \ge 1)$ are (not necessarily distinct) variables, w is the semigroup word $x_1x_2\cdots x_n$, and y is a variable not occurring in w, then we use [w, y] to denote the nontrivial groupoid term $x_1(x_2(\cdots(x_ny)\cdots))$. The proof of the next lemma is straightforward.

Lemma 8 Suppose \mathbf{A} is the groupoid defined above from the data V, S, W, f. Suppose further that some $\sigma \in S$ has a fixed point. Let $\operatorname{Partial}(V)$ be the semigroup of all partial maps $V \to V$ under composition. Then for any groupoid terms s and t, $\mathbf{A} \models s = t$ if and only if one of the following is true:

- (1) s and t are both trivial;
- (2) s and t are the same variable;
- (3) s = [w, y] and t = [w', y] where w and w' are nonempty semigroup words in n variables, y is a variable not occurring in w or w', and Partial(V) $\models w(\bar{\sigma}) = w'(\bar{\sigma})$ for all $\bar{\sigma} \in S^n$.

Now we come to our construction, which is a simple variation of a construction due to Shallon [9]. By a **graph** we mean a pair G = (V, E) where Vis a nonempty set and E is a symmetric binary relation on V. If G = (V, E)is a graph, let $V^* = \{v^* : v \in V\}$ be a set disjoint from V and in bijective correspondence with V via $v \mapsto v^*$, and let \mathbf{G}^* be a groupoid with universe

$$G^* = V \cup V^* \cup \{\infty\}$$

(where $\infty \notin V \cup V^*$), in which multiplication is given by

$$a^* \cdot b = a$$
 if $a, b \in V$ and aEb
 $x \cdot y = \infty$ in all other cases.

We call \mathbf{G}^* a graph *-algebra. We say that G and \mathbf{G}^* are looped if E is reflexive. Observe that every looped graph *-algebra is of the kind described in Lemma 8.

If w is any nonempty semigroup word built from variables, define

- V(w) = the set of variables occurring in w
- $E(w) = \{ (x, x') : x, x' \in V(w), x \neq x', \text{ and } xx' \text{ or } x'x \text{ is a subword of } w \}$
- L(w) = the left-most variable in w
- R(w) = the right-most variable in w

 $Data(w) = \langle V(w), E(w), L(w), R(w) \rangle$

Also let $G_3 = (V, E)$ be the graph with $V = \{0, 1, 2\}$ and $E = V^2 \setminus \{(0, 2), (2, 0)\}$. The proof of the next lemma is straightforward, and is similar to the proofs of Theorems 1(*i*) and 2' in [9].

Lemma 9 Suppose G is a looped graph.

- (1) If $\mathbf{G}^* \models s = t$, then either s,t are both trivial or s,t are the same variable or s = [w, y] and t = [w', y] for some w, w', y.
- (2) Suppose w, w' are words and y is a variable occurring in neither w nor w'. If Data(w) = Data(w') then $\mathbf{G}^* \models [w, y] = [w', y]$.
- (3) If $G = G_3$ then the converse to item (2) is true.
- (4) If G is connected, has more than one vertex, and no two vertices of G have the same neighborhood, then G* is subdirectly irreducible with monolith μ defined in Lemma 7.

The following corollary may be of independent interest (cf. [5], Problem 5).

Corollary 10 $V(\mathbf{G}_3^*)$ is 2-step strongly solvable, contains all looped graph *-algebras, and is residually large. There is no cardinal upper bound to the sizes of the blocks of the monoliths of subdirectly irreducible members of $V(\mathbf{G}_3^*)$.

Finally, following [9] we prove

Theorem 11 \mathbf{G}_3^* is inherently nonfinitely based.

Proof: We shall display, for each n > 0, a nonlocally finite groupoid \mathbf{B}_n which satisfies all of the *n*-variable equations true in \mathbf{G}_3^* . (This will suffice, since if \mathcal{W} is a finitely based variety which contains \mathbf{G}_3^* , then \mathcal{W} will also contain \mathbf{B}_n for sufficiently large n, so \mathcal{W} will not be locally finite.) Let

$$W = \{0, 1, 2, \dots, n\}$$

$$W^* = \{0^*, 1^*, \dots, n^*\}$$

$$E = \{(a, b) \in W^2 : a - b \equiv -1, 0 \text{ or } +1 \pmod{n+1}\}$$

$$G = (W, E).$$

Thus G is a looped (n+1)-cycle. Define \mathbf{B}_n to be the groupoid whose universe is $Z \cup W^* \cup \{\infty\}$ and in which multiplication is given by: if $a \in W$ and $b \in Z$, then

$$a^* \cdot b = \begin{cases} b-1 & \text{if } a \equiv b-1 \pmod{n+1} \\ b & \text{if } a \equiv b \pmod{n+1} \\ b+1 & \text{if } a \equiv b+1 \pmod{n+1} \end{cases}$$

while $x \cdot y = \infty$ in all other cases.

Clearly \mathbf{B}_n is infinite but is generated by the finite subset $W^* \cup \{0\}$, and hence is not locally finite. Note that \mathbf{B}_n is a groupoid of the kind described in Lemma 8. Suppose that $s(x_1, \ldots, x_n)$ and $t(x_1, \ldots, x_n)$ are two groupoid terms in the specified variables such that $\mathbf{G}_3^* \models s = t$. We wish to show that $\mathbf{B}_n \models s = t$. By Lemmas 8 and 9, it suffices to consider the case when s = [w, y] and t = [w', y] where $y = x_n$ and w, w' are nonempty words satisfying $\operatorname{Data}(w) = \operatorname{Data}(w')$ and $V(w) = \{x_1, \ldots, x_{n-1}\}$. Let $L(w) = x_l$ and $R(w) = x_r$. Let $\alpha_1, \ldots, \alpha_n \in B_n$ be given. If $\alpha_i \notin W^*$ for some $i = 1, \ldots, n-1$, or if $\alpha_n \notin Z$, then $s^{\mathbf{B}_n}(\bar{\alpha}) = \infty = t^{\mathbf{B}_n}(\bar{\alpha})$. Suppose $\alpha_i = a_i^* \in W^*$ for $1 \leq i < n$ and $\alpha_n = c \in Z$. Choose $a_n \in W$ so that $c \equiv a_n$ (mod n + 1). If for some $(x_i, x_j) \in E(w)$ it happens that $(a_i, a_j) \notin E$, or if $(a_r, a_n) \notin E$, then $again s^{\mathbf{B}_n}(\bar{\alpha}) = \infty = t^{\mathbf{B}_n}(\bar{\alpha})$.

Finally, suppose that $(a_i, a_j) \in E$ whenever $(x_i, x_j) \in E(w)$, and that $(a_r, a_n) \in E$. We argue as in [9]. Since |W| = n + 1, there exists $b \in W$ such that $b \notin \{a_1, \ldots, a_n\}$; say $0 \notin \{a_1, \ldots, a_n\}$. The word wx_n (read right-to-left) together with the assignment $x_i \mapsto a_i$ describe a path in G from a_n to a_l . This path never passes through the vertex 0, that is, it is restricted to the

looped n-chain which is obtained from G be deleting 0. It follows that

$$s^{\mathbf{B}_n}(a_1^*,\ldots,a_{n-1}^*,c) = a_l + (c-a_n).$$

Since Data(w) = Data(w') the same argument shows that

$$t^{\mathbf{B}_n}(a_1^*,\ldots,a_{n-1}^*,c) = a_l + (c-a_n).$$

Thus $\mathbf{B}_n \models s = t$ as desired. \Box

References

- J.T. Baldwin and J. Berman, The number of subdirectly irreducible algebras in a variety, Algebra Universalis 5 (1975), 379–389.
- [2] J. Berman, Varieties with log-linear free spectra, manuscript, 1984.
- [3] G. Birkhoff, On the structure of abstract algebras, Proc. Camb. Philos. Soc. 31, 433–454.
- [4] R. Bryant, The laws of finite pointed groups, Bull. London Math. Soc. 14 (1982), 119-123.
- [5] D. Hobby and R. McKenzie, The Structure of Finite Algebras, Contemporary Mathematics AMS, 76, 1988.
- [6] E.W. Kiss, Each Hamiltonian variety has the congruence extension property, Algebra Universalis 12 (1981), 395–398.
- [7] E.W. Kiss and M. Valeriote, Abelian algebras and the Hamiltonian property, J. Pure and Applied Algebra 87 (1993), 37–49.
- [8] L. Klukovits, Hamiltonian varieties of universal algebras, Acta. Sci. Math. 37 (1975), 11–15.
- [9] G. F. McNulty and C. R. Shallon, Inherently nonfinitely based finite algebras, in R. S. Freese and O. C. Garcia, eds., Universal Algebra and Lattice Theory, Lecture Notes in Mathematics no. 1004, Springer-Verlag (1983), 206-231.

Department of Mathematics Harvey Mudd College Claremont, CA 91711, USA Department of Pure Mathematics University of Waterloo Waterloo, Ontario, Canada N2L 3G1