Lattice-theoretic decision problems in universal algebra

Stanley Burris¹) and H. P. Sankappanavar²)

§1. Introduction

As an introduction to our study of lattice-theoretic decision problems perhaps a brief survey of several significant results already in print would be appropriate. In 1949 Tarski [25] showed that the first-order theory of the lattices of subspaces of twodimensional projective geometries (whose points have homogeneous rational coordinates) is undecidable. Decidability questions for the theories of closure algebras and Brouwerian algebras (which appear in the study of topology) were discussed by Grzegorczyk in [8]. Kargapolov [11] initiated the study of decision problems for lattices of subgroups by showing the undecidability of the theory of the class of lattices of subgroups of Abelian groups. (Since subgroups of Abelian groups are normal this result can be viewed as an undecidability result for lattices of congruences of Abelian groups.) The lattices of subgroups of more restricted classes of groups were subsequently analyzed by Kargapolov [11], Kozlov [12] and Taitslin [23]. In [21] Taitslin proved that the theory of the lattice of ideals of a polynomial ring with at least two unknowns is hereditarily undecidable, whereas the case of a polynomial ring in one unknown leads to a decidable theory.

In this paper we continue the above studies by examining lattices of subrings of rings with unity, congruence lattices of semigroups and unary algebras, and lattices of varieties. Several of our theorems are based on results in the theory of lattices of partitions.

§2. The method of semantic embedding for undecidability proofs

In 1964, Rabin [19] presented a method for establishing undecidability. A similar method was used by Ershov and Taitslin (see [5]) to prove the recursive inseparability of $T$ and $T_f$ for a theory $T$ (these terms will be defined below). These elegant methods call for the semantic embedding of one theory into another and generalize techniques of Tarski [24].

A language means a first-order language with equality which has only a finite number of non-logical symbols. We denote by $E(L)$ the set of sentences in a language

¹) Research supported by N.R.C. Grant A7256.
²) Research supported by a Province of Ontario Graduate Fellowship.

Presented by R. McKenzie. Received June 12, 1974. Accepted for publication in final form November 13, 1974.
L. A theory $T$ based on a language $L$ (in short, in $L$) is a subset of $E(L)$ which is closed under logical deduction. A sentence $\sigma \in L$ is called finitely refutable in $T$ if and only if there exists a finite model of $T$ in which $\neg \sigma$ is true. We denote by $T_{\text{fin}}$ the set of all sentences in $L$ which are true of all the finite models of $T$, and $T_f$ denotes the set of all finitely refutable sentences in $L$. (It is obvious that $T_f = E(L) \setminus T_{\text{fin}}$.)

Let $L$ be a language and let $c_1, \ldots, c_n$ be constants not appearing in $L$. We denote by $L[c_1, \ldots, c_n]$ the extension of $L$ obtained by adding the symbols $c_1, \ldots, c_n$ to $L$. If $T$ is a theory in $L$, an inessential extension of $T$ is a theory in $L[c_1, \ldots, c_n]$, for some constants $c_1, \ldots, c_n$, which is the closure of $T$ with respect to logical deduction in $L[c_1, \ldots, c_n]$. If $\mathcal{M}$ is a structure of $L$ with universe $M$ and $a_1, \ldots, a_n \in M$, we denote by $\langle \mathcal{M}; a_1, \ldots, a_n \rangle$ the structure of $L[c_1, \ldots, c_n]$ obtained from $\mathcal{M}$ by the addition of $a_1, \ldots, a_n$ as distinguished elements with the understanding that $c_i$ is interpreted as $a_i$, $1 \leq i \leq n$.

DEFINITION. Let $L$ be a language with $k$ binary predicate symbols $p_1, \ldots, p_k$, $L_1$ another language (not necessarily distinct from $L$) and let $c_1, \ldots, c_n$ be constants not in $L_1$. Let $\delta(x)$ and $\varphi_1(x, y), \ldots, \varphi_k(x, y)$ be formulas of $L_1[c_1, \ldots, c_n]$.

Given a structure $\mathcal{M}_1$, of $L_1$ with universe $M_1$ and $a_1, \ldots, a_n \in M_1$, we define a structure of $L$—denoted by $\mathcal{M}_1(\delta, \varphi_1, \ldots, \varphi_k; a_1, \ldots, a_n)$—induced by $\delta, \varphi_1, \ldots, \varphi_k$ as follows:

$$\mathcal{M}_1(\delta, \varphi_1, \ldots, \varphi_k; a_1, \ldots, a_n) = \langle D; R_1, \ldots, R_k \rangle$$

where

$$D = \{ a \in M_1 : \langle \mathcal{M}_1; a_1, \ldots, a_n \rangle \models \delta(a) \},$$

and

$$R_i = \{ \langle a, b \rangle \in M_1^2 : a, b \in D \text{ and } \langle \mathcal{M}_1; a_1, \ldots, a_n \rangle \models \varphi_i (a, b) \}, \quad i = 1, \ldots, k.$$

We shall now state the basic result we need which is a blending of the theorems of Rabin (see [19], Theorem 1) and of Ershov and Taitslin (see [5], Theorem 3.3.2).

THEOREM 2.1. Let $T$ be a theory in a language $L$ with the property that the sets $T$ and $T_f$ are recursively inseparable. Let $T_1$ be a theory in another (not necessarily distinct from $L$) language $L_1$. Assume that there exist constants $c_1, \ldots, c_n$ not in $L_1$ and formulas $\delta(x), \varphi_1(x, y), \ldots, \varphi_k(x, y)$ of $L_1[c_1, \ldots, c_n]$ such that

1. for every finite model $\mathcal{N}$ of $T$ there exists a finite model $\mathcal{M}_1$ of $T_1$ and elements $a_1, \ldots, a_n$ of $\mathcal{M}_1$ such that the induced structure $\mathcal{M}_1(\delta, \varphi_1, \ldots, \varphi_k; a_1, \ldots, a_n) \cong \mathcal{N}$, and

2. for every model $\mathcal{M}_1$ of $T_1$ and for every $a_1, \ldots, a_n \in M_1$, the induced structure $\mathcal{M}_1(\delta, \varphi_1, \ldots, \varphi_k; a_1, \ldots, a_n)$ is a model of $T$.

Then $T_1$ and $T_{1f}$ are recursively inseparable.

In the rest of the paper, if a theory $T$ and $T_f$ are recursively inseparable then we simply say that $T$ is recursively inseparable.
§3. The elementary theory of partition lattices

Let $\Pi_A$ denote the lattice of all partitions on a set $A$ which, as is well-known, is isomorphic with the lattice of equivalence relations on $A$. Let $L_1$ be the language of lattices with the two binary operation symbols $\vee$ and $\wedge$ as its non-logical symbols. Throughout this section $\mathcal{P}$ denotes the class of all partition lattices. We denote by $\text{Th}(\mathcal{P})$ the theory of $\mathcal{P}$, i.e. the set of all sentences in $L_1$ which are true of every partition lattice.

**Theorem 3.1.** $\text{Th}(\mathcal{P})$ is recursively inseparable.

**Proof.** Let $T''$ be the theory of two equivalence relations. It is shown in Lavrov [13] that $T''$ and $T_j$ are recursively inseparable. Letting $\xi$ be the sentence $\exists x \exists y \exists z \exists w (x \neq y \& x \neq z \& x \neq w \& y \neq z \& y \neq w \& z \neq w)$ we will choose for the $T$ of Theorem 2.1 the theory axiomatized by $T'' \cup \{\xi\}$.

It is easy to write down in $L_1$ formulas Atom$(x)$, Coatom$(x)$ and Max$(x)$ which say respectively that ‘$x$ is an atom’, ‘$x$ is a coatom’ and ‘$x$ is the greatest element’. It is also possible to write down a formula Config$(x)$ in $L_1$ which asserts that ‘for an element $x$ the sublattice of elements less than or equal to $x$ is isomorphic with $\mathcal{M}_3$’ (see Figure 1).

![Fig. 1.](image)

Let $\mathcal{N} = \langle A, R_1, R_2 \rangle$ be a model of $T$, and we choose $\mathcal{M}_1 = \Pi_A$. Let $\pi_{R_1}$ and $\pi_{R_2}$ be the partitions on $A$ associated with $R_1$ and $R_2$. We further pick two new constants $c_1$ and $c_2$, and consider the following formulas in $L_1[c_1, c_2]$, where $x \leq y$ is an abbreviation for $x = x \wedge y$:

\[
\delta(x) \leftrightarrow \text{Coatom}(x) \& \forall y \forall z [(y \neq z \& \text{Atom}(y) \& \text{Atom}(z) \& \\
& \& \text{Max}(x \vee y) \& \text{Max}(x \vee z) \to \text{Config}(y \vee z)],
\]

\[
def
\delta(x) \leftrightarrow \text{Coatom}(x) \& \forall y \forall z [(y \neq z \& \text{Atom}(y) \& \text{Atom}(z) \& \\
& \& \text{Max}(x \vee y) \& \text{Max}(x \vee z) \to \text{Config}(y \vee z)],
\]
and for $i=1, 2$,

$\varphi_1(x, y) \leftrightarrow \delta(x) \& \delta(y) \& [x \neq y \rightarrow \exists z (\text{Atom}(z) \& z \leq c_i \& \\
\& \text{Coatom}(z \lor (x \land y)) \& \neg \delta(z \lor (x \land y)))]$.

Given $a \in A$ we define a partition $\pi_a$ on $A$ by $\pi_a = \{\{a\}, A - \{a\}\}$ which is clearly a coatom (i.e. maximal element $\neq 1$) in $\Pi_A$. We want to single out precisely the coatoms of the form $\pi_a$ with $a \in A$ by a formula in $L_1[c_1, c_2]$, and we claim that the formula $\delta(x)$ does this for us.

**CLAIM 1.** $\Pi_A \vdash \delta(\pi)$ iff $\pi$ is of the form $\pi_a$ for some $a \in A$. To prove this, let $a \in A$ and we first show that $\Pi_A \vdash \delta(\pi_a)$. Since $\xi \in T$ it follows that $|\mathcal{A}| \geq 4$ (as $\mathcal{N}$ is a model of $T$). Let $\pi_1$ and $\pi_2$ be any two distinct atoms in $\Pi_A$ such that $\pi_a \lor \pi_1 = 1 = \pi_a \lor \pi_2$ (where 1 denotes the largest partition). It is clear that we can write $\pi_1$ and $\pi_2$ as

$\pi_1 = \{\{a, e_i\}\} \cup \{\{b\} : b \in A, b \neq a, e_i\}$,

where $e_i \in A - \{a\}$, $i = 1, 2$, and $e_1 \neq e_2$. Then

$\pi_1 \lor \pi_2 = \{\{a, e_1, e_2\}\} \cup \{\{b\} : b \in A, b \neq a, e_1, e_2\}$.

Observe that the elements below $\pi_1 \lor \pi_2$ are precisely $0, \pi_1, \pi_2, \pi_3$ and $\pi_1 \lor \pi_2$, where $0$ is the smallest partition, and

$\pi_3 = \{\{e_1, e_2\}\} \cup \{\{b\} : b \in A, b \neq e_1, e_2\}$.

From this it is easy to see that $[0, \pi_1 \lor \pi_2] \cong M_3$, proving that $\Pi_A \vdash \delta(\pi_a)$. Conversely, suppose $\Pi_A \vdash \delta(\pi)$. We want to show that $\pi = \pi_a$ for some $a \in A$. Assume that $\pi \neq \pi_a$ for any $a \in A$; then $\pi = \{F, A - F\}$ where $F \subseteq A$, $|F| \geq 2$ and $|A - F| \geq 2$, hence there exist elements $f_1, f_2 \in F$ with $f_1 \neq f_2$ and $g_1, g_2 \in A - F$ with $g_1 \neq g_2$. Now consider the following partitions on $A$:

$\pi_i = \{\{f_i, g_i\}\} \cup \{\{b\} : b \in A, b \neq f_i, g_i\}$, $i = 1, 2$.

These are both atoms in $\Pi_A$ and $\pi \lor \pi_i = 1$, $i = 1, 2$. Since $\pi_1 \lor \pi_2 = \{\{f_1, g_1\}, \{f_2, g_2\}\}$

$\cup \{\{b\} : b \in A, b \neq f_1, f_2, g_1, g_2\}$, it follows that $|[0, \pi_1 \lor \pi_2]| = 4$ and hence $[0, \pi_1 \lor \pi_2]$ is not isomorphic with $\mathcal{M}_3$, implying that $\Pi_A \not\vdash \delta(\pi)$ which is a contradiction – hence claim 1 is proved.

It should be noted that $\Pi_A \vdash \delta(\pi)$ iff $\langle \Pi_A ; \pi_{R_1}, \pi_{R_2} \rangle \vdash \delta(\pi)$.

**CLAIM 2.** For $a, b \in A$, $\langle a, b \rangle \in R_i$ iff $\langle \Pi_A ; \pi_{R_1}, \pi_{R_2} \rangle \vdash \varphi_i(\pi_a, \pi_b)$, $i = 1, 2$. The case $a = b$ is trivial, so let $\langle a, b \rangle \in R_i, a \neq b$. Define a partition $\pi$ on $A$ by $\pi = \{\{a, b\}\} \cup \{\{h\} : h \in A, h \neq a, b\}$. Then, for $i = 1, 2$, $\pi$ is an atom and $\pi \leq \pi_{R_i}$. Also $\pi \lor (\pi_a \land \pi_b) = \{\{a, b\}, A - \{a, b\}\}$ which is a coatom and is not of the form $\pi_h$, $h \in A$. This shows that $\langle \Pi_A ;$
\(\pi_1, \pi_2 \models q_1(\pi_a, \pi_b), i = 1, 2\). Conversely, suppose \(q_i(\pi_a, \pi_b)\) is true in \(\langle \Pi_A; \pi_1, \pi_2 \rangle\).

Then there is an atom partition \(\pi = \{c, d\} \cup \{h\} : h \in A, h \neq c, d\), \(c, d \in A\) such that \(\pi \leq \pi_1\) and \(\pi \lor (\pi_a \land \pi_b)\) is a coatom which does not satisfy \(\delta\). From this it follows that \(\{c, d\} = \{a, b\}\), and since \(\pi \leq \pi_1\), we conclude that \(\langle a, b \rangle \in R_1\), proving the claim.

From claims 1 and 2 it is immediately that if \(D = \{\pi_a \in \Pi_A : a \in A\}\) and \(E_1 = \{\langle \pi_a, \pi_b \rangle : \langle \Pi_A; \pi_1, \pi_2 \rangle \models q_1(\pi_a, \pi_b)\}, i = 1, 2\), then \(\langle D, E_1, E_2 \rangle \cong \langle A, R_1, R_2 \rangle\). Thus (1) of Theorem 2.1 holds, and (2) is easily checked, hence the theory of all \(\Pi_A\) with \(|A| \geq 4\) is recursively inseparable. Consequently \(Th(\mathcal{P})\) is recursively inseparable.

In the following corollary \(\text{Mod} T\) denotes the class of all models of a theory \(T\).

**COROLLARY 3.2.** For any infinite set \(A\), \(\Pi_A \notin \text{Mod} Th(\{\pi_n : n \in \omega\})\).

*Proof.* Since the theory \(T\) used in the above theorem is finitely axiomatized and since \(T\) and \(T_f\) are recursively inseparable, it follows that \(T\) and \(T_{\text{fin}}\) are distinct. Hence there exists a sentence \(\sigma\) in the language of \(T\) such that \(\sigma \in T_{\text{fin}}\) and \(\neg \sigma\) is true in some infinite model of \(T\). By Lowenheim-Skolem's Theorem there exists a model \(\mathcal{N}\) of \(T \cup \{\neg \sigma\}\) whose universe has cardinality equal to that of \(A\) and thus we may take \(\mathcal{N}\) to be \(\langle A, R_1, R_2 \rangle\) for suitable \(R_1, R_2\). Now if we let \(\mathcal{M} = \langle \Pi_A; \pi_1, \pi_2 \rangle\) then the induced structure is isomorphic with \(\mathcal{N}\) as shown in the proof of the above theorem. From this it follows that the translate \(t(\sigma)\) of \(\sigma\) into \(L_1\), whereby the quantifiers are relativized to \(\delta(x)\), \(P_i\) is replaced by \(q_i\), and the (inessential) constants \(c_1, c_2\) are replaced by universally quantified variables, fails in \(\Pi_A\), and for \(n \geq 4\) we have \(\Pi_n \models t(\sigma)\).

From this it is easy to see that \(t(\xi \rightarrow \sigma) \in Th(\{\Pi_n : n \in \omega\}) - Th(\Pi_A)\).

The following corollary is an improvement on Theorem 3.1.

**COROLLARY 3.3.** Let \(K_\omega\) be a class consisting of infinitely many distinct finite partition lattices (or infinitely many distinct duals of finite partition lattices.) Then \(Th(K_\omega)\) is recursively inseparable.

*Proof.* Note that any \(\Pi_m, m \in \omega\), is isomorphic to a subinterval of \(\Pi_n\) if \(m < n\).

**COROLLARY 3.4.** \(Th(\Pi_\omega)\) and \(Th(\text{dual of } \Pi_\omega)\) are hereditarily undecidable (i.e. every subtheory is undecidable).

*Proof.* Every finite partition lattice is isomorphic to some interval of \(\Pi_\omega\), so the corollary is immediate.

§4. Rings and algebras over a field

In this section we apply a result of the last section to the theories of lattices of subrings of rings with unity and of lattices of subalgebras of algebras over the field \(\mathbb{Z}_p\) where \(p\) is prime.
LEMMA 4.1. The ring \( \langle Z_p, +, \cdot, -, 0, 1 \rangle \) is primal for every prime \( p \).

Proof. We need to show that every \( n \)-ary function, for \( n \in \omega \), is a polynomial. Let \( f: Z_p^n \rightarrow Z_p \) be a function, and consider the \( n \)-ary polynomial:

\[
p(x_1, x_2, \ldots, x_n) = \sum_{\mathclap{1 \leq i \leq n}} \prod_{\mathclap{1 \leq i \leq n}} \left( \prod_{\mathclap{y \neq a_i}} (x_i - y) \right) \cdot f(a_1, \ldots, a_n).
\]

It is straightforward to verify that \( f(a_1, \ldots, a_n) = p(a_1, \ldots, a_n) \) for \( a_1, \ldots, a_n \in Z_p \), so the lemma is proved.

Let \( n \in \omega \) with \( n \geq 1 \) and let \( p \) be a prime.

DEFINITION. For each subring \( R \) of \( Z_p^n \) we define an equivalence relation \( E(R) \) on \( n \) by

\[
E(R) = \{ \langle i, j \rangle \in n^2 : \forall f(f \in R \rightarrow f(i) = f(j)) \}.
\]

(It is a simple matter to verify that \( E(R) \) is indeed an equivalence relation.)

DEFINITION. For an equivalence relation \( E \) on \( n \) we define a subset \( R(E) \) of \( Z_p^n \) by

\[
R(E) = \{ f \in Z_p^n : f(i) \neq f(j) \rightarrow \langle i, j \rangle \notin E \}.
\]

LEMMA 4.2. \( R(E) \) is a subring of \( Z_p^n \), and \( 1 \in R(E) \).

Proof. Trivially the functions 0 and 1 are in \( R(E) \). Since the members of \( R(E) \) are by definition constant on each equivalence class of \( R \), it is immediate that \( R(E) \) is closed under the operations +, \cdot and −.

LEMMA 4.3. For a subring \( R \subseteq Z_p^n \), \( R = R(E(R)) \) if \( 1 \in R \).

Proof. If \( R \triangleq Z_p \), then \( E(R) \) has just one equivalence class, namely the set \( n \) itself and so the lemma is obviously true. Hence we suppose that \( R \) has at least one element which is not a constant function. It is clear by definition that \( R \subseteq R(E(R)) \). Suppose \( x_A \) denotes the characteristic function of an equivalence class \( A \) of \( E(R) \). Then observe that every member of the ring \( R(E(R)) \) is of the form \( \sum c_i x_{A_i} \) where \( c_i \) is constant and \( A_i \) is an equivalence class of \( E(R) \). Hence the proof of the lemma is complete if we show that the characteristic functions of the equivalence classes of \( E(R) \) belong to \( R \).

Let \( A_i \) be a proper equivalence class of \( E(R) \). For \( j \notin A_i \) choose a function \( f \in R \) such that \( f(k) \neq f(j) \), where \( k \in A_i \). If \( f(k) = 0 \) for \( k \in A_i \), replace \( f \) by \( f + 1 \). Define \( \theta_j: Z_p \rightarrow Z_p \) by \( \theta_j(f(j)) = 0 \), \( \theta_j(f(k)) = 1 \) for \( k \in A_i \), and \( \theta_j \) is arbitrary otherwise. Then by Lemma 4.1 there exists a polynomial \( p(x) \) such that \( \theta_j = p \). From this it follows that \( \theta_j f \in R \).

Since \( x_{A_i} = \prod_{j \in A_i} \theta_j f \), we have that \( x_{A_i} \in R \).
LEMMA 4.4. *If E is an equivalence relation on n then E = E\{R(E)\}.*

Proof. Trivial.

It is obvious that if \( R_1, R_2 \) are subrings of \( Z_p^n \) then \( R_1 \subseteq R_2 \) implies \( E(R_1) \equiv E(R_2) \), and if \( E_1, E_2 \) are equivalence relations on \( n \) then \( E_1 \subseteq E_2 \) implies \( R(E_1) \equiv R(E_2) \). Hence Lemmas 4.3 and 4.4 yield the following.

THEOREM 4.5. The lattice of subrings with unity of \( Z_p^n \) is isomorphic with the dual of \( \Pi_n \).

THEOREM 4.6 Let \( K \) be a class of rings with unity such that \( Z_p^n \in K \) for \( p \) prime and for infinitely many distinct \( n \). If \( T \) is the theory of lattices of subrings with unity of rings in \( K \) then \( T \) is recursively inseparable.

Proof. The theorem is an immediate consequence of Corollary 3.2 and Theorem 4.5.

COROLLARY 4.7. Let \( K \) be a class of algebras over the field \( Z_p \) for \( p \) prime such that \( Z_p^n \in K \) for infinitely many distinct \( n \). If \( T \) is the theory of lattices of subalgebras over \( Z_p \) of algebras in \( K \) then \( T \) is recursively inseparable.

Proof. The corollary follows from Corollary 3.3, Theorem 4.5 and noting that subrings with unity of \( Z_p^n \) are indeed subalgebras over \( Z_p \).

Remark. We note that in Theorem 4.5 only the fact that \( Z_p \) is primal is used. From this observation one can see that the lattice of subalgebras of \( A^n \) where \( A \) is a primal algebra is isomorphic to the dual of \( \Pi_n \) and hence it follows that the theory of the subalgebra lattices of algebras in a variety generated by a primal algebra is recursively inseparable.

COROLLARY 4.8. The theory of the subalgebra lattices of Boolean algebras is recursively inseparable.

Remark. It is interesting to point out that it is a consequence of the results proved in a remarkable paper by Rabin (see \([20]\)) that the theory of congruence lattices of countable Boolean algebras is decidable.

§5. The lattice of varieties of type \( \tau \)

The notation is taken from Grätzer \([7]\). A type \( \tau \) of algebras is a sequence \( \langle n_0, n_1, \ldots, n_\gamma, \ldots \rangle \) of non-negative integers \( n_\gamma, \gamma \in 0(\tau) \), where \( 0(\tau) \) is an ordinal. For every \( \gamma \in 0(\tau) \) there is given an \( n_\gamma \)-ary operation symbol \( f_\gamma \). If \( \tau \) is a type, the multiplicity type \( \mu \) associated with \( \tau \) is \( \mu = \langle m_0, m_1, \ldots, m_i, \ldots \rangle \) where \( m_i \) is the number of \( i \)-ary operations. We denote by \( \mathcal{L}(\tau) \) the lattice of varieties of type \( \tau \) (it is well-known that a precise definition of \( \mathcal{L}(\tau) \) can be given using the deductively closed sets of identities).
THEOREM 5.1. If \(0(\tau) \geq \omega\) or \(\sum i \cdot m_i > 1\) then \(Th(\mathcal{L}(\tau))\) is hereditarily undecidable (i.e. every subtheory is undecidable).

Proof. Suppose \(0(\tau) \geq \omega\) or \(\sum i \cdot m_i > 1\). This implies either \(m_0 \geq \omega\) or \(m_i \geq 2\) or \(m_j \geq 1\) for some \(j \geq 2\). Then \(\mathcal{L}(\tau)\) contains the dual of \(\Pi_\omega\) as an interval as shown by Burris [1]. Hence the result follows from Corollary 3.4.

However, we have some positive results.

THEOREM 5.2. If \(m_0 < \omega\), \(m_i = 0\), \(i \neq 0\) then \(Th(\mathcal{L}(\tau))\) is decidable.

Proof. Observe that \(\mathcal{L}(\tau) \cong \Pi_{m_0}\) which is finite.

THEOREM 5.3. \(Th(\mathcal{L}(\langle 1 \rangle))\) is decidable.

Before proving this theorem we list three well-known theorems and prove some lemmas.

THEOREM 5.4. (Presburger [18]). \(Th(\langle \omega, + \rangle)\) is decidable and hence \(Th(\langle \omega, \preceq \rangle)\) is decidable.

THEOREM 5.5. (Mostowski [15]). \(Th(\langle \omega - \{0\}, 1 \rangle)\) is decidable where ‘\(|\)’ denotes the divisibility relation.

THEOREM 5.6. (Fefferman-Vaught [6]). The theory of the direct product of two algebraic systems is decidable if each factor has a decidable theory.

LEMMA 5.7. Let \(\mathcal{L}\) be a lattice. If \(Th(\langle L, \preceq \rangle)\) is decidable then \(Th(\langle L, \lor, \land \rangle)\) is decidable.

Proof. It is sufficient to observe that the operations \(\lor\) and \(\land\) are explicitly definable in terms of \(\preceq\). For example the following formula \(J(x, y, z)\) defines \(\lor\):

\[
J(x, y, z) \leftrightarrow x \preceq z \land y \preceq z \land \forall w((x \preceq w \land y \preceq w) \rightarrow z \preceq w).
\]

DEFINITION. Let \(P = \langle P, \leq \rangle\) be a poset. We define \(P^*\) to be the poset \(\langle P \cup \{1\}, \leq \rangle\) where \(1\) is a new element adjoined to \(P\) such that every element of \(P\) is less than \(1\) and \(P^*_a\) to be the poset \(\langle P \cup \{0\}, \leq \rangle\) where \(0\) is a new element adjoined to \(P\) such that every element of \(P\) is greater than \(0\).

LEMMA 5.8. \(Th(P)\) is decidable implies \(Th(P^*)\) and \(Th(P^*_a)\) are decidable.

Proof. Enrich the language of posets by adding \(1\) as a constant and consider the following conversion process: if a formula \(\psi\) is of the form \(\exists x \phi(x, y)\) then define \(\psi_1\) as \(\exists x(\phi(1, y) \lor ((x \neq 1) \land \phi(x, y)))\) and if it is of the form \(\forall x \phi(x, y)\) then define \(\psi_1\) as \(\forall x(\phi(1, y) \land ((x \neq 1) \rightarrow \phi(x, y)))\). Now let \(\sigma\) be an arbitrary sentence and we may
suppose that $\sigma$ is in its prenex normal form. Apply the above process first to the innermost quantifier then to the second innermost quantifier etc. until all quantifiers have been relativized to $P$. If an atomic formula in our new sentence is of the form $1 \leq 1$, $x \leq 1$ or $1 \leq x$ then we can replace it with $x = x$ or $x \neq x$ as the first two cases would be true, the third false. The resulting sentence would be equivalent to a sentence about $\mathcal{P}$ in our original language, hence decidable. Thus $Th(\mathcal{P}^*)$ is decidable. Likewise $Th(\mathcal{P}_*^*)$ is decidable.

**Proof of Theorem 5.3.** It is well-known (see Jacobs and Schwabauer [9]) that every proper variety in $\mathcal{L}(\langle 1 \rangle)$ is 1-based and the equation which forms the basis for that variety is in one of the following forms, where $f$ is the fundamental operation:

$$ f^i(x) = f^i + f(x); $$

or

$$ f^i(x) = f^i(y); $$

or

$$ x = y. $$

Thus with each proper variety we can associate a pair $\langle i, j \rangle$ where $i, j \in \omega$. The ordering induced by the set-theoretical containment of the varieties is given by

$$ \langle i, j \rangle \leq \langle i', j' \rangle \text{ iff } i \leq i', \text{ and } j \neq 0 \text{ implies } j \mid j', \text{ and } j \leq j'. $$

From this it follows that $\langle L(\langle 1 \rangle), \leq \rangle \cong (\langle \omega, \leq \rangle \times (\langle \omega - \{0\}, \mid \rangle)_*^*, \text{ where } L(\langle 1 \rangle)$ is the universe of $\mathcal{L}(\langle 1 \rangle)$.

Now from Theorem 5.5 $Th(\langle \omega, \leq \rangle)$ is decidable, and from Theorem 5.5 and Lemma 5.8 $Th((\langle \omega - \{0\}, \mid \rangle)_*^*)$ is decidable. Hence using Theorem 5.6 and Lemma 5.8 we conclude that $Th(\langle L(\langle 1 \rangle), \leq \rangle)$ is decidable. The proof is complete in view of Lemma 5.7.

**THEOREM 5.9.** $Th(\mathcal{L}(\langle 1, 0 \rangle))$ is decidable.

The proof of this theorem depends on the following lemma which is easily verified.

**LEMMA 5.10.** Let $\mathcal{A} = \langle A, R \rangle$ where $R$ is a binary relation and let $\phi(x, y)$ be a formula in the language of $\mathcal{A}$. Furthermore let $\mathcal{B} = \langle \{ \langle a, b \rangle \in A \times A : A = \phi(a, b) \}, R \rangle$. Then $Th(\mathcal{A})$ is decidable implies $Th(\mathcal{B})$ is decidable.

**Proof of Theorem 5.9.** An equational basis of any variety of type $\langle 1, 0 \rangle$ is one of the following, where $a$ is the distinguished constant:

$$ \{ x = x \}; $$
or
\[ \{ f^m(x) = f^{m+k}(x), f^t(a) = f^{t+r}(a) \} \text{ with } t \leq m; \ k, r \neq 0 \text{ and } r \mid_* k \text{ where } \mid_* \text{ is a} \]
\[ \text{'divisibility' relation on } \omega \text{ defined by } r \mid_* k \text{ iff } r \leq k, \text{ and } r \neq 0 \text{ implies } r \mid k; \]
or
\[ \{ f^m(x) = f^t(a) \} \text{ with } t \leq m. \]

Thus with each proper variety we can associate a 4-tuple \( \langle m, k, t, r \rangle \) where \( m, k, t, r \in \omega, t \leq m, r \mid_* k, \) and \( k = 0 \iff r = 0. \) The ordering induced by the ordering of the varieties is given by \( \langle m, k, t, r \rangle \leq \langle m', k', t', r' \rangle \) iff \( m \leq m', k \mid_* k', t \leq t' \text{ and } r \mid_* r'. \) From this it can be seen that \( \mathcal{L}(\langle 1, 0 \rangle) \cong (\mathcal{L}_1 \times \mathcal{L}_2)^* \) where
\[ \mathcal{L}_1 = \langle \{ \langle m, t \rangle : t \leq m \}, \leq \rangle \]
and
\[ \mathcal{L}_2 = \langle \{ \langle k, r \rangle : r \mid_* k \text{ and } (k = 0 \iff r = 0) \}, \mid_* \rangle. \]

From Lemma 5.10 and Theorem 5.6 \( \text{Th}(\mathcal{L}_1 \times \mathcal{L}_2) \) is decidable, hence it follows that \( \text{Th}(\mathcal{L}(\langle 1, 0 \rangle)) \) is decidable.

The cases \( 1 < m_0 < \omega, m_1 = 1 \) and \( m_j = 0 \text{ for } j \geq 2 \) are open. (We strongly suspect \( \text{Th}(\mathcal{L}(\tau)) \) is decidable in these cases.)

§ 6. The theory of congruence lattices of semilattices

By a semilattice we mean a \( \land \)-semilattice and we denote by \( \text{Con } \mathcal{S} \) the congruence lattice of a semilattice \( \mathcal{S}. \) Given \( a \in S, \) define a relation \( \hat{a} \) on \( S \) by \( \langle x, y \rangle \in \hat{a} \iff x \land a = y \land a. \) Papert [17] has shown that \( \text{Con } \mathcal{S} \) is pseudocomplemented and for \( a \in S, \hat{a} \) is a closed element (i.e. \( \hat{a} = \theta^*, \) the pseudocomplement of some \( \theta \in \text{Con } \mathcal{S} \)) in \( \text{Con } \mathcal{S}; \) furthermore the set of all closed elements in \( \text{Con } \mathcal{S} \) forms a Boolean lattice. If \( a \) is an element of a lattice then \( [a] \) denotes the set of all elements which are greater than or equal to \( a. \)

Recall that \( L_1 \) is the language of lattices; in \( L_1 \) we can write down a formula \( \text{Min}(x) \) which asserts that \( x \) is the smallest element. Let us define in \( L_1 \) the formula \( \text{Dense } (x) \) by
\[ \text{Dense}(x) \iff \forall y(\neg \text{Min}(y) \rightarrow \neg \text{Min}(x \land y)). \]

It is useful to note that in a pseudocomplemented lattice an element \( a \) is dense iff \( a^* = 0. \)

We denote by \( \mathcal{C} \) the class of all congruence lattices of semilattices and \( \text{Th}(\mathcal{C}) \) denotes the theory of \( \mathcal{C} \) in \( L_1, \) which of course is the set of all sentences in \( L_1 \) that are true in every member of \( \mathcal{C}. \)

We shall now give another application of Theorem 2.1.
THEOREM 6.1. Th(\mathcal{C}) is recursively inseparable.

Proof. Let us take T to be the theory of an irreflexive, symmetric binary relation R. It is shown in Ershov [5] that T and T_r are recursively inseparable.

Let \mathcal{M} = \langle A, R \rangle be a model of T with |A| \geq 3. With each pair a, b \in A such that \langle a, b \rangle \in R we associate a new symbol t_{ab} and require t_{ab} = t_{ba}. Let A_1 = \{t_{ab} : \langle a, b \rangle \in R\} and let 0 be a new symbol which is neither in A nor in A_1. We now let S = A \cup A_1 \cup \{0\}, and define an operation \wedge : S \times S \to S as follows:

(i) if s \in S, put s \wedge s = s and s \wedge 0 = 0 \wedge s = 0;
(ii) if a, b \in A with a \neq b, put a \wedge b = b \wedge a = 0;
(iii) if a, b \in A, put t_{ab} \wedge a = a \wedge t_{ab} = a;
(iv) if a, b, c \in A, put t_{ab} \wedge t_{ac} = a;

and

(v) if a, b, c, d \in A and \{a, b\} \cap \{c, d\} = \emptyset then define t_{ab} \wedge t_{cd} = 0.

It is easy to see that \wedge is defined for every pair \langle s_1, s_2 \rangle \in S \times S and that \langle S, \wedge \rangle is indeed a semilattice. This construction is illustrated in Figure 2 where A = \{a, b, c, d, e\} and R = \{\langle a, b \rangle, \langle a, c \rangle, \langle b, c \rangle, \langle c, d \rangle, \langle b, a \rangle, \langle c, a \rangle, \langle c, b \rangle, \langle d, c \rangle\}.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{figure2.png}
\caption{Fig. 2.}
\end{figure}

Let us choose \mathcal{M}_1 = \text{Con} \mathcal{S} and consider the following formulas in L_1:

\[ \delta(x) \leftrightarrow \text{Catom}(x) \land \text{Dense}(x), \]

\[ \psi(x, y) \leftrightarrow \delta(x) \land \delta(y) \land \exists z (\text{Dense}(z) \land \text{Catom}(z) \land z > x \land y). \]

CLAIM 1: Con \mathcal{S} \vdash \delta(\theta) if and only if \theta = \hat{a} for some \hat{a} \in A. To prove claim 1, we suppose \theta \in A and show that Con \mathcal{S} \vdash \delta(\hat{a}). It is easy to notice that \hat{a} has precisely two con-
gruence classes, namely \([a]\) and \(S - [a]\), and hence \(\hat{a}\) is a coatom in \(\text{Con} \mathcal{S}\). Since \(\hat{a}\) is closed in \(\text{Con} \mathcal{S}\), it follows that \(\hat{a}\) is not dense in \(\text{Con} \mathcal{S}\); thus \(\text{Con} \mathcal{S} \nvdash \delta(\hat{a})\). Conversely, let \(\text{Con} \mathcal{S} \vdash \delta(\theta)\). Since \(\theta\) is a coatom, \(\theta\) has exactly two congruence classes (as \(\{0, 1\}\) is the only simple semilattice), say \(I\) and \(S - I\). If \(|I \cap A| \geq 2\) and \(|(S - I) \cap A| \geq 2\), then the element \(0\) would belong to each of them and we would have a contradiction. Hence we may suppose, w.l.o.g., that \(|I \cap A| \leq 1\). Let us assume that \(I\) and \(A\) are disjoint. Then \(A \subseteq S - I\) and so \(0 \in S - I\) because \(|A| \geq 3\). From this it immediately follows that \(I \subseteq A_1\). Since the meet of any two distinct elements of \(A_1\) is either an element of \(A\) or the element 0, it follows that \(I = \{t_{ab}\}\) for some \(a, b \in A\). Thus \(\theta\) has two congruence classes, viz. \(\{t_{ab}\}\) and \(S - \{t_{ab}\}\), which implies that \(\theta\) is dense in \(\text{Con} S\), giving a contradiction. So we conclude that \(|I \cap A| = 1\), hence let \(a \in A\) be such that \(I \cap A = \{a\}\). Then \(A - \{a\} \subseteq S - I\) and so \(0 \in S - I\) since \(|A| \geq 3\). If \(t \in S\) is such that \(t > a\) and \(t \in S - I\), then \(\langle t, 0 \rangle \in \theta\) which implies \(\langle a, 0 \rangle \in \theta\) and so \(a \in S - I\), giving a contradiction. So \(t > a\) implies \(t \in I\), i.e. \([a] \subseteq I\). On the other hand if \(s \in S\) is such that \(a \not\leq s\) and \(s \in I\) then \(0 = a \wedge s \in I\) which is impossible. Thus \(I = [a]\) and hence \(\theta = \hat{a}, a \in A\). This proves claim 1.

**CLAIM 2.** For \(\langle a, b \rangle \in A^2, \langle a, b \rangle \in R\) iff \(\text{Con} \mathcal{S} \not\vdash q(\hat{a}, \hat{b})\).

*Proof of claim 2.* Suppose \(\langle a, b \rangle \in R\) and let \(\alpha\) be a congruence with just two classes \(\{t_{ab}\}\) and \(S - \{t_{ab}\}\). Then clearly \(\alpha\) is a coatom which is dense in \(\text{Con} \mathcal{S}\). Since the congruence classes of \(\hat{a} \wedge \hat{b}\) are \([a] \cap [b], [a] \cap (S - [b]), [b] \cap (S - [a])\) and \((S - [a]) \cap (S - [b])\) and since \([a] \cap [b] = \{t_{ab}\}\), it is clear that \(t_{ab} = \hat{a} \wedge \hat{b}\). Observe that \(\alpha \geq t_{ab}\), hence \(\alpha \geq \hat{a} \wedge \hat{b}\) in which the equality clearly does not hold since \(\hat{a} \wedge \hat{b}\) is not maximal. Thus \(\text{Con} \mathcal{S} \not\vdash q(\hat{a}, \hat{b})\). To prove the converse, suppose \(\text{Con} \mathcal{S} \nvdash q(\hat{a}, \hat{b})\). The congruence classes of \(\hat{a} \wedge \hat{b}\) are precisely \([a] \cap [b], [a] \cap (S - [b]), (S - [a]) \cap [b]\) and \((S - [a]) \cap (S - [b])\). Suppose \([a, b] \not\in R\); then \([a] \cap [b]\) is empty and hence we see that the congruence classes of \(\hat{a} \wedge \hat{b}\) are \([a], [b]\) and \(S - ([a] \cap [b])\). Then we assert that if \(\theta\) is any congruence on \(\mathcal{S}\) such that \(\theta \supseteq \hat{a} \wedge \hat{b}\) then \(\theta = \hat{a}\) or \(\theta = \hat{b}\) or \(\theta\) is the greatest congruence on \(\mathcal{S}\). For the only possibilities are:

(i) \(\langle a, b \rangle \in \theta\), which implies \(\langle a, 0 \rangle \in \theta\) and hence \(\theta\) has just one class; so \(\theta\) is the greatest congruence;

(ii) \(\langle a, f \rangle \in \theta\) for some \(f \in S - ([a] \cap [b])\). This means the congruence classes of \(\theta\) are \([b]\) and \(S - [b]\), so \(\theta = \hat{b}\); and

(iii) \(\langle b, f \rangle \in \theta\) for some \(f \in S - ([a] \cap [b])\) which, as in (ii), implies \(\theta = \hat{a}\).

This shows that there is no dense congruence which contains \(\hat{a} \wedge \hat{b}\) because \(\hat{a}, \hat{b}\) and the greatest congruence are all closed in \(\text{Con} \mathcal{S}\). This proves claim 2.

Claims 1 and 2 imply that condition 1 of Theorem 2.1 holds.

On the other hand it is easy to verify that \(\{\langle a, b \rangle: \text{Con} \mathcal{S} \nvdash q(\hat{a}, \hat{b})\}\) is an irreflexive symmetric relation on \(\{\hat{a}: a \in A\}\) which implies that condition 2 of Theorem 2.1 holds. Hence the proof of the theorem is complete.
COROLLARY. Let $K$ be the class of all those lattices $\mathcal{L}$ which have the following properties:

1. $\mathcal{L}$ is upper-semimodular,
2. every interval $[a, b]$ in $\mathcal{L}$ is pseudocomplemented,
3. $\mathcal{L}$ is coatomatic, and
4. $\mathcal{L}$ is an algebraic lattice.

Then $Th(K)$ is recursively inseparable.

Proof. The corollary follows immediately from the theorem and the fact that the congruence lattice of a semilattice has all the properties above (see Papert [17]).

§7. Congruence lattices of semigroups

A variety is an equationally defined class of algebras of the same type. A subvariety of $V$ is a subclass of $V$ which is a variety. It is well known that the subvarieties of $V$ form a lattice which we denote by $\mathcal{L}(V)$. The atoms of $\mathcal{L}(V)$ are called the equationally complete varieties.

In this section we consider only the varieties of semigroups. The following definitions are taken from Evans [4]:

- $\mathcal{L}$ = the lattice of varieties of semigroups, defined by $(\alpha)\colon x(yz) = (xy)z$;
- $Z_l$ = the variety of left-zero semigroups, defined by $\{xy = x, \alpha\}$;
- $Z_r$ = the variety of right-zero semigroups, defined by $\{xy = y, \alpha\}$;
- $C$ = the variety of constant semigroups, defined by $\{xy = zt, \alpha\}$;
- $A_n$ = the variety of all Abelian groups satisfying $x^n = 1$, which may be defined as a variety of semigroups by $\{xy = yx, x^n y = y, \alpha\}$;
- $A_{m, n}$ = the variety of all commutative semigroups defined by $\{x^m = x^{m+n}, xy = yx, \alpha\}$.

We note that $A_{1, 1}$ is the variety of semilattices. It was first shown by Kalicki and Scott [10] that the equationally complete varieties of semigroups are the varieties $Z_l, Z_r, A_{1, 1}, C$ and $A_p$ for $p$ prime.

THEOREM 7.1. Let $V$ be a variety of semigroups which is not a variety of groups. Then the theory of the class of all congruence lattices of semigroups in $V$ is recursively inseparable.

Proof. It is known that a variety of semigroups consists entirely of groups iff it does not contain $Z_l, Z_r, C$ or $A_{1, 1}$ (see Evans [4]). Hence it follows that $V$ contains either $Z_l, Z_r, C$, or $A_{1, 1}$. Now it is easy to see that if $\mathcal{S} \in Z_l$ or $\mathcal{S} \in Z_r$ or $\mathcal{S} \in C$ then any
equivalence relation on $S$ is a congruence on $S$ and hence the congruence lattice of $S$ is isomorphic with the partition lattice on the universe of $S$. Hence by Theorem 3.1 the theory of the congruence lattices of semigroups in $Z_1$, or $Z_{or C}$ is recursively inseparable. Also we have the theory of the class of all congruence lattices of semigroups in $A_{1,1}$ (i.e. of semilattices) is recursively inseparable by Theorem 6.1. From this it follows that the theory of the class of all congruence lattices of semigroups in $V$ is recursively inseparable.

THEOREM 7.2. The theory of the lattice of varieties of semigroups satisfying $xy = yx$ is hereditarily undecidable, as well as the lattice of varieties of semigroups satisfying $x^2 = x^3$.

Proof. It is shown in Burris and Nelson [2] that the lattice of varieties of semigroups satisfying $xy = yx$ contains an interval isomorphic to the dual of $\Pi_m$ for every $m \in \omega$ and in [3] that the lattice for $x^2 = x^3$ has a subinterval isomorphic to the dual of the partition lattice of an infinite set. Hence the theorem follows from Corollary 3.3 and Corollary 3.4.

Remark. Finally we wish to note that the lattice of varieties of commutative monoids is isomorphic to $L(\langle 1 \rangle)$, hence decidable.

§8. Varieties of unary algebras

Let $\mathcal{V}$ be a non-trivial variety of unary algebras of type $\tau$, i.e. $\tau = \langle 1, 1, \ldots \rangle$ and for some $\mathcal{A} \in \mathcal{V}$, $\mathcal{A} \not\approx x = y$. $\mathcal{F}_\tau(\omega)$ denotes the free algebra in $\mathcal{V}$ on the generators $x_0, x_1, \ldots$. Let $P$ denote the set of polynomials of type $\tau$. Define a subset $T$ of $P$ by
$$T = \{p(x_0) \in P: \text{ for } g \in P, \mathcal{F}_\tau(\omega) \not\approx gp(x) = x\}$$
and let $T = \{\langle p(x_i), p(x_j) \rangle: p \in T\} \cup \Delta$ where $\Delta$ is the diagonal relation on $\mathcal{F}_\tau(\omega)$. It is easily verified that $T$ is a congruence on $\mathcal{F}_\tau(\omega)$. For $\pi \in \Pi_\omega$ define a congruence $\theta(\pi)$ on $\mathcal{F}_\tau(\omega)$ by
$$\theta(\pi) = \{\langle p(x_i), p(x_j) \rangle: p \in P, \{i, j\} \subseteq A \text{ for some } A \in \pi\}.$$ 

The following lemma is a slight improvement on a result in Nation [16].

LEMMA 8.1. $\Pi_\omega$ is isomorphic to a subinterval of $\operatorname{Con}(\mathcal{F}_\tau(\omega))$, the congruence lattice of $\mathcal{F}_\tau(\omega)$.

Proof. It is straightforward to verify that the mapping $\pi \rightarrow \theta(\pi) \lor T$ is the desired isomorphism of $\Pi_\omega$ onto the subinterval $[T, \theta(1)]$ of $\operatorname{Con}(\mathcal{F}_\tau(\omega))$, where $I$ is the maximum element of $\Pi_\omega$.

THEOREM 8.2 $\operatorname{Th}(\operatorname{Con}(\mathcal{F}_\tau(\omega)))$ is hereditarily undecidable.

Proof. (Immediate from Lemma 8.1 and Corollary 3.4.)
COROLLARY 8.3. If $K$ is the class of congruence lattices of members of any non-trivial variety of unary algebras then $\text{Th}(K)$ is recursively inseparable.

REFERENCES


University of Waterloo,
Waterloo, Ontario
Canada