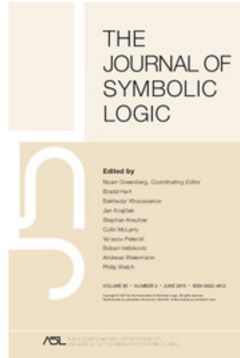

Hereditary undecidability of some theories of finite structures

Ross Willard

The Journal of Symbolic Logic / Volume 59 / Issue 04 / December 1994, pp 1254 - 1262
DOI: 10.2307/2275703, Published online: 12 March 2014

THE JOURNAL OF SYMBOLIC LOGIC
Volume 59, Number 4, December 1994

HEREDITARY UNDECIDABILITY OF SOME THEORIES OF FINITE STRUCTURES

ROSS WILLARD

Abstract. Using a result of Gurevich and Lewis on the word problem for finite semigroups, we give short proofs that the following theories are hereditarily undecidable: (1) finite graphs of vertex-degree at most 3; (2) finite nonvoid sets with two distinguished permutations; (3) finite-dimensional vector spaces over a finite field with two distinguished endomorphisms.

§1. **Introduction.** All theories in this note are first-order, consistent but not necessarily complete, and have finite languages. Let T_1 and T_2 be theories in possibly different languages. We write $T_1 \leq T_2$ to mean there exists $\mathscr{K}_1 \subseteq \mathrm{Mod}(T_1)$ such that $\mathrm{Th}(\mathscr{K}_1) = T_1$ and the members of $\mathscr{K}_1$ are uniformly interpretable by formulas in the models of T_2, as this is defined in [2], [12]. (This variant of Rabin's method [15] allows the use of parameters and definable factor relations.) Also, let $T_1 \equiv T_2$ mean $T_1 \leq T_2 \leq T_1$. $\leq$ induces a partial ordering of the $\equiv$ classes, roughly measuring the complexity of the models of a theory. This ordering is compatible with some of the properties of interest to model theorists: e.g., the classes of theories all of whose models are stable, superstable, or $\aleph_0$-categorical form down-sets with respect to $\leq$. The ordering is known to have a maximum element, represented by the theory of the class $\mathscr{G}$ of graphs, but otherwise has not been explored.

Recent results on the decidability of theories of locally finite varieties are perhaps better stated in terms of $\leq$. For example, the beautiful theorem of McKenzie and Valeriote [12] can be viewed as giving a transparent structural characterization of those finitely generated varieties $\mathscr{V}$ in a finite language satisfying $\mathrm{Th}(\mathscr{V}) \not\equiv \mathrm{Th}(\mathscr{G})$, and reducing the corresponding problem for locally finite varieties to the special case of discriminator varieties. Another example is the ongoing classification of those sufficiently recursive rings R for which the class $\mathscr{M}_R$ of R-modules has a decidable theory. This project, at least when restricted to finite rings, seems (see, e.g. [1], [13], [14]) to amount to classifying R according to whether $\mathrm{Th}(\mathscr{M}_K^{2\,\mathrm{aut}}) \not\leq \mathrm{Th}(\mathscr{M}_R)$ for all finite fields K. (Here $\mathscr{M}_K^{2\,\mathrm{aut}}$ is the class of K-vector spaces with 2 distinguished automorphisms.)

Received June 28, 1993; revised February 1, 1994.

1991 *Mathematics Subject Classification*. Primary 03D35; Secondary 03C13.

Key words and phrases: Undecidable theory, interpretable, finite graphs, finite modules, word problem.

This research was supported by the NSERC of Canada.

Let T_1 be either $\mathrm{Th}(\mathscr{G})$ or $\mathrm{Th}(\mathscr{M}_K^{2\,\mathrm{aut}})$ for some finite field K. T_1 is undecidable (by [16] and [1], [13], respectively), and also finitely axiomatizable. Thus

$$(1) \qquad T_1 \leq T_2 \Rightarrow T_2 \text{ is undecidable.}$$

In general, any theory T_1 satisfying (1) is said to be *hereditarily undecidable*. The two examples in the previous paragraph can also be seen as (partial) affirmations of the following thesis: if $\mathscr{V}$ is a locally finite variety (in a finite language) such that $\mathrm{Th}(\mathscr{V})$ is *not* hereditarily undecidable, then $\mathscr{V}$ has good structure.

Attention among universal algebraists is now turning to the search for structure in arbitrary *pseudovarieties* (classes of finite algebras closed under quotients, subalgebras, and products) whose theories are not hereditarily undecidable [7], [8], [9], [10], [19]. Since $\mathrm{Th}(\mathscr{G}) \not\leq \mathrm{Th}(\mathscr{V})$ and $\mathrm{Th}(\mathscr{M}_K^{2\,\mathrm{aut}}) \not\leq \mathrm{Th}(\mathscr{V})$ if $\mathscr{V}$ is a class of finite structures, hereditary undecidability of a pseudovariety $\mathscr{V}$ lacking structure must be established by other means. In all results currently known to us this is accomplished by showing $\mathrm{Th}(\mathscr{G}_{\mathrm{fin}}) \leq \mathrm{Th}(\mathscr{V})$, where $\mathscr{G}_{\mathrm{fin}}$ denotes the class of all *finite* graphs (whose theory is hereditarily undecidable by [11]).

Our purpose in this note is to give a few more tools for proving the hereditary undecidability of pseudovarieties. Let k-$\mathscr{G}$ denote the class of all graphs of vertex-degree at most k; let n-$\mathscr{P}$ denote the class of all nonvoid sets with n distinguished permutations; for a finite field K let $\mathscr{M}_K^{2\mathrm{end}}$ be the class of all K-vector spaces with two distinguished endomorphisms, and for a class $\mathscr{K}$ let $\mathscr{K}_{\mathrm{fin}}$ denote the class of finite members of $\mathscr{K}$. We prove:

(1) for all $k \geq 3$ and $n \geq 2$, $\mathrm{Th}(k\text{-}\mathscr{G}) \equiv \mathrm{Th}(3\text{-}\mathscr{G}) \equiv \mathrm{Th}(n\text{-}\mathscr{P}) \equiv \mathrm{Th}(2\text{-}\mathscr{P})$ and $\mathrm{Th}(k\text{-}\mathscr{G}_{\mathrm{fin}}) \equiv \mathrm{Th}(3\text{-}\mathscr{G}_{\mathrm{fin}}) \equiv \mathrm{Th}(n\text{-}\mathscr{P}_{\mathrm{fin}}) \equiv \mathrm{Th}(2\text{-}\mathscr{P}_{\mathrm{fin}})$;

(2) each theory in the previous item is hereditarily undecidable;

(3) for each finite field K, $\mathrm{Th}((\mathscr{M}_K^{2\mathrm{end}})_{\mathrm{fin}})$ is hereditarily undecidable.

Item (1) implies that every graph of bounded vertex-degree is superstable, hence $\mathrm{Th}(\mathscr{G}_{\mathrm{fin}}) \not\leq \mathrm{Th}(3\text{-}\mathscr{G})$. Item (3) together with known results proves the hereditary undecidability of $\mathrm{Th}((\mathscr{M}_R)_{\mathrm{fin}})$ for many finite rings R. Items (2) and (3) are proved via a result of Gurevich and Lewis on the word problem for finite semigroups.

§**2. Results.** For $n \geq 2$ let L_n be the language consisting of the n binary relation symbols $R_0, \dots, R_{n-1}$. Let n-$\mathscr{I}$ be the class of all L_n-structures in which each R_i is the graph of a partial injective function. If $\langle A; R_0, \dots, R_{n-1}\rangle \in n\text{-}\mathscr{I}$, then we let $\mathrm{dom}(R_i)$ and $\mathrm{ran}(R_i)$ denote the projections of R_i onto its first and second coordinates, and we write $R_i(a) = b$ to mean $(a,b) \in R_i$.

THEOREM 2.1. *For all $k \geq 3$ and $n \geq 2$,*

(1) $\mathrm{Th}(k\text{-}\mathscr{G}) \equiv \mathrm{Th}(3\text{-}\mathscr{G}) \equiv \mathrm{Th}(n\text{-}\mathscr{I}) \equiv \mathrm{Th}(2\text{-}\mathscr{I}) \equiv \mathrm{Th}(n\text{-}\mathscr{P}) \equiv \mathrm{Th}(2\text{-}\mathscr{P})$;

(2) *Same as the previous item but with each class replaced by its finite members.*

PROOF. Clearly, $\mathrm{Th}(3\text{-}\mathscr{G}) \leq \mathrm{Th}(k\text{-}\mathscr{G})$ and $\mathrm{Th}(n\text{-}\mathscr{P}) \leq \mathrm{Th}(n\text{-}\mathscr{I})$, and similarly for the corresponding classes of finite structures. Therefore, to prove item (1) it will suffice to prove $\mathrm{Th}(k\text{-}\mathscr{G}) \leq \mathrm{Th}((k+1)\text{-}\mathscr{I}), \mathrm{Th}(n\text{-}\mathscr{I}) \leq \mathrm{Th}(2\text{-}\mathscr{P})$, and $\mathrm{Th}(2\text{-}\mathscr{I}) \leq \mathrm{Th}(3\text{-}\mathscr{G})$, and item (2) will follow from the corresponding claims for the finite structures.

We first show $\mathrm{Th}(k\text{-}\mathscr{G}) \leq \mathrm{Th}((k+1)\text{-}\mathscr{I})$. Let $\langle V, E\rangle$ be a graph of vertex-

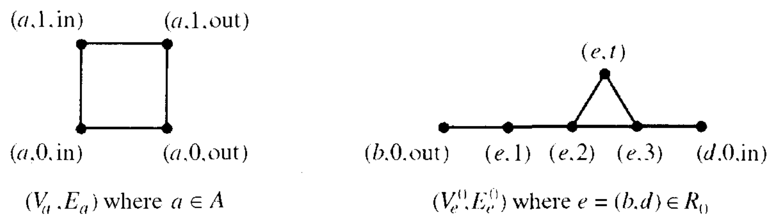

FIGURE 1

degree at most k. By Vizing's theorem (which is true for infinite as well as finite graphs), the edges of $\langle V, E\rangle$ can be $(k+1)$-colored. Choose such a coloring $\chi\colon E \to \{0, 1, \ldots, k\}$. Fix a well-ordering $<$ of V. Now we construct a member of $(k+1)$-$\mathscr{I}$ with universe V by defining $R_i(v) = w$ if and only if $v < w$, $\{v, w\} \in E$, and $\chi(\{v, w\}) = i$. $\langle V, E\rangle$ can be recovered from $\langle V; R_0, \ldots, R_k\rangle$ by means of the following formulas:

$$V(x)\colon x = x,$$

$$E(x, y)\colon \bigvee_{i=0}^{k} [R_i(x) = y \vee R_i(y) = x].$$

This proves both

$$\mathrm{Th}(k\text{-}\mathscr{G}) \leq \mathrm{Th}((k+1)\text{-}\mathscr{I}) \quad \text{and} \quad \mathrm{Th}(k\text{-}\mathscr{G}_{\mathrm{fin}}) \leq \mathrm{Th}((k+1)\text{-}\mathscr{I}_{\mathrm{fin}}).$$

Next we show $\mathrm{Th}(2\text{-}\mathscr{I}) \leq \mathrm{Th}(3\text{-}\mathscr{G})$. Let $\mathbf{A} = \langle A; R_0, R_1\rangle$ be an arbitrary member of 2-$\mathscr{I}$. We shall build a graph $\langle V, E\rangle$ of vertex-degree at most three in which $\mathbf{A}$ can be defined. First, let $\hat{A} = A \times \{0, 1\} \times \{\text{in}, \text{out}\}$, $\hat{R}_0 = R_0 \times \{1, 2, 3, t\}$ and $\hat{R}_1 = R_1 \times \{1', 2', 3', 4', t'\}$. Put $V = \hat{A} \cup \hat{R}_0 \cup \hat{R}_1$. For each $a \in A$ and $e = (b, d) \in R_0$ let $\langle V_a, E_a\rangle$ and $\langle V_e^0, E_e^0\rangle$ be the graphs in Figure 1. Similarly, if $e = (b, d) \in R_1$ then let $\langle V_e^1, E_e^1\rangle$ be built using the vertices $(b, 1, \text{out})$, $(e, 1')$, $(e, 2')$, $(e, 3')$, $(e, 4')$, (e, t'), and $(d, 1, \text{in})$, but this time with $(e, 4')$ connected to $(d, 1, \text{in})$ and the triangle built on $(e, 3')$, $(e, 4')$, and (e, t'). Then E shall be the union of all the E_a's $(a \in A)$ and the E_e^i's $(e \in R_i, i < 2)$. Because R_i is a partial injective function $(i = 0, 1)$ it follows that $\langle V, E\rangle$ has vertex-degree at most three.

It should be clear that $\mathbf{A}$ can be recovered from $\langle V, E\rangle$. To be precise, let $A(x_1, x_2, x_3, x_4)$ be the following formula:

$$A(\bar{x})\colon x_1 E x_2 E x_3 E x_4 E x_1 \wedge x_1 \neq x_3 \wedge x_2 \neq x_4.$$

Then let $\mathrm{Eq}(\bar{x}, \bar{y})$ and $R_0(\bar{x}, \bar{y})$ be formulas asserting:

$$\mathrm{Eq}(\bar{x}, \bar{y})\colon A(\bar{x}) \wedge A(\bar{y}) \wedge \{x_1, \ldots, x_4\} = \{y_1, \ldots, y_4\}$$

$$\begin{aligned} R_0(\bar{x}, \bar{y})\colon & A(\bar{x}) \wedge A(\bar{y}) \\ & \wedge \exists z_0 \exists z_1 \cdots \exists z_5 (|\{z_0, \ldots, z_5\}| = 6 \wedge z_0 E z_1 E z_2 E z_3 E z_4 E z_2 \\ & \qquad \wedge z_3 E z_5 \wedge \{z_0, z_1\} \cap \{x_1, \ldots, x_4\} = \{z_0\} \\ & \qquad\qquad \wedge \{z_3, z_5\} \cap \{y_1, \ldots, y_4\} = \{z_5\}), \end{aligned}$$

and let $R_1(\bar{x}, \bar{y})$ be defined in the obvious analogous way. Then $\theta := \mathrm{Eq}^{\langle V, E\rangle}$ is a factor relation of the L_2-structure $\mathbf{A}' := \langle A^{\langle V, E\rangle}; R_0^{\langle V, E\rangle}, R_1^{\langle V, E\rangle}\rangle$, and $\mathbf{A}'/\theta \cong \mathbf{A}$. The above formulas did not depend in any way on $\mathbf{A}$, which proves $\mathrm{Th}(2\text{-}\mathscr{I}) \leq \mathrm{Th}(3\text{-}\mathscr{G})$. Since in this construction $\langle V, E\rangle$ is finite if $\mathbf{A}$ is, we also get $\mathrm{Th}(2\text{-}\mathscr{I}_{\mathrm{fin}}) \leq \mathrm{Th}(3\text{-}\mathscr{G}_{\mathrm{fin}})$.

Finally, we show $\mathrm{Th}(n\text{-}\mathscr{I}) \leq \mathrm{Th}(2\text{-}\mathscr{P})$. Let $\mathbf{A} = \langle A; R_0, \ldots, R_{n-1}\rangle \in n\text{-}\mathscr{I}$ be given. Our goal is to construct an algebra $\mathbf{B} = \langle B; f, g\rangle$, where f and g are permutations of B and in which $\mathbf{A}$ may be defined. For each $a \in A$ let C_a be the set $\{a\} \times \{0, 1, \ldots, n-1\} \times \{\mathrm{in}, \mathrm{out}\}$ with f and g partially defined as follows:

$$f((a, i, \mathrm{in})) = (a, i, \mathrm{out}),$$

$$g((a, i, \mathrm{in})) = \begin{cases} (a, i+1, \mathrm{in}) & \text{if } i < n-1, \\ (a, n-1, \mathrm{out}) & \text{if } i = n-1, \end{cases}$$

$$g((a, i, \mathrm{out})) = \begin{cases} (a, i-1, \mathrm{out}) & \text{if } i > 0, \\ (a, 0, \mathrm{in}) & \text{if } i = 0. \end{cases}$$

(The reader is advised to draw a picture.) Note that C_a is rigid as a partial bi-unary algebra. Let $\hat{A}$ be the union of all the C_a's.

Next for $i < n$ let $\hat{R}_i = R_i \times \{i\}$, and put $B_0 = \hat{A} \cup \hat{R}_0 \cup \cdots \cup \hat{R}_{n-1}$. Extend f and g by defining, for each $i < n$ and $e = (b, d) \in R_i$,

$$f((b, i, \mathrm{out})) = (e, i), \qquad f((e, i)) = (d, i, \mathrm{in}), \qquad g((e, i)) = (e, i).$$

Note that g is a permutation of B_0 while f, though injective, is only partially defined. Thus, we have not yet finished our construction of $\mathbf{B}$. Nonetheless it may be helpful at this point to say what our formulas will be. Let $A(x_0, \ldots, x_{2n-1})$ be the conjunction of $\bigwedge_{i<j<2n} x_i \neq x_j$ and

$$\begin{aligned} & \bigwedge_{i<n} f(x_i) = x_{n+i} \wedge \bigwedge_{i<n} f(x_{n+i}) \notin \{x_0, \ldots, x_{2n-1}\} \\ & \quad \wedge \bigwedge_{i<n-1} g(x_i) = x_{i+1} \wedge g(x_{n-1}) = x_{2n-1} \\ & \quad \wedge \bigwedge_{i<n-1} g(x_{n+i+1}) = x_{n+i} \wedge g(x_n) = x_0, \end{aligned}$$

while for each $i < n$ let $R_i(\bar{x}, \bar{y})$ be the formula

$$A(\bar{x}) \wedge A(\bar{y}) \wedge \exists z[g(z) = z \wedge f(x_{n+i}) = z \wedge f(z) = y_i].$$

Now we complete the construction of **B**. For each $i < n$ and $a \in A \setminus \mathrm{dom}(R_i)$ choose an infinite set S_a^i and designated element p_a^i, together with unary functions $f = f_a^i$ and $g = g_a^i$ on S_a^i satisfying: (i) g is a bijection; (ii) for all $x \in S_a^i$ and $m < n < \omega$, $g^m(x) \neq g^n(x)$; (iii) f is total and injective; (iv) $\mathrm{ran}(f) = S_a^i \setminus \{p_a^i\}$. Construct the union of B_0 and all of the S_a^i's (making sure the underlying sets are pairwise disjoint), and further extend f by defining $f((a,i,\mathrm{out})) = p_a^i$ if $a \in A \setminus \mathrm{dom}(R_i)$. Then perform the dual construction for each $a \in A \setminus \mathrm{ran}(R_i)$. The resulting structure, which we call **B**, is a member of 2-$\mathscr{P}$ and satisfies $\langle A^{\mathbf{B}}; R_0^{\mathbf{B}}, \ldots, R_{n-1}^{\mathbf{B}} \rangle \cong \mathbf{A}$. This proves $\mathrm{Th}(n\text{-}\mathscr{I}) \leq \mathrm{Th}(2\text{-}\mathscr{P})$.

Unfortunately **B** is infinite even if **A** is finite (unless every R_i happens to be a permutation). Therefore, a different construction is needed to prove $\mathrm{Th}(n\text{-}\mathscr{I}_{\mathrm{fin}}) \leq \mathrm{Th}(2\text{-}\mathscr{P}_{\mathrm{fin}})$. Suppose $\mathbf{A} \in n\text{-}\mathscr{I}_{\mathrm{fin}}$. Let B_0 be defined as before. Fix $i < n$. Because R_i is a partial injective function, and by finiteness, we can pick a bijection $\phi_i \colon A \setminus \mathrm{dom}(R_i) \to A \setminus \mathrm{ran}(R_i)$. For each $a \in \mathrm{dom}(\phi_i)$ add two new points $(a,i,1)$ and $(a,i,2)$, and define $g((a,i,j)) = (a,i,j)$ $(j = 1,2)$ and $f((a,i,\mathrm{out})) = (a,i,1)$, $f((a,i,1)) = (a,i,2)$ and $f((a,i,2)) = (\phi_i(a), i, \mathrm{in})$. Let this be done for all $i < n$, and let **B** be the resulting structure. Again $\mathbf{B} \in 2\text{-}\mathscr{P}$ and $\langle A^{\mathbf{B}}; R_0^{\mathbf{B}}, \ldots, R_{n-1}^{\mathbf{B}} \rangle \cong \mathbf{A}$, and this time **B** is finite. □

Next we describe a result of Gurevich and Lewis [6] which we shall need. A *cancellation semigroup with zero and identity* is a semigroup with zero and identity which satisfies

$$\text{if } xy = xz \neq 0 \text{ or } yx = zx \neq 0, \text{ then } y = z.$$

Let A be the set of quasi-identities valid in all semigroups, and let $\neg FC$ be the set of quasi-identities refuted in some finite cancellation semigroup with zero and identity. Gurevich and Lewis proved that A and $\neg FC$ are recursively inseparable. To prove this, they adopted a specialized version of Turing machines, which among other things requires at least two halting states, one of which is q_1. Then they described an effective procedure which to each such Turing machine M with associated tape symbol set $T = T_0 \cup \{a_0\}$ (a_0 being the blank symbol) assigns a finite semigroup presentation $\langle \Delta; E \rangle$ having several nice properties. In the discussion which follows, we shall let $\langle \Delta; E \rangle$ be exactly as described in [6], *except* that we delete the symbol A_0 from Δ, and we delete the 'initialization rule' $A_0 = \uparrow q_0^0 \uparrow$ from E (so that item (5) below will be true).

We adopt the following notation: Δ^* is the semigroup of all words over the alphabet Δ; $\overset{E}{\sim}$ is the congruence of Δ^* generated by E. (Thus, $\Delta^* / \overset{E}{\sim}$ is the semigroup presented by $\langle \Delta; E \rangle$.) The useful properties of $\langle \Delta; E \rangle$ are:

(1) $T \cup \{\uparrow\} \subseteq \Delta$. ($\uparrow$ is an end-of-tape marker.)

(2) Δ contains a set Q' of symbols, disjoint from $T \cup \{\uparrow\}$, one member being q_0^0. (Q' is in two-to-one correspondence with the set of states of M.)

(3) Δ contains a symbol 0 such that $x0 \overset{E}{\sim} 0x \overset{E}{\sim} 0$ for all $x \in \Delta^*$.

(4) For all $w \in T_0^*$, M on input w halts in state q_1 if and only if $\uparrow q_0^0 w \uparrow \overset{E}{\sim} 0$.

The above items are typical of encodings of Turing machines in semigroup word problems. Next come the special properties. Let

$$Y = \{x \in \Delta^* : x \overset{E}{\not\sim} 0 \text{ and } x \text{ has at most one occurrence of a symbol from } Q'\}.$$

(5) Y is closed under $\overset{E}{\sim}$.

(6) For all $w \in T_0^*$, M on input w halts in a state different from q_1 if and only if $\uparrow q_0^0 w \uparrow \in Y$ and the $\overset{E}{\sim}$-class containing $\uparrow q_0^0 w \uparrow$ is finite.

(7) For all $x, y, z \in \Delta^*$, if $xy, xz \in Y$ and $xy \overset{E}{\sim} xz$, then $y \overset{E}{\sim} z$; and if $yx, zx \in Y$ and $yx \overset{E}{\sim} zx$, then $y \overset{E}{\sim} z$.

(In their paper, Gurevich and Lewis prove items (4) and (6) only when w is the empty word, but their proofs work for all w. Item (5) is an immediate consequence of the definition of E, while item (7) is essentially proved in their analysis of G on page 190. The reader should note the following misprint in [6]: the transition symbols σ_m must be indexed by $m \in (Q' \times T) \cup \{0\}$, and the transition rules must be modified by requiring that $m = \langle q_i^e, a_k \rangle$.)

For each $n < \omega$ let Q_n denote the set of all quasi-identities in the variables $v_0, \ldots, v_{n-1}$ (in the language of semigroups). Recall that A is the set of quasi-identities valid in all semigroups, while $\neg FC$ is the set of quasi-identities refuted in some finite cancellation semigroup with zero and identity. Also, let $\neg F$ be the set of quasi-identities refuted in some finite semigroup. A slight modification of the argument in [6] yields:

LEMMA 2.2. (1) *There exists $n < \omega$ such that $A \cap Q_n$ and $\neg FC \cap Q_n$ are recursively inseparable.*

(2) *$A \cap Q_2$ and $\neg F \cap Q_2$ are recursively inseparable.*

PROOF. Begin by choosing a finite alphabet T_0 and two recursively enumerable subsets U_1, U_2 of T_0^* such that U_1 and U_2 are recursively inseparable. By standard methods it can be shown that there is a Turing machine M of the kind used by Gurevich and Lewis, having exactly two halting states q_1, q_2, and such that for all $w \in T_0^*$, M on input w halts in state q_i if and only if $w \in U_i$ ($i = 1, 2$). Obtain $\langle \Delta; E \rangle$ for M as described above, and let $n = |\Delta|$. We may assume with no loss of generality that $\{v_0, \ldots, v_{n-1}\} = \Delta$. Let ϕ be the conjunction of the relations (equations) in E. For each $w \in T_0^*$ let $\phi_w \in Q_n$ be the quasi-identity $\phi \to (\uparrow q_0^0 w \uparrow = 0)$. We claim that (i) $w \in U_1$ if and only if $\phi_w \in A$, and (ii) if $w \in U_2$ then $\phi_w \in \neg FC$. (i) follows from item (4) above. (ii) is proved as in [6]: if $w \in U_2$ then let W be the $\overset{E}{\sim}$-class containing $\uparrow q_0^0 w \uparrow$ and let X be the set of all subwords (including the empty word) of members of W. X is a finite subset of Y and is closed under $\overset{E}{\sim}$. Let $X^c = \Delta^* \backslash X$; then $X^c / \overset{E}{\sim}$ is an ideal of the semigroup $\Delta^* / \overset{E}{\sim}$. Thus, $X / \overset{E}{\sim} \cup \{0\}$ with the product $(x / \overset{E}{\sim})(y / \overset{E}{\sim})$ defined to be $(xy) / \overset{E}{\sim}$ if $xy \in X$, and 0 otherwise, is a finite semigroup with zero and identity which refutes ϕ_w; moreover, it satisfies the cancellation law by item (7) above. This proves (ii). Since the map $w \mapsto \phi_w$ is effective and sends U_1 into $A \cap Q_n$ and U_2 into $\neg FC \cap Q_n$, it follows that $A \cap Q_n$ and $\neg FC \cap Q_n$ are recursively inseparable.

To prove the second item, choose a two-element alphabet $\{a, b\}$ and let $h\colon \Delta^* \to \{a, b\}^*$ be the injective homomorphism defined by $h(v_i) = ba^{i+1}b$. Let $\langle\{a, b\}; hE\rangle$ be the semigroup presentation obtained by replacing each $x = y \in E$ by $h(x) = h(y)$. Clearly, if $x \in \Delta^*$ and $y' \in \{a, b\}^*$, then $h(x) \overset{hE}{\sim} y'$ if and only if $y' = h(y)$ for some $y \in \Delta^*$ such that $x \overset{E}{\sim} y$. Thus, if $w \in T_0^*$ then M on input w halts in state q_1 if and only if $h(\uparrow q_0^0 w \uparrow) \overset{hE}{\sim} h(0)$, while M on input w halts in state q_2 if and only if $h(\uparrow q_0^0 w \uparrow) \in h(Y)$ and the $\overset{hE}{\sim}$-class containing $h(\uparrow q_0^0 w \uparrow)$ is finite. In the latter case, if X' is the set of all subwords of members of the $\overset{hE}{\sim}$-class containing $h(\uparrow q_0^0 w \uparrow)$, then $X' / \overset{hE}{\sim} \cup \{0\}$ with the obvious multiplication is a finite semigroup satisfying the relations in hE and refuting $h(\uparrow q_0^0 w \uparrow) \overset{hE}{\sim} h(0)$. The reduction to quasi-identities in the previous paragraph shows that $A \cap Q_2$ and $\neg F \cap Q_2$ are recursively inseparable. □

THEOREM 2.3. (1) $\mathrm{Th}(3\text{-}\mathscr{G}_{\mathrm{fin}})$ *and* $\mathrm{Th}(2\text{-}\mathscr{P}_{\mathrm{fin}})$ *are hereditarily undecidable.*

(2) *For each finite field* K, $\mathrm{Th}((\mathscr{M}_K^{2\mathrm{end}})_{\mathrm{fin}})$ *is hereditarily undecidable.*

PROOF. (1) Let n witness the claim in Lemma 2.2.1. Recall that $n\text{-}\mathscr{I}$ is the class of structures $\langle U; R_0, \dots, R_{n-1}\rangle$, where each R_i is the graph of a partial injective function on U. Let $n\text{-}\mathscr{C}$ be the class of algebras $\langle U; f_0, \dots, f_{n-1}; 0\rangle$, where 0 is a constant and each f_i is a unary operation satisfying the axiom

$$f_i(0) = 0 \wedge \forall x \forall y (f_i(x) = f_i(y) \neq 0 \to x = y).$$

Clearly $\mathrm{Th}(n\text{-}\mathscr{C}_{\mathrm{fin}}) \equiv \mathrm{Th}(n\text{-}\mathscr{I}_{\mathrm{fin}})$. Thus by Theorem 2.1 it suffices to prove that $\mathrm{Th}(n\text{-}\mathscr{C}_{\mathrm{fin}})$ is hereditarily undecidable. For each word $\sigma = v_{i_1} \cdots v_{i_k}$ in the variables $v_0, \dots, v_{n-1}$ let $\hat{\sigma}(x)$ be the term $f_{i_1} \cdots f_{i_k}(x)$. If $\psi \in Q_n$ is

$$(\sigma_1 = \tau_1 \wedge \cdots \wedge \sigma_m = \tau_m) \to \sigma_0 = \tau_0,$$

then let $\hat{\psi}$ be the sentence in the language of $n\text{-}\mathscr{C}$ obtained by replacing each $\sigma_i = \tau_i$ with $\forall x[\hat{\sigma}_i(x) = \hat{\tau}_i(x)]$. Clearly, ψ is true of all semigroups if and only if $\models \hat{\psi}$. On the other hand, suppose S is a finite cancellation semigroup with zero and identity which refutes ψ; pick $a_0, \dots, a_{n-1} \in S$ witnessing this. For each $i < n$ define $f_i(x) = a_i x$, and define $\mathbf{S} = \langle S; f_0, \dots, f_{n-1}; 0\rangle$. Then $\mathbf{S} \in n\text{-}\mathscr{C}_{\mathrm{fin}}$. As S has an identity if follows that $S \models \sigma_i(\overline{a}) = \tau_i(\overline{a})$ if and only if $\mathbf{S} \models \forall x[\hat{\sigma}_i(x) = \hat{\tau}_i(x)]$; hence $\mathbf{S}$ refutes $\hat{\psi}$. These remarks together with Lemma 2.2.1 prove that $\mathrm{Th}(n\text{-}\mathscr{C}_{\mathrm{fin}})$ is hereditarily undecidable.

(2) Since every (finite) semigroup can be embedded in the semigroup of all endomorphisms of a (finite-dimensional) K-vector space, the above argument can essentially be repeated (using Lemma 2.2.2 this time) to prove hereditary undecidability of $\mathrm{Th}((\mathscr{M}_K^{2\mathrm{end}})_{\mathrm{fin}})$. □

Here are some comments regarding Theorem 2.3. (i) It is possible that part 1 of the theorem is folklore; if so, then we hope that our presentation of it is sufficiently novel to warrant publication. (ii) In particular, Garfunkel and Shank [5] have claimed (correctly) that the class of finite planar cubic graphs has a hereditarily undecidable theory; however, the proof remains unpublished (cf. [18]). (iii) Part 2 of the theorem together with results in the literature allow one to deduce the hereditary undecidability of $\mathrm{Th}((\mathscr{M}_R)_{\mathrm{fin}})$ for many finite rings R. For example, let p be a prime and put $R = \mathbb{Z}_{p^9}[x : x^2 = 0]$. Baur [1] showed how to interpret $\mathscr{M}^{2\text{end}}_{\mathbb{Z}_p}$ in $\mathscr{M}_R$; the same argument interprets $(\mathscr{M}^{2\text{end}}_{\mathbb{Z}_p})_{\text{fin}}$ in $(\mathscr{M}_R)_{\text{fin}}$.

The hereditary undecidability of both $\mathrm{Th}(\mathscr{M}^{2\,\text{aut}}_K)$ and $\mathrm{Th}((\mathscr{M}^{2\text{end}}_K)_{\text{fin}})$ suggests an obvious problem.

PROBLEM 1. Is $\mathrm{Th}((\mathscr{M}^{2\,\text{aut}}_K)_{\text{fin}})$ hereditarily undecidable, if K is a finite field?

The answer should be yes, but the result of Gurevich and Lewis does not seem to be strong enough to prove it. What is apparently needed is the recursive inseparability of the sets of (i) open formulas in 2 variables (in the language $\{\cdot,{}^{-1}\}$) which are valid in all groups, and (ii) open formulas in 2 variables which are refuted in some finite group. The best result in this direction is due to Slobodskoi [17]: there exists $n < \omega$ such that the sets of (i) open formulas in n variables valid in all *periodic* groups, and (ii) open formulas in n variables refuted in some finite group, are recursively inseparable. Slobodskoi's result can be used to deduce the undecidability (though not the hereditary undecidability) of $\mathrm{Th}((\mathscr{M}^{n\,\text{aut}}_K)_{\text{fin}})$ for sufficiently large n.

Here is another problem, this time concerning discriminator varieties. Recall that a *discriminator variety* is any variety of the form $\mathbf{HSP}(\mathscr{K})$, where $\mathscr{K}$ is a class of algebras satisfying

$$\forall x \forall y \forall z[(t(x,x,z) = z) \;\&\; (x \neq y \to t(x,y,z) = x)]$$

for some term $t(x,y,z)$ in the language of $\mathscr{K}$. We have conjectured that if $\mathscr{V}$ is a locally finite discriminator variety in a finite language, then $\mathrm{Th}(\mathscr{V})$ is undecidable if and only if $\mathrm{Th}(\mathscr{G}) \equiv \mathrm{Th}(\mathscr{V})$. However, the corresponding conjecture for $\mathscr{V}_{\text{fin}}$ may be false. Let $\mathscr{K}$ be the class of all finite algebras $\langle A; b, t\rangle$ where t is the ternary discriminator function on A (i.e., $t(x,y,z) = x$ if $x \neq y, t(x,x,z) = z$), and b is a binary operation satisfying the axiom

$$\begin{aligned} &\forall x \forall y[b(x,y) \in \{x,y\} \wedge (b(x,y) = x \leftrightarrow b(y,x) = y)] \\ &\qquad \wedge \forall x \forall y_1 \forall y_2 \forall y_3 \forall y_4[(b(x,y_1) = b(x,y_2) = b(x,y_3) = b(x,y_4) = x) \\ &\qquad\qquad \to |\{x, y_1, y_2, y_3, y_4\}| < 5]. \end{aligned}$$

Let $\mathscr{V} = \mathbf{HSP}(\mathscr{K})$. $\mathscr{V}$ is locally finite. Since $\mathscr{K}$ coincides with the class of finite models of its universal theory, $\mathscr{V}_{\text{fin}}$ is simply the class of finite direct products of members of $\mathscr{K}$ (see [4, Theorem IV.9.4]). The reader should see that $\mathscr{K}$ is bi-interpretable with $3\text{-}\mathscr{G}_{\text{fin}}$, so $\mathrm{Th}(3\text{-}\mathscr{G}_{\text{fin}}) \leq \mathrm{Th}(\mathscr{V}_{\text{fin}})$. (It can also be shown by the methods in [3] or [20] that $\mathrm{Th}(\mathscr{G}) \equiv \mathrm{Th}(\mathscr{V})$.)

PROBLEM 2. Is it true that $\mathrm{Th}(\mathscr{G}_{\text{fin}}) \not\leq \mathrm{Th}(\mathscr{V}_{\text{fin}})$?

REFERENCES

[1] W. BAUR, *Undecidability of the theory of abelian groups with a subgroup*, ***Proceedings of the American Mathematical Society***, vol. 55 (1976), pp. 125–128.

[2] S. BURRIS and R. MCKENZIE, *Decidability and Boolean representations*, ***Memoirs of the American Mathematical Society***, American Mathematical Society, Providence, Rhode Island, 1981.

[3] S. BURRIS, R. MCKENZIE, and M. VALERIOTE, *Decidable discriminator varieties from unary varieties*, this JOURNAL, vol. 56 (1991), pp. 1355–1368.

[4] S. Burris and H. P. Sankappanavar, ***A course in universal algebra***, Springer-Verlag, New York, 1981.

[5] S. Garfunkel and H. Shank, *On the undecidability of finite planar cubic graphs*, this Journal, vol. 37 (1972), pp. 595–597.

[6] Yu. Gurevich and H. R. Lewis, *The word problem for cancellation semigroups with zero*, this Journal, vol. 49 (1984), pp. 184–191.

[7] P. Idziak, *Varieties with decidable finite algebras I: linearity*, ***Algebra Universalis***, vol. 26 (1989), pp. 234–246.

[8] ———, *Varieties with decidable finite algebras II: permutability*, ***Algebra Universalis***, vol. 26 (1989), pp. 247–256.

[9] J. Jeong, *Finitary decidability implies congruence permutability for congruence modular varieties*, ***Algebra Universalis***, vol. 29 (1992), pp. 441–448.

[10] ———, *Finitely decidable congruence modular varieties*, ***Transactions of the American Mathematical Society***, vol. 339 (1993), pp. 623–642.

[11] I. A. Lavrov, *Effective inseparability of the sets of identically true formulae and finitely refutable formulae for certain elementary theories*, ***Algebra i Logika***, vol. 2 (1963), pp. 5–18. (Russian)

[12] R. McKenzie and M. Valeriote, ***The structure of decidable locally finite varieties***, Birkhäuser, Boston, 1989.

[13] M. Prest, *Model theory and modules*, ***London Mathematical Society Lecture Note Series***, vol. 130, Cambridge University Press, Cambridge, 1988.

[14] ———, *Wild representation type and undecidability*, ***Communications in Algebra***, vol. 19 (1991), pp. 919–929.

[15] M. O. Rabin, *A simple method for undecidability proofs and some applications*, ***Logic, methodology and philosophy of science*** (Y. Bar-Hillel, editor), North-Holland, Amsterdam, 1965.

[16] H. Rogers, *Certain logical reduction and decision problems*, ***Annals of Mathematics***, vol. 64 (1956), pp. 264–284.

[17] A. M. Slobodskoi, *Unsolvability of the universal theory of finite groups*, ***Algebra and Logic***, vol. 20 (1981), pp. 139–156.

[18] A. B. Slomson, *review of* [5], ***Mathematical Reviews***, vol. 47 #4781.

[19] M. Valeriote and R. Willard, *Some properties of finitely decidable varieties*, ***International Journal of Algebra and Computation***, vol. 2 (1992), pp. 89–101.

[20] R. Willard, *Decidable discriminator varieties from unary classes*, ***Transactions of the American Mathematical Society***, vol. 336 (1993), pp. 311–333.

DEPARTMENT OF PURE MATHEMATICS
UNIVERSITY OF WATERLOO
WATERLOO, ONTARIO N2L 3G1, CANADA

E-mail: rdwillar@flynn.uwaterloo.ca