

Decidable unary varieties

MATTHEW A. VALERIOTE

0. Introduction

Recently R. McKenzie and the author [5] have shown that in order for a locally finite variety to be decidable it must decompose into the varietal product of three special subvarieties; an affine subvariety, a discriminator subvariety, and a strongly abelian subvariety. A variety is locally finite if every finitely generated member is finite. An important element of the proof is the characterization of the decidable locally finite strongly abelian varieties.

The class of strongly abelian algebras was first defined by McKenzie in [4]. An algebra \mathbf{A} is said to be strongly abelian if for all terms $t(x_1, \dots, x_n)$,

$$\mathbf{A} \models \forall a_1, \dots, a_n, b_1, \dots, b_n, c_2, \dots, c_n [t(a_1, \dots, a_n) \approx t(b_1, \dots, b_n) \\ \rightarrow t(a_1, c_2, \dots, c_n) \approx t(b_1, c_2, \dots, c_n)].$$

The simplest kind of strongly abelian algebra is the multi-unary algebra, and so any characterization of the decidable strongly abelian varieties must thus include a characterization of the decidable multi-unary varieties.

The problem of characterizing the locally finite, decidable multi-unary varieties is addressed and solved in this paper. Two notable results which precede this paper are those of Ehrenfeucht [3] where it is announced that the variety of all mono-unary algebras is decidable, and Trakhtenbrot [9] where the variety of all bi-unary algebras is shown to be undecidable. Our Theorem 4.1 includes the theorem of Trakhtenbrot and relies on Ehrenfeucht's result. The reader may wish to consult [6] and [7] as alternate sources for the work of Ehrenfeucht and Trakhtenbrot just mentioned. A generalization of our main theorem to heterogeneous algebras is used by the author in his Ph.D. thesis to characterize the decidable locally finite strongly abelian varieties.

Research supported by NSERC of Canada postgraduate fellowship.

Presented by Jan Mycielski. Received January 8, 1986. Accepted for publication in final form September 29, 1986.

For those readers not familiar with interpretations and decidability proofs consult Burris and McKenzie [1] Part 1, Chapter 3, and Burris, Sankappanavar [2]. For the most part our notation follows that of the two works just cited. A few new concepts will be introduced.

DEFINITION 0.1.

- i) We say that a class \mathcal{V} is decidable if the full first order theory of \mathcal{V} , $\text{Th}(\mathcal{V})$, is recursive, i.e., there is an algorithm for deciding whether a given first order formula in the language of \mathcal{V} is true for all members of \mathcal{V} .
- ii) We say \mathcal{V} is hereditarily undecidable if \mathcal{W} is undecidable (not decidable) for all classes $\mathcal{W} \supseteq \mathcal{V}$.

We now focus our attention on multi-unary varieties of finite type, and define a monoid associated with such a variety.

DEFINITION 0.2. Let \mathcal{V} be a multi-unary variety of finite type, and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(\mathbf{x})$ be the \mathcal{V} -free algebra on one generator. Let $\mathbf{M}(\mathcal{V}) = \langle F, \cdot, \mathbf{1} \rangle$ be the monoid with universe F and multiplication defined by: $m(\mathbf{x}) \cdot n(\mathbf{x}) = m(n(\mathbf{x}))$. Let $\mathbf{1} = \mathbf{x}$.

Notice that $\mathbf{M}(\mathcal{V})$ is finite iff \mathcal{V} is locally finite, and $\mathbf{M}(\mathcal{V})$ is finitely generated, since \mathcal{V} is of finite type. For convenience we will not distinguish between elements of $\mathbf{M}(\mathcal{V})$, and the corresponding terms in the language. Often elements of $\mathbf{M}(\mathcal{V})$ will be regarded as actual terms, especially in the first order formulas constructed for our interpretations.

DEFINITION 0.3. Let A be a set, and $f: A \rightarrow A$ a function on A .

- i) For $a, b \in A$, we say $a \xrightarrow{f} b$ if $b = f^n(a)$ for some $n \geq 0$.
- ii) We say $a \in A$ is f -initial if for all $c \in A$, $c \xrightarrow{f} a$ implies $c = a$.

The relation \xrightarrow{f} is a transitive, reflexive relation, but not necessarily a partial ordering. Evidently an element $a \in A$ is f -initial iff $f^{-1}(a) \subseteq \{a\}$. For the remainder of this paper, let \mathcal{V} be some fixed locally finite unary variety of finite type.

1. Monoids

Associated with any monoid is the ordering of rightsided divisibility. This ordering, along with a related one, will be examined in this section, paying special

attention to the case in which the monoid is finite. For the remainder of this section, let \mathbf{M} be some fixed, finite monoid. Let $G \subseteq M$ be the set of invertible elements of \mathbf{M} . It is clear that G is nonempty, and \mathbf{G} is a submonoid of \mathbf{M} .

DEFINITION 1.1.

- (1) For $x, y \in M$, we write $x \leq y$ if for some $w \in M$, $x = wy$, and we write $x \leq y$ if for some $g \in G$, $x \leq yg$.
- (2) For $x, y \in M$, we write $x \equiv y$ if $x \leq y$ and $y \leq x$, and $x \succ y$ if $x \leq y$ and $y \not\leq x$.
- (3) \mathbf{M} is said to be *linear (quasi-linear)* if for every $x, y \in M$, $x \leq y$ or $y \leq x$ ($x \leq y$ or $y \leq x$).

PROPOSITION 1.2.

- (1) Both \leq and \leq define transitive, reflexive relations on M .
- (2) Both \equiv and \succ define equivalence relations on M . Modulo the respective equivalence relations, \leq and \leq define partial orderings.
- (3) \mathbf{M} is linear (quasi-linear) iff \leq modulo \equiv (\leq modulo \succ) is a linear ordering.
- (4) For $x, y \in M$, if $x \leq y$, then $x \leq y$.
- (5) If $m \in M$ is left or right invertible, then m is invertible.

Proof. The proof of this proposition is straightforward, and so will not be given. \square

DEFINITION 1.3. For $x \in M$, let $G_x = \{g \in G : x \leq xg\}$.

PROPOSITION 1.4.

- (1) For each $x \in M$, \mathbf{G}_x is a subgroup of \mathbf{G} , and if $g \in G_x$, then $x \equiv xg \equiv xg^{-1}$.
- (2) \mathbf{M} is a linear monoid iff $G_x = G$ for all $x \in M$ and \mathbf{M} is quasi-linear.

Proof.

- (1) This follows from the fact that G is finite, and any subset of a finite group which is closed under \cdot is a subgroup.
- (2) \Rightarrow If \mathbf{M} is linear, then \mathbf{M} is quasi-linear, since \leq is a refinement of \leq . If $x \in M$, and $g \in G$, we have either $x \leq xg$ or $xg \leq x$. If the former holds then $g \in G_x$, and if the latter holds, we have that $xg = wx$ for some $w \in M$, and so $x \leq xg^{-1}$. Thus $g^{-1} \in G_x$, and as G_x is a subgroup of G , we must also have that $g \in G_x$. Therefore $G_x = G$.

\Leftarrow Suppose \mathbf{M} is quasi-linear and $G_x = G$ for all $x \in M$. Let $x, y \in M$ and assume without loss of generality that $x \leq y$. Then for some $g \in G$, $x \leq yg$, and as $yg \leq y$, we conclude that $x \leq y$. Thus \mathbf{M} is linear. \square

We will see in the following two sections that in order for \mathcal{V} to be decidable, it is necessary and sufficient for the finite monoid $\mathbf{M}(\mathcal{V})$ to be linear.

2. Decidability and linearity

Throughout this section, assume that $\mathbf{M} = \mathbf{M}(\mathcal{V})$ is linear. Let $\text{Card}(M) = \kappa$.

DEFINITION 2.1. Let $\mathbf{A} \in \mathcal{V}$, and $a \in A$. The *orbit* of a in \mathbf{A} , \mathcal{O}_a is defined by

$$\mathcal{O}_a = \{m^\wedge(a) : m \in M\}.$$

\mathbf{O}_a will denote the subalgebra of \mathbf{A} with universe \mathcal{O}_a .

PROPOSITION 2.2. Let $\mathbf{A} \in \mathcal{V}$ and $a \in A$.

- (1) If $B \subseteq \mathcal{O}_a$ is a nonempty subuniverse of \mathbf{A} , then $B = \mathcal{O}_b$ for some $b \in B$.
- (2) The set of subuniverses of \mathbf{A} contained in \mathcal{O}_a is linearly ordered by inclusion.

Proof.

- (1) If $B \subseteq \mathcal{O}_a$ is a nonempty subuniverse, then for some left ideal N of M , $B = \{n^\wedge(a) : n \in N\}$. Choose $m \in N$ maximal with respect to \leq . Then $B = \mathcal{O}_{m(a)}$, for if $c \in B$ then $c = n^\wedge(a)$ for some $n \leq m$ in N , and so $n = wm$ for some $w \in M$. Then

$$c = n^\wedge(a) = (wm)^\wedge(a) = w(m^\wedge(a)) \in \mathcal{O}_{m(a)}.$$

Clearly $\mathcal{O}_{m(a)} \subseteq B$, and so $B = \mathcal{O}_{m(a)}$.

- (2) Now let B, C be nonempty subuniverses of \mathbf{A} contained in \mathcal{O}_a , say $B = \mathcal{O}_b$ and $C = \mathcal{O}_c$ for some $b \in B$ and $c \in C$. Since $b, c \in \mathcal{O}_a$, there are $m, n \in M$ with $b = m^\wedge(a)$ and $c = n^\wedge(a)$. If $m \leq n$, then it follows that $b \in \mathcal{O}_c$, and thus $B \subseteq C$. $n \leq m$ leads to $C \subseteq B$. \square

DEFINITION 2.3. Let $\mathbf{A} \in \mathcal{V}$, and $a \in A$.

- (1) A function $f: \mathcal{O}_a \rightarrow \mathcal{O}_a$ is a *coding function* for \mathbf{O}_a if
 - i) for all $b \in \mathcal{O}_a$, $f(\mathcal{O}_b) \subseteq \mathcal{O}_b$, and
 - ii) the relation \xrightarrow{f} on \mathcal{O}_a , defined in Section 0, is a linear ordering.

- (2) A function $f:A \rightarrow A$ is a *coding function* for \mathbf{A} if for all $a \in A$, $f(\mathcal{O}_a) \subseteq \mathcal{O}_a$, and f restricted to \mathcal{O}_a is a coding function for \mathbf{O}_a .

To establish the decidability of \mathcal{V} , we will interpret \mathcal{V} into the variety of all mono-unary algebras, and so in some sense, each algebra of \mathcal{V} will be encoded by a single unary function on some set. The coding functions just defined will be used to construct our interpretation.

We present a few elementary facts about coding functions, without proof, in the next proposition.

PROPOSITION 2.4. *Let $\mathbf{A} \in \mathcal{V}$ be one-generated.*

- (1) *There is a coding function for \mathbf{A} .*
- (2) *If $b \in A$, and $g:\mathcal{O}_b \rightarrow \mathcal{O}_b$ is a coding function for \mathbf{O}_b , then g can be extended to a coding function for \mathbf{A} . Conversely, if $f:A \rightarrow A$ is a coding function for \mathbf{A} , then f restricted to \mathcal{O}_b is a coding function for \mathbf{O}_b .*
- (3) *If f is a coding function for \mathbf{A} and $a' \in A$ is the unique f -initial element of A , then $\mathcal{O}_{a'} = A$.*
- (4) *If f is a coding function for \mathbf{A} , and $b, c \in A$ with $b \xrightarrow{f} c$, then $c \in \mathcal{O}_b$.*

LEMMA 2.5. *For every $\mathbf{A} \in \mathcal{V}$, there is a coding function for \mathbf{A} .*

Proof. This proof involves the use of Zorn's Lemma, since the algebra \mathbf{A} may be infinite. Let

$$\mathcal{H} = \{ \langle \mathbf{B}; g \rangle : \mathbf{B} \text{ is a subalgebra of } \mathbf{A}, \text{ and } g \text{ is a coding function for } \mathbf{B} \}.$$

For $\langle \mathbf{B}_1; g_1 \rangle, \langle \mathbf{B}_2; g_2 \rangle \in \mathcal{H}$, we say

$$\langle \mathbf{B}_1; g_1 \rangle \subset \langle \mathbf{B}_2; g_2 \rangle \quad \text{if} \quad B_1 \subset B_2 \quad \text{and} \quad g_2|_{B_1} = g_1.$$

This defines a partial ordering on \mathcal{H} such that any ascending chain has an upper bound in \mathcal{H} , namely the union of the chain. Thus by Zorn's Lemma, there is $\langle \mathbf{B}; f \rangle$ in \mathcal{H} maximal with respect to \subset . \mathbf{B} must be equal to \mathbf{A} , for if $a \in A \setminus B$, we can extend f to a coding function on the subalgebra \mathbf{B}' with universe $B \cup \mathcal{O}_a$ as follows.

If $B \cap \mathcal{O}_a = \emptyset$, then for $h:\mathcal{O}_a \rightarrow \mathcal{O}_a$ any coding function for \mathbf{O}_a , if we set $f' = f \cup h$, we see that f' is a coding function for \mathbf{B}' , and so $\langle \mathbf{B}; f \rangle \subset \langle \mathbf{B}'; f' \rangle$ in \mathcal{H} , contrary to our choice of $\langle \mathbf{B}; f \rangle$.

If $B \cap \mathcal{O}_a \neq \emptyset$, then $B \cap \mathcal{O}_a = \mathcal{O}_c$ for some $c \in B$, by Proposition 2.1. Since $f|_{\mathcal{O}_c}$

is a coding function for \mathbf{O}_c , we can extend it to a coding function $h: \mathcal{O}_a \rightarrow \mathcal{O}_a$ for \mathbf{O}_a . Setting $f' = f \cup h$, we again conclude that f' is a coding function for \mathbf{B}' , and $\langle \mathbf{B}; f \rangle \subset \langle \mathbf{B}'; f' \rangle$ in \mathcal{K} .

Therefore $\mathbf{B} = \mathbf{A}$, and $f: A \rightarrow A$ is a coding function for \mathbf{A} . \square

LEMMA 2.6. *Let $\mathbf{A} \in \mathcal{V}$ be one-generated, and let $h: A \rightarrow A$ be a coding function for \mathbf{A} , with h -initial element a . For all $m \in M$, there is a first order formula $\Phi_m^h(x; y, z)$ in the language of one unary operation such that for all $b, c \in A$,*

$$\mathbf{A} \models m(b) = c \quad \text{iff} \quad \langle A, h \rangle \models \Phi_m^h(a; b, c).$$

Furthermore, if $\mathbf{B} \in \mathcal{V}$ is one-generated, $g: B \rightarrow B$ is a coding function for \mathbf{B} , with g -initial element b , and the structures $\langle \mathbf{A}; h \rangle$ and $\langle \mathbf{B}; g \rangle$ are isomorphic, then for any $u, v \in B$,

$$\mathbf{B} \models m(u) = v \quad \text{iff} \quad \langle B, g \rangle \models \Phi_m^h(b; u, v).$$

Proof. To prove this we first define some auxilliary formulas. Let

$$\mathbf{d}_0(x, y) \quad \text{be} \quad x \approx y$$

and for $i \geq 0$, let

$$\mathbf{d}_{i+1}(x, y) \quad \text{be} \quad \neg \mathbf{d}_i(x, y) \wedge \mathbf{d}_i(f(x), y).$$

Thus for $u, v \in A$, $\langle A, h \rangle \models \mathbf{d}_i(u, v)$ for some i iff $u \xrightarrow{h} v$. Also, for each $u \in A$, there is a unique number, call it $\sigma(u)$ such that

$$\langle A, h \rangle \models \mathbf{d}_{\sigma(u)}(a, u).$$

We can now define $\Phi_m^h(x; y, z)$ to be

$$\bigvee_{u \in A} [\mathbf{d}_{\sigma(u)}(x, y) \wedge \mathbf{d}_{\sigma(m(u))}(x, z)].$$

This is indeed a first order formula in the language of one unary operation, since A is finite, and $\{\sigma(u) : u \in A\}$ is a finite collection of natural numbers.

This formula does the job since for $u, v \in A$,

$$\langle A, h \rangle \models \mathbf{d}_{\sigma(u)}(a, v) \quad \text{iff} \quad u = v,$$

and so,

$$\langle A, h \rangle \models \Phi_m^h(a; u, v) \quad \text{iff} \quad m(u) = v.$$

If the structure $\langle \mathbf{B}; g \rangle$ is isomorphic to $\langle \mathbf{A}; h \rangle$ via the map φ , and b is the g -initial element, then $\varphi(b) = a$, and for any $m \in M$ and $u, v \in B$, we have:

$$\mathbf{B} \models m(u) = v \quad \text{iff} \quad \mathbf{A} \models m(\varphi(u)) = \varphi(v)$$

$$\text{iff} \quad \langle A, h \rangle \models \Phi_m^h(a; \varphi(u), \varphi(v))$$

$$\text{iff} \quad \langle B, g \rangle \models \Phi_m^h(b; u, v). \quad \square$$

Since \mathcal{V} is a locally finite variety, the \mathcal{V} -free algebra on one generator is finite, and in fact is equal in size to M . So, up to isomorphism, there are only finitely many one-generated algebras in \mathcal{V} . It follows that up to isomorphism there are only finitely many structures of the type $\langle \mathbf{A}; f \rangle$, where $\mathbf{A} \in \mathcal{V}$ is one-generated, and $f: A \rightarrow A$ is a coding function for \mathbf{A} . Let

$$\langle \mathbf{A}_1; f_1 \rangle, \dots, \langle \mathbf{A}_l; f_l \rangle$$

be a collection of these structures so that if $\langle \mathbf{B}; g \rangle$ is also such a structure, then it is isomorphic to $\langle \mathbf{A}_i; f_i \rangle$ for some unique $i \leq l$. We say that the type of g as a coding function is i .

LEMMA 2.7. \mathcal{V} is a decidable variety.

Proof. We'll construct formulas that give an interpretation of \mathcal{V} into the decidable variety of mono-unary algebras. Let $\mathbf{A} \in \mathcal{V}$ and let $f: A \rightarrow A$ be a coding function for \mathbf{A} . To make the presentation neater, assume that $A \cap (A \times \omega) = \emptyset$.

Setting I to be the set of f -initial elements of A , we see that I is a generating set for \mathbf{A} , since for all $b \in A$, $a \xrightarrow{f} b$ for some $a \in I$, implying $b \in \mathcal{O}_a$. In fact I is a minimal generating set for \mathbf{A} .

For each $a \in I$, $f|_{\mathcal{O}_a}: \mathcal{O}_a \rightarrow \mathcal{O}_a$ is a coding function for \mathcal{O}_a , and so has some type

$i \leq l$, which we'll denote by $\text{tp}(a)$. Let

$$\text{Fl}(a) = \{\langle a, j \rangle : 1 \leq j \leq \text{tp}(a)\},$$

and let

$$A' = A \cup \bigcup_{a \in I} \text{Fl}(a).$$

Extend f to a function $f' : A' \rightarrow A'$ by

$$f'(\langle a, j \rangle) = a \text{ for } a \in I, \text{ and } j \leq \text{tp}(a).$$

$\mathbf{A}' = \langle A', f' \rangle$ is the mono-unary algebra into which we will interpret \mathbf{A} .

Consider the following formulas;

$$\mathbf{Un}(x) : \exists y(f(y) \approx x)$$

$$\mathbf{Flag}(x) : \neg \mathbf{Un}(x)$$

$$\mathbf{Init}(x) : \exists y(\mathbf{Flag}(y) \wedge f(y) \approx x)$$

for $1 \leq i \leq l$,

$$\begin{aligned} \mathbf{Tp}_i(x) : \mathbf{Init}(x) \wedge \exists y_1, \dots, y_i \left[\left(\bigwedge_{1 \leq j \leq i} f(y_j) \approx x \right) \wedge \left(\bigwedge_{1 \leq j < k \leq i} y_j \neq y_k \right) \right. \\ \left. \wedge \forall z (f(z) \approx x \rightarrow \bigvee_{1 \leq j \leq i} z \approx y_j) \right] \end{aligned}$$

$$\mathbf{Orb}(x; y, z) : \mathbf{Init}(x) \wedge \left(\bigvee_{i \leq \kappa} \mathbf{d}_i(x, y) \right) \wedge \left(\bigvee_{j \leq \kappa} \mathbf{d}_j(x, z) \right)$$

and for $m \in M$,

$$\mathbf{\Gamma}_m(y, z) : \exists x \left(\mathbf{Orb}(x; y, z) \wedge \bigwedge_{0 \leq i \leq l} [\mathbf{Tp}_i(x) \rightarrow \mathbf{\Phi}_m^i(x; y, z)] \right).$$

CLAIM. For $b \in A'$,

- 1) $\mathbf{A}' \models \mathbf{Un}(b)$ iff $b \in A$,
- 2) $\mathbf{A}' \models \mathbf{Flag}(b)$ iff $b = \langle a, j \rangle$ for some $a \in I$ and $j \leq \text{tp}(a)$,

- 3) $\mathbf{A}' \models \mathbf{Init}(b)$ iff $b \in I$,
- 4) $\mathbf{A}' \models \mathbf{Tp}_i(b)$ iff $b \in I$ and $\text{tp}(b) = i$.
- 5) For $a, b, c \in A'$, $\mathbf{A}' \models \mathbf{Orb}(a; b, c)$ iff $a \in I$ and $b, c \in \mathcal{O}_a$.
- 6) For $m \in M$, and $b, c \in A'$, $\mathbf{A}' \models \mathbf{\Gamma}_m(b, c)$ iff $b, c \in A$, and $\mathbf{A} \models m(b) = c$.

Proof. The first four claims follow immediately from our construction of \mathbf{A}' .

For (5), if $\mathbf{A}' \models \mathbf{Orb}(a; b, c)$, then $a \in I$, and $\mathbf{A}' \models \mathbf{d}_i(a, b) \wedge \mathbf{d}_j(a, c)$ for some i, j and so $b, c \in \mathcal{O}_a$. Conversely, if $b, c \in \mathcal{O}_a$ for some $a \in I$, then since $f|_{\mathcal{O}_a}$ is a coding function for \mathbf{O}_a , and a is $f|_{\mathcal{O}_a}$ -initial, there are $i, j \leq \kappa$ such that $\mathbf{A}' \models \mathbf{d}_i(a, b) \wedge \mathbf{d}_j(a, c)$. We should point out that since $\text{Card}(M) = \kappa$ then every one-generated member of \mathcal{V} will have cardinality at most κ .

Finally, for $m \in M$, and $b, c \in A'$,

$$\mathbf{A}' \models \mathbf{\Gamma}_m(b, c)$$

implies $b, c \in \mathcal{O}_a$ for some $a \in I$, with $\text{tp}(a) = i$, and

$$\mathbf{A}' \models \mathbf{\Phi}_m^i(a; b, c).$$

But then

$$\langle \mathcal{O}_a, f'|_{\mathcal{O}_a} \rangle \models \mathbf{\Phi}_m^i(a; b, c),$$

since \mathcal{O}_a is a subuniverse of \mathbf{A}' containing a, b and c , and $\mathbf{\Phi}_m^i$ is preserved under subuniverses. This is equivalent to

$$\mathbf{O}_a \models m(b) = c$$

by Lemma 2.6, since a is $f'|_{\mathcal{O}_a}$ -initial, and $\text{tp}(a) = i$. Thus

$$\mathbf{A} \models m(b) = c.$$

The converse of 6) is handled similarly.

Thus we have interpreted \mathbf{A} into \mathbf{A}' , and it follows that we can interpret any algebra of \mathcal{V} into some mono-unary algebra, using the formulas given above. Therefore since \mathcal{V} is finitely axiomatizable, it is decidable. \square

COROLLARY 2.8. *\mathcal{V} is interpretable into the theory of one unary operation.*

3. Undecidability and nonlinearity

For this section $\mathbf{M} = \mathbf{M}(\mathcal{V})$ is nonlinear. Proposition 1.4 demonstrated that linearity can fail for two distinct reasons, either;

- i) $G_u \neq G$ for some $u \in M$ or,
- ii) \mathbf{M} is not quasi-linear,

In either case, we will establish the (hereditary) undecidability of \mathcal{V} by interpreting the theory of two equivalence relations into \mathcal{V} .

LEMMA 3.1. *If \mathbf{M} is not quasi-linear, but $G_x = G$ for all $x \in M$, then \mathcal{V} is hereditarily undecidable.*

Proof. Since \mathbf{M} is not quasi-linear, then for some $u, v \in M$, we have $u \not\leq v$ and $v \not\leq u$. It follows that $u, v \notin G$, and that the variety \mathcal{V} cannot satisfy any equation of the form

$$ug(x) \approx wv(x)$$

or

$$vg(x) \approx wu(x)$$

for any $w \in M$, and $g \in G$.

The basic idea of the proof is that since u and v are not \leq -comparable, then as unary operations acting on \mathcal{V} -free algebras, they are somewhat unrelated, and so the two equivalence relations defined by the kernels of these operations are also unrelated. This allows us to semantically embed the undecidable theory of two equivalence relations into \mathcal{V} .

Let the structure $\mathbf{A} = \langle A, E_1, E_2 \rangle$ be a set with two equivalence relations E_1 and E_2 on it, and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(A)$ be the \mathcal{V} -free algebra freely generated by the set A . Consider the sets

$$S_1 = \{ \langle u(a), u(b) \rangle : a, b \in A, \text{ and } \langle a, b \rangle \in E_1 \}$$

$$S_2 = \{ \langle v(a), v(b) \rangle : a, b \in A, \text{ and } \langle a, b \rangle \in E_2 \}$$

and the congruence Θ on \mathbf{F} generated by S_1 and S_2 .

CLAIM 1. *For $a \in A$ and $g \in G$, we have*

- i) $g(a)/\Theta = \{g(a)\}$,
- ii) $ug(a)/\Theta = \{ug(b) : b \in A \text{ and } \langle a, b \rangle \in E_1\}$,
- iii) $vg(a)/\Theta = \{vg(b) : b \in A \text{ and } \langle a, b \rangle \in E_2\}$.

Proof. i) If $\text{Card}(g(a)/\Theta) > 1$, then since S_1 and S_2 generate Θ , we can find some $b \in A$, and $w \in M$ such that $g(a) = w(u(b))$ or $g(a) = w(v(b))$. From this it follows that $g = wu$ or $g = wv$ in \mathbf{M} , and so either $u \in G$ or $v \in G$, a contradiction.

ii) Since $G_u = G$, then for $g \in G$, there is some $w \in M$ such that $ug = wu$. From this it follows that

$$B = \{ug(b) : b \in A \text{ and } \langle a, b \rangle \in E_1\} \subseteq ug(a)/\Theta$$

since for $\langle a, b \rangle \in E_1$,

$$\langle ug(a), ug(b) \rangle = \langle w(u(a)), w(u(b)) \rangle, \text{ and } \langle u(a), u(b) \rangle \in S_1.$$

Thus to establish equality, it will suffice to show that B is a block of the congruence Θ . To do this it will be enough to show that if $\langle \mu, \nu \rangle \in S_1 \cup S_2$, $w \in M$, and $w(\mu) \in B$, then so is $w(\nu)$.

First of all, if $\langle \mu, \nu \rangle \in S_2$, say $\langle \mu, \nu \rangle = \langle v(b), v(c) \rangle$, and $w \in M$, then it is impossible for $wv(b)$ to be equal to $ug(d)$ for any $d \in A$, for this would imply that

$$\mathcal{V} \models ug(x) \approx wv(x)$$

forcing

$$ug = wv \text{ in } \mathbf{M}$$

and so

$$u \leq v,$$

a contradiction.

Now suppose $\langle \mu, \nu \rangle \in S_1$, say $\langle \mu, \nu \rangle = \langle u(b), u(c) \rangle$, and $w \in M$ with $wu(b) = ug(d)$ for some $d \in a/E_1$. If $b = d$, then

$$\mathcal{V} \models wu(x) \approx ug(x),$$

implying

$$wu(c) = ug(c) \in B$$

since $\langle a, c \rangle \in E_1$.

On the other hand, if $b \neq d$, then

$$\mathcal{V} \models wu(x) \approx ug(y)$$

implying

$$\mathcal{V} \vDash wu(x) \approx u(y),$$

since g is invertible. But then

$$\mathcal{V} \vDash u(x) \approx u(y),$$

implying

$$u = uv \text{ in } \mathbf{M}$$

and so

$$u \leq v, \text{ a contradiction.}$$

Therefore $B = ug(a)/\Theta$.

iii) The proof is similar to the one given for ii).

Let $\mathbf{A}^* = \mathbf{F}/\Theta \in \mathcal{V}$, and consider the following formulas. Let

$$\mathbf{Un}(x) \text{ be } \forall y \left(\bigwedge_{m \in M \setminus G} m(y) \neq x \right),$$

$$\mathbf{Eq}(x, y) \text{ be } \bigvee_{g \in G} g(x) \approx y,$$

$$\mathbf{E}_1(x, y) \text{ be } \mathbf{Un}(x) \wedge \mathbf{Un}(y) \wedge \exists x'y' (\mathbf{Eq}(x, x') \wedge \mathbf{Eq}(y, y') \wedge u(x') \approx u(y'))$$

and

$$\mathbf{E}_2(x, y) \text{ be } \mathbf{Un}(x) \wedge \mathbf{Un}(y) \wedge \exists x'y' (\mathbf{Eq}(x, x') \wedge \mathbf{Eq}(y, y') \wedge v(x') \approx v(y')).$$

We propose that these formulas provide a way to interpret \mathbf{A} into \mathbf{A}^* . The following claim shows this.

CLAIM 2.

- i) For $\mu \in A^*$, $\mathbf{A}^* \vDash \mathbf{Un}(\mu)$ iff $\mu = g(a)/\Theta$ for some $a \in A$ and $g \in G$.
- ii) $\mathbf{Eq}(x, y)$ defines an equivalence relation on \mathbf{A}^* such that if $\mu, \nu \in A^*$,

then

$$\mathbf{A}^* \vDash \mathbf{Un}(\mu) \wedge \mathbf{Un}(\nu) \wedge \mathbf{Eq}(\mu, \nu)$$

iff

$$\mu = g(a)/\Theta \quad \text{and} \quad \nu = h(a)/\Theta$$

for some $a \in A$, and $g, h \in G$.

iii) For $i = 1, 2$, and $\mu, \nu \in A^*$,

$$\mathbf{A}^* \vDash \mathbf{E}_i(\mu, \nu)$$

iff

$$\mu = g(a)/\Theta \quad \text{and} \quad \nu = h(b)/\Theta$$

for some $h, g \in G$, and $a, b \in A$ with $\langle a, b \rangle \in E_i$.

Proof. i) If $\mu = g(a)/\Theta$, and $m(w(b)/\Theta) = \mu$ for some $m \in M \setminus G$, then

$$\langle mw(b), g(a) \rangle \in \Theta$$

implying

$$mw(b) = g(a) \text{ in } \mathbf{F}$$

and so

$$mw = g \text{ in } \mathbf{M}$$

contradicting

$$m \notin G.$$

Thus

$$\mathbf{A}^* \vDash \mathbf{Un}(\mu), \quad \text{if} \quad \mu = g(a)/\Theta.$$

Conversely, if $\mu = w(a)/\Theta$ for some $w \in M \setminus G$, and $a \in A$, then clearly $\mathbf{A}^* \not\models \mathbf{Un}(\mu)$.

ii) Since \mathbf{G} is a group, $\mathbf{Eq}(x, y)$ defines an equivalence relation on \mathbf{A}^* , and if $\mu = g(a)/\Theta$ and $\nu = h(b)/\Theta$, then

$$\mathbf{A}^* \models \mathbf{Eq}(\mu, \nu)$$

iff

$$g(a)/\Theta = kh(b)/\Theta \text{ for some } k \in G$$

iff

$$a = b \text{ in } A$$

$$\text{since } g(a)/\Theta = \{g(a)\}.$$

iii) Let $i = 1$, and $\mu = g(a)/\Theta$, $\nu = h(b)/\Theta$ for some $g, h \in G$, and $a, b \in A$ with $\langle a, b \rangle \in E_1$. Setting $\mu' = a/\Theta$, and $\nu' = b/\Theta$, we see that

$$\mathbf{A}^* \models \mathbf{Eq}(\mu, \mu') \wedge \mathbf{Eq}(\nu, \nu') \wedge u(\mu') = u(\nu'),$$

since $\langle u(a), u(b) \rangle \in \Theta$. Thus $\mathbf{A}^* \models \mathbf{E}_1(\mu, \nu)$.

Conversely, if

$$\mathbf{A}^* \models \mathbf{E}_1(\mu, \nu),$$

then

$$\mu = g(a)/\Theta \text{ and } \nu = h(b)/\Theta$$

for some $g, h \in G$, $a, b \in A$, and

$$ug'(a)/\Theta = uh'(b)/\Theta$$

for some $g', h' \in G$.

But then it follows from the previous claim that

$$ug' = uh' \text{ in } \mathbf{M}, \text{ and } \langle a, b \rangle \in E_1.$$

The case $i = 2$ is identical.

Thus the structures

$$\mathbf{A} = \langle A, E_1, E_2 \rangle \quad \text{and} \quad \langle \mathbf{Un}^{\mathbf{A}^*}, \mathbf{E}_1^{\mathbf{A}^*}, \mathbf{E}_2^{\mathbf{A}^*} \rangle / \mathbf{Eq}^{\mathbf{A}^*}$$

are isomorphic via the map which sends a in A to the \mathbf{Eq} class in \mathbf{A}^* that contains a/Θ . Since the structure \mathbf{A} was arbitrary, we have provided a scheme for interpreting the theory of two equivalence relations into \mathcal{V} . Since this theory is finitely axiomatizable and undecidable, it follows that \mathcal{V} is hereditarily undecidable. \square

We now present the final lemma needed to prove our main result.

LEMMA 3.2. *If for some $u \in M$, $G_u \neq G$, then \mathcal{V} is hereditarily undecidable.*

Proof. The proof is similar, but more subtle than the proof of the previous lemma. As in that proof, we will interpret the theory of two equivalence relations into \mathcal{V} .

The hypothesis implies that \mathbf{M} is non-linear, and that $G \setminus G_u$ is nonempty. A useful observation is that

$$(*) \quad \mathcal{V} \not\models u(x) \approx u(y),$$

for otherwise, we would have $u = um$ for all $m \in M$, and in particular, $u \leq ug$ for all $g \in G \setminus G_u$, a contradiction.

Let $\mathbf{A} = \langle A, E_1, E_2 \rangle$ be a nonempty set with two equivalence relations E_1 , and E_2 . Let A' be a set disjoint from, but in bijective correspondence with A via the map $a \mapsto a'$, and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(A \cup A')$. Consider the sets

$$\begin{aligned} S_1 &= \{ \langle ug(a), ug(b) \rangle : a, b \in A, g \in G_u \text{ and } \langle a, b \rangle \in E_1 \} \\ S_2 &= \{ \langle ug(a), ug(b) \rangle : a, b \in A, g \in G \setminus G_u \text{ and } \langle a, b \rangle \in E_2 \} \\ S_3 &= \{ \langle g(a'), h(a') \rangle : a \in A \text{ and } g, h \in G \} \\ S_4 &= \{ \langle ug(a'), ug(a) \rangle : a \in A \text{ and } g \in G \setminus G_u \} \end{aligned}$$

and the congruence Θ on \mathbf{F} generated by $S_1 \cup S_2 \cup S_3 \cup S_4$.

CLAIM 1. For $a \in A$ and $g \in G$,

- i) $g(a)/\Theta = \{g(a)\}$,
- ii) $g(a')/\Theta = \{h(a') : h \in G\}$.
- iii) If $g \in G_u$, then $ug(a)/\Theta = \{ug(b) : b \in A, \text{ and } \langle a, b \rangle \in E_1\}$.

iv) If $g \in G \setminus G_u$, then

$$ug(a)/\Theta = \{uh(b): b \in A, h \in G \setminus G_u \text{ and } \langle a, b \rangle \in E_2\} \\ \cup \{uk(b'): b \in A, k \in G \text{ and } \langle a, b \rangle \in E_2\}.$$

Proof. This claim is similar to one from the previous lemma. A complete proof of iii) will be given in order to illustrate the techniques needed to prove this claim.

It is clear that if $g \in G_u$ and $a \in A$, then

$$B = \{ug(b): b \in A, \text{ and } \langle a, b \rangle \in E_1\} \subseteq ug(a)/\Theta.$$

In order to establish equality it suffices to show that B is a block of Θ . To do this it will be enough to show that if $\langle \mu, \nu \rangle \in S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_4^*$, $w \in M$, and $w(\mu) \in B$, then so is $w(\nu)$. A case by case study is required.

Let $\langle \mu, \nu \rangle = \langle uh(b), uh(c) \rangle \in S_1$, with $h \in G_u$ and $\langle b, c \rangle \in E_1$. If $w(\mu) = ug(d) \in B$ for $w \in M$, then

$$wuh(b) = ug(d) \text{ in } \mathbf{F}.$$

Now, $b \neq d$ would force $u(x) \approx u(y)$ to hold in \mathcal{V} , since \mathbf{F} is \mathcal{V} -free, and b and d are generators. This is contrary to $(*)$, and so b must equal d .

Then $\mathcal{V} \models wuh(x) \approx ug(x)$, and thus

$$w(\nu) = wuh(c) = ug(c) \in B \text{ since } b = d \text{ implies } \langle a, c \rangle \in E_1.$$

Let $\langle \mu, \nu \rangle = \langle uh(c), uh(d) \rangle \in S_2 \cup S_4 \cup S_4^*$, with $h \in G \setminus G_u$ and $c, d \in A \cup A'$. If $w(\mu) = ug(d) \in B$ for $w \in M$, then

$$\mathcal{V} \models wuh(x) \approx ug(x),$$

and so

$$wuh = ug \text{ in } \mathbf{M}.$$

Then $u \leq uhg^{-1}$ implying $hg^{-1} \in G_u$. But then $h \in G_u$, since $g \in G_u$, contrary to $h \in G \setminus G_u$.

Finally, let $\langle \mu, \nu \rangle = \langle h(b'), k(b') \rangle \in S_3$ with $b \in A$ and $h, k \in G$. If $w(\mu) = ug(d) \in B$, then

$$\mathcal{V} \models wh(x) \approx ug(y),$$

since $b' \neq d$ are generators of \mathbf{F} . This implies, since g is invertible, that

$$\mathcal{V} \vDash u(x) \approx u(y), \quad \text{contrary to } (*).$$

Thus we have established that B is a block of Θ , and so have shown that $ug(a)/\Theta = B$.

Let $\mathbf{A}' = \mathbf{F}/\Theta$ in \mathcal{V} , and consider the following formulas. Let

$$\mathbf{Gen}(x) \text{ be } \forall y \left(\bigwedge_{m \in M \setminus G} m(y) \neq x \right)$$

$$\mathbf{Eq}(x, y) \text{ be } \bigvee_{g \in G} g(x) \approx y$$

$$\mathbf{Un}(x) \text{ be } \mathbf{Gen}(x) \wedge \exists y (\mathbf{Eq}(x, y) \wedge x \neq y)$$

$$\mathbf{G}_u(x) \text{ be } \mathbf{Un}(x) \wedge \forall y ((\mathbf{Gen}(y) \wedge \neg \mathbf{Un}(y)) \rightarrow u(x) \neq u(y))$$

$$\mathbf{E}_1(x, y) \text{ be } \mathbf{Un}(x) \wedge \mathbf{Un}(y) \wedge \exists x'y' (\mathbf{Eq}(x, x') \wedge \mathbf{Eq}(y, y') \wedge \mathbf{G}_u(x') \wedge \mathbf{G}_u(y') \wedge u(x') \approx u(y'))$$

and

$$\mathbf{E}_2(x, y) \text{ be } \mathbf{Un}(x) \wedge \mathbf{Un}(y) \wedge \exists x'y' (\mathbf{Eq}(x, x') \wedge \mathbf{Eq}(y, y') \wedge \neg \mathbf{G}_u(x') \wedge \neg \mathbf{G}_u(y') \wedge u(x') \approx u(y'))$$

CLAIM 2. Let $\mu, \nu \in A^*$.

- i) $\mathbf{A}^* \vDash \mathbf{Gen}(\mu)$ iff $\mu = g(a)/\Theta$ or $g(a')/\Theta$ for some $a \in A$ and $g \in G$.
- ii) $\mathbf{Eq}(x, y)$ defines an equivalence relation on \mathbf{A}^* .
- iii) $\mathbf{A}^* \vDash \mathbf{Un}(\mu)$ iff $\mu = g(a)/\Theta$ for some $a \in A$ and $g \in G$.
- iv) $\mathbf{A}^* \vDash \mathbf{Un}(\mu) \wedge \mathbf{Un}(\nu) \wedge \mathbf{Eq}(\mu, \nu)$ iff $\mu = g(a)/\Theta$ and $\nu = h(a)/\Theta$ for some $a \in A$ and $g, h \in G$.
- v) $\mathbf{A}^* \vDash \mathbf{G}_u(\mu)$ iff $\mu = h(a)/\Theta$ for some $a \in A$ and $h \in G_u$.
- vi) For $i = 1, 2$, $\mathbf{A}^* \vDash \mathbf{E}_i(\mu, \nu)$ iff $\mu = g(a)/\Theta$, $\nu = h(b)/\Theta$ for some $g, h \in G$ and $a, b \in A$ with $\langle a, b \rangle \in E_i$.

Proof.

- i) This is similar to clause i) of Claim 2 in Lemma 3.1.
- ii) That $\mathbf{Eq}(x, y)$ defines an equivalence relation follows from the fact that \mathbf{G} is a group.
- iii) Let $\mathbf{A}^* \vDash \mathbf{Un}(\mu)$. Then $\mu = g(a)/\Theta$ or $g(a')/\Theta$ for some $a \in A$ and $g \in G$. If $\mu = g(a')/\Theta$, then for all $\lambda \in A^*$ with $\mathbf{A}^* \vDash \mathbf{Eq}(\mu, \lambda)$ we have $\lambda = hg(a')/\Theta$ for some $h \in G$. But then $\mu = \lambda$ in \mathbf{A}^* , since $\langle g(a'), hg(a') \rangle \in$

- Θ . Thus $\mathbf{A}^* \models \mathbf{Un}(\mu)$ forces $\mu = g(a)/\Theta$. The converse is easier, and follows from Claim 1.
- iv) This follows from ii) and iii).
- v) Let $\mathbf{A}^* \models \mathbf{G}_u(\mu)$. Then $\mu = g(a)/\Theta$ for some $a \in A$ and $g \in G$. If $g \notin G_u$, then setting $\lambda = a'/\Theta$ we have $\mathbf{A}^* \models \mathbf{Gen}(\lambda) \wedge \neg \mathbf{Un}(\lambda) \wedge u(\mu) = u(\lambda)$, since $\langle ug(a), u(a') \rangle \in \Theta$ when $g \in G \setminus G_u$ and $a \in A$. But this is contrary to $\mathbf{A}^* \models \mathbf{G}_u(\mu)$, and therefore $g \in G_u$. The converse is similar, and uses the facts about Θ proved in Claim 1.
- vi) If $\mathbf{A}^* \models \mathbf{E}_1(\mu, \nu)$ then $\mu = g(a)/\Theta$, $\nu = h(b)/\Theta$ for some $h, g \in G$ and $a, b \in A$, and for some $g', h' \in G_u$, $ug'(a)/\Theta = uh'(b)/\Theta$ in \mathbf{A}^* . But then $\langle ug'(a), uh'(b) \rangle \in \Theta$, and so by Claim 1, we conclude that $\langle a, b \rangle \in E_1$. The converse is easier, and the claim for $\mathbf{E}_2(x, y)$ is handled similarly.

Thus the structures

$$\mathbf{A} = \langle A, E_1, E_2 \rangle \quad \text{and} \quad \langle \mathbf{Un}^{\mathbf{A}^*}, \mathbf{E}_1^{\mathbf{A}^*}, \mathbf{E}_2^{\mathbf{A}^*} \rangle / \mathbf{Eq}^{\mathbf{A}^*}$$

are isomorphic via the map which sends a in A to the \mathbf{Eq} class in \mathbf{A}^* that contains a/Θ .

As in Lemma 3.1, we can conclude that \mathcal{V} is hereditarily undecidable. \square

COROLLARY 3.3. *If \mathbf{M} is nonlinear, then \mathcal{V} is hereditarily undecidable.*

Proof. This follows from the characterization of linearity given by Proposition 1.4. \square

4. Conclusion

The main result of the paper can now be given. Let \mathcal{V} be a multi-ary, locally finite variety of finite type. \mathcal{V}_{Fin} will denote the class of finite algebras in \mathcal{V} .

THEOREM 4.1. The following are equivalent:

- 1) \mathcal{V} is undecidable
- 2) \mathcal{V} is hereditarily undecidable
- 3) \mathcal{V}_{Fin} is hereditarily undecidable
- 4) $\mathbf{M}(\mathcal{V})$ is nonlinear.

Proof. The only part left to prove is 4) implies 3). We stated above that the theory of two equivalence relations is undecidable, when in fact the class of finite models of this theory is undecidable. Our constructions in Lemmas 3.1 and 3.2 preserve finiteness, and so they actually prove that \mathcal{V}_{Fin} is hereditarily undecidable. \square

COROLLARY 4.2.

- 1) If \mathcal{V} is decidable, then \mathcal{V} is interpretable into the theory of one unary function.
- 2) If \mathcal{V} is undecidable, then the theory of two unary functions is interpretable into \mathcal{V} .

Proof. This follows since the theory of two functions is interpretable into the theory of two equivalence relations and interpretability is a transitive relation. \square

COROLLARY 4.3. *Given a fixed finite type of unary algebras, there is an algorithm to determine whether a finite algebra of that type (appropriately coded) generates a decidable variety.*

After learning of the above results, Professor Lampe of the University of Hawaii informed the author of Professor Sichler's work on multi-unary varieties. Combining Theorem 4.1 with the main result of [8], we obtain the following surprising result.

DEFINITION 4.4. A variety \mathcal{W} is group universal if for all groups \mathbf{G} , there is some $\mathbf{A} \in \mathcal{W}$ with $\mathbf{G} \approx \mathbf{Aut}(\mathbf{A})$.

THEOREM 4.5. *The following are equivalent:*

- 1) \mathcal{V} is undecidable
- 2) \mathcal{V} is group universal
- 3) $\mathbf{M}(\mathcal{V})$ is nonlinear.

Although Professor Sichler proved the equivalence of 2) and 3) without the assumption that \mathcal{V} is locally finite, this assumption is necessary for Theorems 4.1 and 4.5. A counterexample can be constructed using the fact that there is a finitely presented group \mathbf{G} with an undecidable word problem. The multi-unary variety $\mathcal{S}[\mathbf{G}]$ of \mathbf{G} -sets has an undecidable equational theory (using a suitable finite language), and so is undecidable, but $\mathbf{M}(\mathcal{S}[\mathbf{G}]) \approx \mathbf{G}$ is linear.

The complete connection between undecidability and group universality is not yet known. Professor McKenzie has provided the following example which demonstrates that a locally finite undecidable variety of finite type need not be group universal. Let \mathbf{G} be a finite 2 step nilpotent group that satisfies $x^3 = 1$. Let \mathcal{W} be the variety generated by \mathbf{G} . Then

$$\mathcal{W} \models x^3 \approx 1$$

and

$$\mathcal{W} \models x \cdot [y, z] \approx [y, z] \cdot x.$$

Since \mathcal{W} is nonabelian then it is hereditarily undecidable. One can show that if $\mathbf{H} \in \mathcal{W}$, and $\mathbf{Aut}(\mathbf{H})$ is simple, then $\mathbf{Aut}(\mathbf{H})$ is abelian, and so \mathcal{W} cannot be group universal.

REFERENCES

- [1] S. BURRIS and R. MCKENZIE, *Decidability and Boolean Representations*, Memoirs of the AMS. 246 (1981), Vol. 32.
- [2] S. BURRIS and H. P. SANKAPPANAVAR, *A Course in Universal Algebra*, Springer-Verlag, New York, 1981.
- [3] A. EHRENFUCHT, *Decidability of the Theory of One Function*, Notices Amer. Math. Soc. 6 (1959) 268.
- [4] R. MCKENZIE, *Finite Forbidden Lattices*, Universal Algebra and Lattice Theory, Proceedings, Puebla, 1982, Springer Lecture Notes, No. 1004 (1982), 176–205.
- [5] R. MCKENZIE and M. VALERIOTE, *The Structure of Decidable locally Finite Varieties*, Manuscript, 1986.
- [6] J. D. MONK, *Mathematical Logic*, Springer-Verlag, New York, 1976.
- [7] M. O. RABIN, *Decidability of second-order theories and automata on infinite trees*, Trans. Amer. Math. Soc. 141 (1969) 1–35.
- [8] J. SICHLER, *Group-universal Unary Varieties*, Alg. Universalis 11 (1980) 12–21.
- [9] B. A. TRAKHTENBROT, *On recursive separability*, Amer. Math. Soc. Transl. Series 2 23 (1963) 1–5.

*University of California
Berkeley
USA*