Finiteness Properties of Locally Finite Abelian Varieties

Keith A. Kearnes Ross D. Willard *

Abstract

We show that any locally finite abelian variety is generated by a finite algebra. We solve a problem posed by D. Hobby and R. McKenzie by exhibiting a nonfinitely based finite abelian algebra.

1 Introduction

A *variety* of algebras is an equationally definable class of algebras in a fixed language. A variety $\mathcal{V}$ is said to be *locally finite* if its finitely generated algebras are finite. An algebra $\mathbf{A}$ is *abelian* if it satisfies all sentences of the form

$$\forall \mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{u}(t(\mathbf{x}, \mathbf{u}) = t(\mathbf{x}, \mathbf{v}) \Longrightarrow t(\mathbf{y}, \mathbf{u}) = t(\mathbf{y}, \mathbf{v}))$$

where $t(\mathbf{x}, \mathbf{y})$ is an $(m+n)$–ary term in the language of $\mathbf{A}$. A variety of algebras is said to be abelian if all of its members are abelian.

For any ring $\mathbf{R}$ the variety of left $\mathbf{R}$–modules is abelian. For any monoid $\mathbf{M}$ the variety of left $\mathbf{M}$–sets is abelian. A variety of $\mathbf{R}$–modules is locally finite if and only if $\mathbf{R}$ is finite while a variety of $\mathbf{M}$–sets is locally finite if and only if $\mathbf{M}$ is finite. These two types of examples are fundamental, since it is shown in [1] that the polynomial structure of any finite abelian algebra is locally like that of an $\mathbf{R}$–module or an $\mathbf{M}$–set. Therefore it is natural to wonder if one can associate to each locally finite abelian variety $\mathcal{V}$ a finite structure, of which a ring or a monoid is a special case, which acts on the members of $\mathcal{V}$ and which 'determines' $\mathcal{V}$ in some sense. If such were the case, then we would expect a locally finite abelian variety to share the finiteness properties of locally finite varieties of $\mathbf{R}$–modules and $\mathbf{M}$–sets. For example, since a subvariety of a variety of $\mathbf{R}$–modules (or $\mathbf{M}$–sets) may be identified with a variety of $\mathbf{R}'$–modules ($\mathbf{M}'$–sets) where $\mathbf{R}'$ ($\mathbf{M}'$) is a quotient of $\mathbf{R}$ ($\mathbf{M}$), it follows that a variety of either type has finitely many subvarieties. This implies that either type of variety is finitely generated and, with a little extra argument, that either type of variety is finitely based. If to each locally finite abelian variety we could associate a finite structure which determined the variety, we would expect every locally finite abelian variety to be finitely generated, finitely based and to have a finite subvariety lattice.

*Research supported by NSERC.

In the first part of this paper we prove that any locally finite abelian variety is finitely generated. In the second part we then give an example to show that a locally finite abelian variety need not be finitely based (and therefore need not have a finite subvariety lattice). By the first part of the paper, the variety of the second part is generated by a finite abelian algebra. Therefore the results contained in this paper answer in the negative Problem 3 from the book [1] of D. Hobby and R. McKenzie which asks:

> If $\mathbf{A}$ is a finite abelian algebra of finite type, is $\mathcal{V}(\mathbf{A})$ finitely axiomatizable?

The nonfinitely based abelian algebra which we construct generates an abelian variety. By a result of [2] any such algebra fails to be inherently nonfinitely based. It remains open whether there is a finite abelian algebra which is inherently nonfinitely based.

2 Finite Generation

In this section we will prove that every locally finite abelian variety is generated by a finite algebra. We begin by making some general remarks about what it means for a variety to be generated by a finite algebra.

Let $\mathcal{V}$ be a variety. Any equation in the language of $\mathcal{V}$ may be written (after possibly renaming variables and adding 'fictitious variables') as $s(\mathbf{x}, y) = t(\mathbf{x}, y)$ where s and t are $(n+1)$–ary term operations, $\mathbf{x} = (x_1, \ldots, x_n)$ is a sequence of distinct variables and y is a distinguished variable not in the sequence $\mathbf{x}$. We shall consider only equations of this form. The *rank* of the equation $s(\mathbf{x}, y) = t(\mathbf{x}, y)$ is defined to be the length of the sequence $\mathbf{x}$. (Observe that by adding a fictitious variable to this equation we change its rank, so we consider the modified equation to be different from the original equation.) An equation $s(\mathbf{x}, y) = t(\mathbf{x}, y)$ is *falsifiable* in $\mathcal{V}$ if there is some $\mathbf{A} \in \mathcal{V}$ and a tuple $(\mathbf{a}, b) \in A^{n+1}$ such that $s(\mathbf{a}, b) \neq t(\mathbf{a}, b)$. That is, an equation is falsifiable if it is not an equation of $\mathcal{V}$. A *minimal falsifiable equation* is a falsifiable equation $s(\mathbf{x}, y) = t(\mathbf{x}, y)$ which is no longer falsifiable if two variables are set equal.

LEMMA 2.1 *A variety is finitely generated if and only if it is locally finite and there is a finite bound on the rank of any minimal falsifiable equation.*

Proof. Assume that $\mathcal{V} = \mathcal{V}(\mathbf{A})$ where $\mathbf{A}$ is finite. It is well known that the variety generated by a finite algebra is locally finite. Choose a minimal falsifiable equation $s = t$. Since $\mathbf{A}$ generates $\mathcal{V}$ and $s = t$ is a minimal falsifiable equation, we can falsify $s = t$ by a substitution of distinct elements of A into the distinct variables of the equation. This implies that the number of variables in the equation $s = t$ does not exceed $|A|$, and therefore the rank of $s = t$ is $< |A|$. Hence $|A|$ is a finite bound on the rank of any minimal falsifiable equation.

Conversely, assume that $\mathcal{V}$ is a locally finite variety and that N is a finite bound on the rank of any minimal falsifiable equation. Then $\mathbf{F}_{\mathcal{V}}(N)$ is a finite algebra which satisfies all the equations of $\mathcal{V}$ and fails all the equations that can be falsified in $\mathcal{V}$. Thus, $\mathcal{V} = \mathcal{V}(\mathbf{F}_{\mathcal{V}}(N))$. □

From now on $\mathcal{A}$ will denote a fixed but arbitrarily chosen locally finite abelian variety. It is our goal to prove that there is a finite bound on the rank of any minimal falsifiable equation in the language of $\mathcal{A}$. First we explain a reduction. Let δ be a unary term in the language of $\mathcal{A}$ and let $\mathcal{E}_\delta$ denote the set of equations $s(\mathbf{x}, y) = t(\mathbf{x}, y)$ in the language of $\mathcal{A}$ for which

$$\mathcal{A} \models s(y, y, \ldots, y) = \delta(y) = t(y, y, \ldots, y).$$

Clearly, if $\mathcal{A} \models \delta(y) = \delta'(y)$, then $\mathcal{E}_\delta = \mathcal{E}_{\delta'}$. Therefore, since $\mathcal{A}$ has only finitely many unary terms up to equivalence, there are only finitely many different sets of the form $\mathcal{E}_\delta$. Furthermore, if $s(\mathbf{x}, y) = t(\mathbf{x}, y)$ is any minimal falsifiable equation of rank greater than zero, then $\mathcal{A} \models s(y, \ldots, y) = t(y, \ldots, y)$; thus $s = t$ belongs to $\mathcal{E}_\delta$ for $\delta(y) := s(y, y, \ldots, y)$. It follows that there is a finite bound on the rank of all minimal falsifiable equations if and only if there is a finite bound on the rank of the minimal falsifiable equations in $\mathcal{E}_\delta$ for each δ. Henceforth it will be our goal to show that there is a finite bound on the rank of any minimal falsifiable equation in a fixed but arbitrarily chosen $\mathcal{E}_\delta$.

To accomplish our goal we need to understand the structure the minimal falsifiable equations in $\mathcal{E}_\delta$. Our analysis depends in an essential way on the theorem of E. W. Kiss and M. A. Valeriote which connects abelian varieties to Hamiltonian varieties.

Definition 2.2 A variety $\mathcal{V}$ is said to be *Hamiltonian* provided that whenever $\mathbf{A} \in \mathcal{V}$ and S is a subuniverse of $\mathbf{A}$, then S is a congruence block of $\mathbf{A}$.

The theorem of Kiss and Valeriote which is crucial for us is the following.

THEOREM 2.3 *[3] A locally finite abelian variety is Hamiltonian.*

A characterization of Hamiltonian varieties is given by L. Klukovits in [4]. Klukovits showed that a variety $\mathcal{V}$ is Hamiltonian if and only if for each term $t(\mathbf{x})$ and each choice of a variable of this term, say the i–th variable, there is a ternary term $k(u, y, z)$ such that

$$\mathcal{V} \models k(t(x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n), y, z) = t(x_1, \ldots, x_{i-1}, z, x_{i+1}, \ldots, x_n).$$

We call the term k a *Klukovits term for* t *in its* i*–th variable.* For example, if $\mathcal{V}$ is a variety of left $\mathbf{R}$–modules and $t(\mathbf{x}) = r_1x_1 + \cdots + r_nx_n$, then a Klukovits term for t in its i–th variable is $k(u, y, z) = u - r_iy + r_iz$. If $\mathcal{V}$ is a variety of $\mathbf{M}$–sets and $t(\mathbf{x}) = mx_i$, then a Klukovits term for t in its i–th variable is $k(u, y, z) = mz$; a Klukovits term for t in its j–th variable, $j \neq i$, is $k(u, y, z) = u$. The phrase "Klukovits term" will mean any ternary term k which is a Klukovits term for t in its i–th variable for some t and i.

Let K be a complete set of $\mathcal{A}$–inequivalent Klukovits terms. Note that K is finite since Klukovits terms are ternary and $\mathcal{A}$ is locally finite. Let ω denote the set of natural numbers with the usual ordering, and let $\omega^{K\times K}$ denote the set of functions from $K \times K$ to ω ordered pointwise. Define a binary relation $\triangleright$ from $\mathcal{E}_\delta$ to $\omega^{K\times K}$ by the rule that

$$(s = t) \ \triangleright \ f$$

if and only if $f : K \times K \to \omega$ has the property that there exists a sequence

$$\Sigma = \langle (j_1, k_1), (j_2, k_2), \ldots, (j_n, k_n) \rangle,$$

where n is the rank of the equation $s = t$, such that

(1) j_i is a Klukovits term for s in its i–th variable and k_i is a Klukovits term for t in its i–th variable, and

(2) for any $(j,k) \in K \times K$, $f(j,k) =$ the number of times (j,k) occurs in the sequence Σ.

LEMMA 2.4 *The following statements hold for the equations in $\mathcal{E}_\delta$.*

(1) If $(s = t) \rhd f$, then the height of f in $\omega^{K\times K}$ equals the rank of the equation $s = t$.

(2) If $(s = t) \rhd f$, and $g < f$ in $\omega^{K\times K}$, then $s = t$ has a specialization $(s' = t') \in \mathcal{E}_\delta$ such that $(s' = t') \rhd g$.

(3) If $p = q$ and $s = t$ are both $\rhd$–related to the element $f \in \omega^{K\times K}$, then $p = q$ is equivalent to $s = t$ modulo the equations of $\mathcal{A}$. (I.e., $\mathrm{Eq}(\mathcal{A}) \models (p = q) \Leftrightarrow (s = t)$.)

Proof. The height of a function f in $\omega^{K\times K}$ is the sum of the values of f. Now if $(s = t) \rhd f$ where $s = t$ is an equation of rank n, then recall that $f(j,k)$ is defined to be the number of times (j,k) occurs in some sequence $\langle (j_1,k_1),(j_2,k_2),\ldots,(j_n,k_n)\rangle$ where this sequence is a sequence of pairs of Klukovits terms for the first n–variables of the equation $s = t$. It follows that $\Sigma_{(j,k)\in K\times K} f(j,k) = n$, which shows that the height of f is n whenever the rank of $s = t$ is n and $(s = t) \rhd f$. This proves (1).

For (2), assume that $s = t$ is the equation $s(x_1,\ldots,x_n,y) = t(x_1,\ldots,x_n,y)$ where (by part (1)) the height of f is n. From the definitions, there exist a sequence $\langle (j_1,k_1),\ldots,(j_n,k_n)\rangle$ of pairs of Klukovits terms for the first n variables of $s = t$ such that, for any $(j,k) \in K \times K$, the number of times (j,k) occurs in this sequence is $f(j,k) \geq g(j,k)$. Therefore it is possible to select a subset $\{i_1,\ldots,i_m\} \subseteq \{1,\ldots,n\}$ such that $\langle (j_{i_1},k_{i_1}),\ldots,(j_{i_m},k_{i_m})\rangle$ has precisely $g(j,k)$ occurrences of (j,k) for each $(j,k) \in K \times K$. Then define $s'(x_1,\ldots,x_m,y) = t'(x_1,\ldots,x_m,y)$ to be the equation obtained from $s(x_1,\ldots,x_n,y) = t(x_1,\ldots,x_n,y)$ by substituting y for x_h whenever $h \notin \{i_1,\ldots,i_m\}$ and substituting x_g for x_{i_g} $i_g \in \{i_1,\ldots,i_m\}$. The equation $s' = t'$ is in $\mathcal{E}_\delta$ since it is obtained from $s = t$ by substituting new variables for old. Moreover, a sequence of Klukovits terms for the first m variables of $s'(x_1,\ldots,x_m,y) = t'(x_1,\ldots,x_m,y)$ is $\langle (j_{i_1},k_{i_1}),\ldots,(j_{i_m},k_{i_m})\rangle$. It follows that $(s' = t') \rhd g$.

Finally we prove (3). To do this, we first define an action of pairs of Klukovits terms on equations. If $u = v$ is an equation of rank ℓ, then the pair (j,k) of Klukovits terms acts on $u = v$ (on the right) to produce a new equation of rank $\ell + 1$ as follows:

$$(u = v) \circ (j,k) := j(u(x_1,\ldots,x_\ell,y),y,x_{\ell+1}) = k(v(x_1,\ldots,x_\ell,y),y,x_{\ell+1}).$$

To start the proof of (3) assume that $p = q$ and $s = t$ are both $\rhd$–related to f. This implies that there are sequences of pairs $\langle (j_1,k_1),\ldots,(j_n,k_n)\rangle$ and $\langle (J_1,K_1),\ldots,(J_n,K_n)\rangle$ where

(a) the first sequence is a sequence of pairs of Klukovits terms for $p = q$,

(b) the second sequence is a sequence of pairs of Klukovits terms for $s = t$ and

(c) the second sequence is a permutation of the first sequence.

We must use this information to prove that $p = q$ and $s = t$ are equivalent modulo the equations of $\mathcal{A}$.

Claim. Let π be a permutation of $\{1, \ldots, n\}$. Modulo the equations of $\mathcal{A}$, the equation $p = q$ is equivalent to

$$[\cdots[(\delta(y) = \delta(y)) \circ (j_{\pi(1)}, k_{\pi(1)})] \circ \cdots] \circ (j_{\pi(n)}, k_{\pi(n)}).$$

The proof of this claim establishes part (3) of this lemma. To see this, note that we can apply the claim once with π chosen so that $(j_{\pi(i)}, k_{\pi(i)}) = (J_i, K_i)$ to get an expression equivalent to $p = q$ which, by a second application of the claim to the equation $s = t$ and the permutation $\pi = \mathrm{id}$, is equivalent to $s = t$ modulo the equations of $\mathcal{A}$. Thus we get that $p = q$ is equivalent to $s = t$ modulo the equations of $\mathcal{A}$.

To prove the claim, first note that since $(p = q) \in \mathcal{E}_\delta$ we have that $\mathcal{A} \models p(y, y, \ldots, y) = \delta(y) = q(y, y, \ldots, y)$. Therefore we are trying to show that $p = q$ is equivalent to

$$j_{\pi(n)}(\cdots j_{\pi(1)}(p(y, \ldots, y), y, x_1) \cdots, y, x_n) = k_{\pi(n)}(\cdots k_{\pi(1)}(q(y, \ldots, y), y, x_1) \cdots, y, x_n).$$

Using the Klukovits equations, which are equations of $\mathcal{A}$, this equation can be greatly simplified. We simplify it in n steps, working our way through this nested composition from the innermost part outwards. At the first step we have $j_{\pi(1)}(p(y, y, \ldots, y), y, x_1)$ on the lefthand side, and the Klukovits equations reduce this to $p(y, y, \ldots, x_1, \ldots, y)$ with x_1 in the $\pi(1)$–rst position. At the innermost part on the righthand side we have $k_{\pi(1)}(q(y, y, \ldots, y), y, x_1)$ which simplifies to $q(y, y, \ldots, x_1, \ldots, y)$ with x_1 in the $\pi(1)$–rst position. Similarly, as we work our way through each step of the composition we simply replace the y in position $\pi(i)$ on both sides of the equation with the variable x_i during the i–th step. The result is that the previously displayed equation is equivalent modulo the equations of $\mathcal{A}$ to

$$p(x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)}, y) = q(x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)}, y),$$

which differs from the equation $p = q$ only by a permutation of variables. Thus the claim is proved. □

THEOREM 2.5 *$\mathcal{A}$ is finitely generated.*

Proof. Define an order filter in $\omega^{K \times K}$ as follows:

$$F = \{x \in \omega^{K \times K} \,|(\exists g)\ x \geq g \text{ where } (p = q) \triangleright g \text{ for some falsifiable equation } p = q\}.$$

We claim that if $(s = t) \in \mathcal{E}_\delta$ is a minimal falsifiable equation and $(s = t) \triangleright f$, then f is a minimal member of F. To see this, assume that $s = t$ is falsifiable and that f is not minimal in F; we will prove that $s = t$ is not a minimal falsifiable equation. Since f is not minimal in F there is a falsifiable equation $p = q$ such that $(p = q) \triangleright g$ and $g < f$. From Lemma 2.4 we deduce that the equation $s = t$ has a specialization $(s' = t') \in \mathcal{E}_\delta$ such that $(s' = t') \triangleright g$ and $s' = t'$ is equivalent to $p = q$ modulo the equations of $\mathcal{A}$. The equivalence of $s' = t'$ with the falsifiable equation $p = q$ implies that $s' = t'$ is falsifiable, which proves that $s = t$ has a falsifiable specialization of smaller rank. This establishes our claim.

Since K is finite, the ordered set $\omega^{K\times K}$ has the property that its order filters are finitely generated (see [5]). So, there is a natural number N such that every minimal element of F has height $\leq N$. It follows from the previous paragraph and Lemma 2.4 (1) that N is a bound on the rank of any minimal falsifiable equation in $\mathcal{E}_\delta$. As we observed earlier, the fact that this is true for an arbitrarily chosen δ implies the existence of a finite bound on the rank of all minimal falsifiable equations. Lemma 2.1 can now be invoked to deduce that $\mathcal{A}$ is finitely generated. $\square$

3 A Nonfinitely Based Abelian Algebra

In this section we describe a finite algebra which generates a nonfinitely based abelian variety. This provides a strong negative answer to Problem 3 of [1], and complements the result in [2] that states that no finite algebra can generate an inherently nonfinitely based abelian variety.

The idea behind our example is extremely simple, so we give a rough description now before facing the details. We plan to construct a variety $\mathcal{P}$ of algebras whose models are (essentially) pairs of isomorphic Boolean groups[1] $\mathbf{B}$ and $\mathbf{C}$ glued together at a subset containing the common identity element, 0. We try to show that the subvariety of algebras where $B \cap C$ is a subgroup is not finitely based relative to $\mathcal{P}$. That is, we try to show that it is impossible to express the idea that $B \cap C$ is closed under sums without looking at a large number of elements of $B \cap C$ simultaneously.

Our idea does not work in the form just explained, because it is *not* hard to express the fact that $B \cap C$ is closed under sums: one can check elements of $B \cap C$ two at a time to see if their sum is in $B \cap C$. Therefore, to make this idea work, we need a subset Q disjoint from $B \cup C$ and an operation $s : Q \to B \cap C$ whose duty is to 'select' a subset of $B \cap C$. What we actually show is that it is hard to express the fact that the subgroup generated by $s(Q)$ lies in $B \cap C$. Here it may be that all sums of few elements of $s(Q)$ lie in $B \cap C$, but some sum of many elements lies outside $B \cap C$.

We will get a properly decreasing sequence of varieties $\mathcal{P} = \mathcal{V}_1 \supset \mathcal{V}_2 \supset \mathcal{V}_3 \supset \cdots$, where $\mathcal{V}_n$ is the collection of algebras where all sums of $\leq n$ elements of $s(Q)$ are in $B \cap C$. The intersection $\mathcal{V}_\infty = \bigcap_{n<\omega} \mathcal{V}_n$ is the nonfinitely based variety of algebras in $\mathcal{P}$ where $s(Q)$ generates a subgroup of $B \cap C$. Since $\mathcal{V}_\infty$ is locally finite and abelian, the result of the last section proves that $\mathcal{V}_\infty$ is generated by a (nonfinitely based) finite algebra. We produce a concrete 6-element generating algebra for $\mathcal{V}_\infty$ at the end of this section.

Our nonfinitely based algebra is of type $\langle 0, 1, 1, 1, 2, 2\rangle$ and the corresponding operation symbols are $\langle 0, e, f, s, +, \oplus\rangle$. Our algebra will be a member of the (abelian) variety $\mathcal{P}$ whose defining equations assert that in each $\mathbf{A} \in \mathcal{P}$:

[1] A *Boolean group* is a group of exponent 2.

(A) $\{0\}$ is a subuniverse.

(B) $$\begin{aligned}&ee(x) = e(x), ff(x) = f(x), ss(x) = 0,\\ &ef(x) = e(x), fe(x) = f(x),\\ &es(x) = fs(x) = s(x),\\ &se(x) = sf(x) = 0.\end{aligned}$$

(C) $$\begin{aligned}&x + y = e(x) + e(y) = e(x + y) = e(x \oplus y),\\ &x \oplus y = f(x) \oplus f(y) = f(x \oplus y) = f(x + y).\end{aligned}$$

(D) $\langle e(A); +, 0\rangle$ and $\langle f(A); \oplus, 0\rangle$ are Boolean groups.

We will soon see that $\mathcal{P}$ is a locally finite abelian variety which contains a nonfinitely based algebra. First we describe how to construct models of these equations.

We refine our earlier discussion of the models of $\mathcal{P}$ by discussing a class of three–sorted structures of the form
$$\langle \mathbf{B}, \mathbf{C}, Q; \iota; e_Q, s_Q\rangle.$$
Here $\mathbf{B} = \langle B; *, 0\rangle$ and $\mathbf{C} = \langle C; \circ, 0\rangle$ are Boolean groups which have a common identity element. Q is a set which is disjoint from $B \cup C$. The unary function ι is an isomorphism $\iota : \mathbf{C} \to \mathbf{B}$ for which $\iota(x) = x$ for all $x \in B \cap C$. Both $e_Q : Q \to B$ and $s_Q : Q \to (B \cap C)$ are functions. There is no restriction on them other than that they have the correct domain and range.

From such a three–sorted structure $\langle \mathbf{B}, \mathbf{C}, Q; \iota; e_Q, s_Q\rangle$ we can construct a member of $\mathcal{P}$. Our algebra will have universe $A = B \cup C \cup Q$. We interpret the operations $\langle 0, e, f, s, +, \oplus\rangle$ as follows. We interpret 0 as the element already named $0 \in A$. We define e and f by

$$e(x) = \begin{cases} x & \text{if } x \in B,\\ \iota(x) & \text{if } x \in C,\\ e_Q(x) & \text{if } x \in Q,\end{cases} \qquad f(x) = \begin{cases} x & \text{if } x \in C,\\ \iota^{-1}(x) & \text{if } x \in B,\\ \iota^{-1}e_Q(x) & \text{if } x \in Q.\end{cases}$$

We define s so that $s(B \cup C) = \{0\}$ while $s|_Q = s_Q$. Next we define $x + y$ to be $e(x) * e(y)$, where $*$ is the group operation of $\mathbf{B}$. Similarly, $x \oplus y = f(x) \circ f(y)$ where $\circ$ is the group operation of $\mathbf{C}$.

LEMMA 3.1 *The algebra* $\mathbf{A}$ *constructed as in the previous paragraph belongs to* $\mathcal{P}$*. Conversely, any member of* $\mathcal{P}$ *is isomorphic to such an algebra.*

Sketch of Proof. The first statement requires only the straightforward verification that the equations defining $\mathcal{P}$ hold in $\mathbf{A}$.

For the second statement, choose any $\mathbf{D} \in \mathcal{P}$. Let $B = e(D)$, $C = f(D)$ and $Q = D - (B \cup C)$. The equations of $\mathcal{P}$ of types (A), (B) and (D) ensure that B is closed under $+$ and 0, C is closed under $\oplus$ and 0, and that $\mathbf{B} := \langle B; +', 0\rangle$ and $\mathbf{C} := \langle C; \oplus', 0\rangle$ are Boolean groups. Here the prime on $+'$ and $\oplus'$ indicates that we are using the restrictions of the corresponding operations of $\mathbf{D}$. If we let $\iota = e|_C$, then the equations of type (C) guarantee that $\iota : \mathbf{C} \to \mathbf{B}$ is an isomorphism of groups which is the identity on $B \cap C$. Let $e_Q = e|_Q$ and $s_Q = s|_Q$. Of course, $e_Q(Q) \subseteq e(D) = B$. The equations of type (B) involving s ensure that $s_Q(Q) \subseteq e(D) \cap f(D) = B \cap C$. Thus, $\mathbf{D}$ yields a three–sorted structure $\langle \mathbf{B}, \mathbf{C}, Q; \iota; f_Q, s_Q\rangle$.

We can apply the procedure outlined before the proof of this lemma to the three–sorted structure derived from $\mathbf{D}$. By doing so we reconstruct an algebra in $\mathcal{P}$ which has the same universe as $\mathbf{D}$. One can check that each operation of the constructed algebra coincides with the corresponding operation in $\mathbf{D}$. Thus, $\mathbf{D}$ is reconstructible from $\langle \mathbf{B}, \mathbf{C}, Q; \iota; e_Q, s_Q\rangle$. $\Box$

Now we analyze the term operations of $\mathcal{P}$. In the next lemma we let $E(x) = e(x) + s(x)$ and $F(x) = f(x) \oplus s(x)$.

LEMMA 3.2 *Any term of $\mathcal{P}$ is $\mathcal{P}$–equivalent either to a variable or to a term of the form*

$$u_1(x_1) + u_2(x_2) + \cdots + u_n(x_n)$$

where each $u_i \in \{0, e, s, E\}$ or to

$$v_1(x_1) \oplus v_2(x_2) \oplus \cdots \oplus v_n(x_n)$$

where each $v_i \in \{0, f, s, F\}$.

Sketch of Proof. The proof is a straightforward induction argument using the equations for $\mathcal{P}$. $\Box$

COROLLARY 3.3 *$\mathcal{P}$ is a locally finite abelian variety.*

Proof. To see that $\mathcal{P}$ is abelian, choose $\mathbf{A} \in \mathcal{P}$ and a term $t(x, \mathbf{y})$. Without loss of generality we may assume that $t(x, \mathbf{y}) = u_0(x) + u_1(y_1) + \cdots + u_n(y_n)$. To check that the term condition holds for t we must show that for all $a, b \in A$ and $\mathbf{c}, \mathbf{d} \in A^n$

$$u_0(a) + u_1(c_1) + \cdots + u_n(c_n) = u_0(a) + u_1(d_1) + \cdots + u_n(d_n)$$

implies

$$u_0(b) + u_1(c_1) + \cdots + u_n(c_n) = u_0(b) + u_1(d_1) + \cdots + u_n(d_n).$$

The second equality follows from the first by adding $u_0(a) + u_0(b)$ to both sides of the first equality. This shows that $\mathcal{P}$ is abelian.

It follows immediately from the previous lemma that $\mathcal{P}$ has only finitely many n–ary terms up to equivalence for any finite n. Thus $\mathcal{P}$ is locally finite. $\Box$

Next we consider equations of the form

$$(\mathrm{E}_n): \quad s(x_1) + s(x_2) + \cdots + s(x_n) = s(x_1) \oplus s(x_2) \oplus \cdots \oplus s(x_n).$$

Notice that by substituting 0 in for x_n in E_n we obtain E_{n-1}. Thus $\mathrm{E}_n \Rightarrow \mathrm{E}_{n-1}$. The next lemma proves that the reverse implication does not hold.

LEMMA 3.4 *For each $n > 1$ there is an algebra in $\mathcal{P}$ which satisfies E_{n-1}, but which fails E_n.*

Proof. Let $\mathbf{B} = \mathbf{Z}_2^n$ where $\mathbf{Z}_2 = \langle \{0,1\}; *, 0\rangle$ is the two–element group. Let $b_i \in B$ denote the element which has a one in the i–th position and zeros elsewhere. Let $\mathbf{0} \in B$ denote the element which has zeros in every position and let $\mathbf{1} \in B$ be the element with ones in every position. Let $\mathbf{C}$ be a Boolean group obtained from $\mathbf{B}$ by replacing the element $\mathbf{1}$ with a new element $\mathbf{1}'$ and naming the resulting group operation $\circ$. Observe that $B \cap C = B - \{\mathbf{1}\}$.

Let $Q = \{1, 2, \ldots, n\}$. Let $\iota : \mathbf{C} \to \mathbf{B}$ be the isomorphism which fixes $B \cap C$ and maps $\mathbf{1}'$ to $\mathbf{1}$. Define e_Q arbitrarily and for each $i \in Q$ let $s_Q(i) = b_i$. We now have a three–sorted structure $\langle \mathbf{B}, \mathbf{C}, Q; \iota, e_Q, s_Q\rangle$. Satisfaction of E_k in the associated algebra $\mathbf{A} \in \mathcal{P}$ is equivalent to the satisfaction of

$$s_Q(x_1) * \cdots * s_Q(x_k) = s_Q(x_1) \circ \cdots \circ s_Q(x_k)$$

in $\langle \mathbf{B}, \mathbf{C}, Q; \iota, e_Q, s_Q\rangle$. The only way for this equation to fail is for the left hand side to equal $\mathbf{1}$ and (therefore) for the right hand side to equal $\mathbf{1}'$. If $k < n$ there are too few summands for this to happen, but when $k = n$ we may take $x_i = i$ and we get a failure of this equation. Hence the algebra $\mathbf{A}$ fails E_n but satisfies all E_k for $k < n$. $\Box$

Let $\mathcal{V}_n$ denote the subvariety of $\mathcal{P}$ axiomatized by E_n and the equations of $\mathcal{P}$. Let $\mathcal{V}_\infty = \bigcap_{n<\omega} \mathcal{V}_n$. The previous lemma shows that $\mathcal{V}_\infty$ is not finitely based. Since $\mathcal{V}_\infty$ is a locally finite abelian variety it is generated by a finite algebra. We shall produce a finite generating algebra shortly, but first we describe the subvariety lattice of $\mathcal{P}$.

THEOREM 3.5 *The subvarieties of $\mathcal{P}$ are: $\mathcal{P} = \mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_\infty$ and the six proper subvarieties of $\mathcal{V}_\infty$.*

Proof. We begin by considering the situation where $\mathcal{U}$ and $\mathcal{W}$ are subvarieties of $\mathcal{P}$, $\mathcal{U} \subset \mathcal{W} \subseteq \mathcal{P}$ and $\mathcal{U}$ and $\mathcal{W}$ satisfy the same one–variable equations. Let $p = q$ be an equation that holds in $\mathcal{U}$ but fails in $\mathcal{W}$. We shall argue that $p = q$ is $\mathcal{P}$–equivalent to some E_n. The purpose of this is to show that every subvariety of $\mathcal{P}$ is axiomatizable relative to $\mathcal{P}$ by a set of one–variable equations together with some of the E_n's.

If both p and q are $\mathcal{P}$–equivalent to variables, then $p = q$ is $\mathcal{P}$–equivalent to $x = x$ or to $x = y$. Since $p = q$ fails in $\mathcal{W}$ it cannot be equivalent to $x = x$. The equation $x = y$ is $\mathcal{P}$–equivalent to $x = 0$, which is a one–variable equation. Since $p = q$ holds in $\mathcal{U}$ but not in $\mathcal{W}$, and $\mathcal{U}$ and $\mathcal{W}$ satisfy the same one–variable equations, we conclude that $p = q$ is not equivalent to $x = y$, either. Henceforth we assume that p is not $\mathcal{P}$–equivalent to a variable.

Now, according to Lemma 3.2, $p(\mathbf{x})$ is $\mathcal{P}$–equivalent to $p_1(x_1) + \cdots + p_n(x_n)$ or the same with $+$ replaced by $\oplus$. According to which case we are in ($+$ or $\oplus$), this implies that either $ep = p$ or $fp = p$ is an equation of $\mathcal{P}$. If q is $\mathcal{P}$–equivalent to a variable then $p = q$ has the consequence $e(x) = x$, since $eq = ep = p = q$, or else the consequence $f(x) = x$. But $e(x) = x$ and $f(x) = x$ are equivalent modulo the equations of $\mathcal{P}$, so if q is $\mathcal{P}$–equivalent to a variable then $\mathcal{U}$ satisfies the one–variable equation $e(x) = x$. $\mathcal{W}$ must also satisfy this equation. However, the equations of $\mathcal{P}$ together with $e(x) = x$ imply that $e = f = E = F$, $s = 0$ and $x + y = x \oplus y$. $\mathcal{W}$ must now satisfy all of these equations and this is enough to imply that $\mathcal{W}$ is a definitionally equivalent to a variety of Boolean groups. Since the variety of all Boolean groups is a minimal variety and $\mathcal{U}$ is a proper subvariety of $\mathcal{W}$, therefore we must have that $\mathcal{U}$ is the trivial variety. But this contradicts the assumption that $\mathcal{U}$ and

$\mathcal{W}$ satisfy the same one–variable equations, since now $\mathcal{U}$ satisfies $x = 0$ and $\mathcal{W}$ does not. We conclude that q is not $\mathcal{P}$–equivalent to a variable. Therefore $q(\mathbf{x})$ is $\mathcal{P}$–equivalent to $q_1(x_1) + \cdots + q_n(x_n)$ or the same with $+$ replaced by $\oplus$.

By substituting zeros into the equation $p = q$ we can see that for each i

$$p_i(x_i) := p(0, 0, \ldots, x_i, \ldots, 0) = q(0, 0, \ldots, x_i, \ldots, 0) =: q_i(x_i)$$

is a one–variable equation of $\mathcal{U}$ and therefore of $\mathcal{W}$. It follows that each of p and q is $\mathcal{P}$–equivalent to either $p_1(x_1) + \cdots + p_n(x_n)$ or $p_1(x_1) \oplus \cdots \oplus p_n(x_n)$. Since $p = q$ fails to hold in $\mathcal{W}$, it must be that $p = q$ is $\mathcal{P}$–equivalent to

$$p_1(x_1) + \cdots + p_n(x_n) = p_1(x_1) \oplus \cdots \oplus p_n(x_n).$$

Because $x+y = e(x)+e(y)$ and $x \oplus y = f(x) \oplus f(y)$ hold in $\mathcal{P}$, it follows that $ep_i(x_i) = fp_i(x_i)$ is a one–variable equation of $\mathcal{U}$, therefore of $\mathcal{W}$. The only way for this to be true is if $p_i \in \{0, s(x_i)\}$ for all i. Since we may assume that each $p_i(x_i)$ depends on its variable, we may conclude that $p_i(x_i) = s(x_i)$ for all i. Thus, $p = q$ is $\mathcal{P}$–equivalent to E_n. We have shown that if $\mathcal{U} \subset \mathcal{W} \subseteq \mathcal{P}$ and $\mathcal{U}$ and $\mathcal{W}$ satisfy the same one–variable equations, then $\mathcal{U}$ is axiomatized relative to $\mathcal{W}$ by a collection of the E_n's. Thus every subvariety of $\mathcal{P}$ is axiomatizable relative to $\mathcal{P}$ by one–variable equations and some of the E_n's.

The one-variable equations which fail to hold in $\mathcal{P}$ are easy to locate since there are only seven $\mathcal{P}$–inequivalent unary terms: $\{0, x, e(x), f(x), s(x), E(x), F(x)\}$. It is a simple matter to show that each one–variable equation which fails in $\mathcal{P}$ has either $s(x) = 0$ or $e(x) = f(x)$ as a consequence. The first clearly entails all E_n while the second entails $x + y = x \oplus y$ which clearly entails all E_n. Therefore, every one–variable equation which fails in $\mathcal{P}$ entails all E_n. Combining this fact with what we have previously established, we obtain that any subvariety of $\mathcal{P}$ which is not one of $\mathcal{P} = \mathcal{V}_1, \mathcal{V}_2, \ldots$ or $\mathcal{V}_\infty$ must be a subvariety of $\mathcal{V}_\infty$. Moreover, any subvariety of $\mathcal{V}_\infty$ must be axiomatizable relative to $\mathcal{P}$ by one–variable equations. Since there are so few nontrivial one–variable equations it is easy to determine that the subvarieties of $\mathcal{V}_\infty$ are: $\mathcal{V}_{s=0}$, $\mathcal{V}_{e=f}$, $\mathcal{V}_{e=F}$, $\mathcal{V}_{e=x}$, $\mathcal{V}_{e=0}$, and $\mathcal{V}_{x=0}$. The notation $\mathcal{V}_{p=q}$ means that $\mathcal{V}_{p=q}$ is axiomatized by $p(x) = q(x)$ and the equations of $\mathcal{P}$. See Figure 1. $\square$

LEMMA 3.6 *$\mathcal{V}_\infty$ has a six–element generator.*

Proof. Borrowing notation from the previous proof, we must show that there is a six–element algebra in $\mathcal{V}_\infty$ which is not in $\mathcal{V}_{s=0}$ or $\mathcal{V}_{e=f}$. That is, we must produce a six–element algebra $\mathbf{A}$ for which

(1) $\mathbf{A} \in \mathcal{P}$,

(2) $\mathbf{A} \not\models s(x) = 0$,

(3) $\mathbf{A} \not\models e(x) = f(x)$, and

(4) $\mathbf{A} \models \mathrm{E}_n$ for all n.

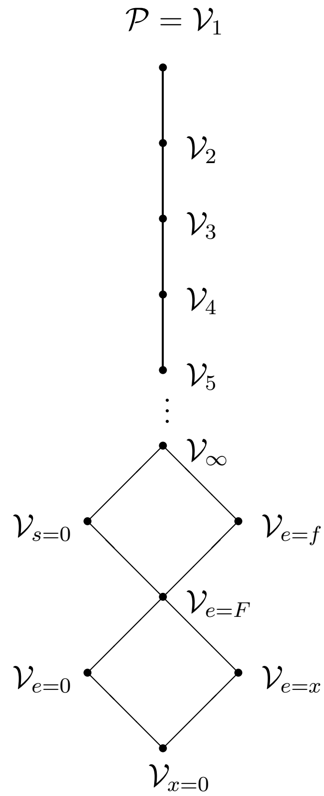

Figure 1: Subvariety Lattice of $\mathcal{P}$

Observe that condition (4) says precisely that $s(A)$ generates a subgroup which is contained in $e(A) \cap f(A)$.

Let $\mathbf{B} = \mathbf{Z}_2^2$ and let $\mathbf{1} = (1, 1) \in B$. Let $\mathbf{C}$ be the group obtained from $\mathbf{B}$ by replacing the element $\mathbf{1}$ with a new element $\mathbf{1}'$. Let $Q = \{q\}$. Let $\iota : \mathbf{C} \to \mathbf{B}$ be the isomorphism which fixes $B \cap C$ and maps $\mathbf{1}'$ to $\mathbf{1}$. Define $e_Q(q) = s_Q(q) = (0, 1) \in B$. This yields a three–sorted structure which is associated to the algebra $\mathbf{A}$ which has six-element universe $B \cup \{\mathbf{1}'\} \cup \{q\}$. Note that the subgroup generated by $s(A)$ is just $\{(0, 0), (0, 1)\} \subseteq e(A) \cap f(A)$. We have that $s(q) \neq 0$ and $e(\mathbf{1}) = \mathbf{1} \neq \mathbf{1}' = f(\mathbf{1})$ so the conditions listed above are met. □

References

[1] D. Hobby and R. McKenzie, *The Structure of Finite Algebras*, Contemporary Mathematics v. 76, American Mathematical Society, 1988.

[2] K. Kearnes and R. Willard, *Inherently nonfinitely based solvable algebras*, Canad. Math. Bull. **37** (1994), 514–521.

[3] E. W. Kiss and M. Valeriote, *Abelian algebras and the Hamiltonian property*, J. Pure Appl. Algebra **87** (1993), 37–49.

[4] L. Klukovits, *Hamiltonian varieties of universal algebras*, Acta Sci. Math. **37** (1975), 11–15.

[5] E. C. Milner, *Basic wqo and bqo theory*, in *Graphs and Order*, I. Rival (ed.), D. Reidel Publishing Company, 1985, 487–502.

Department of Mathematics
University of Louisville
Louisville, Ky 40292
USA

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada