

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 two-dimensional 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 Grzegorzczuk 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 Taitlin [23]. In [21] Taitlin 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 Taitlin (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.

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 iff there exists a finite model of T in which $\neg \sigma$ is true. We denote by T_{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, \dots, c_n be constants not appearing in L . We denote by $L[c_1, \dots, c_n]$ the extension of L obtained by adding the symbols c_1, \dots, c_n to L . If T is a theory in L , an *inessential extension* of T is a theory in $L[c_1, \dots, c_n]$, for some constants c_1, \dots, c_n , which is the closure of T with respect to logical deduction in $L[c_1, \dots, c_n]$. If \mathcal{M} is a structure of L with universe M and $a_1, \dots, a_n \in M$, we denote by $\langle \mathcal{M}; a_1, \dots, a_n \rangle$ the structure of $L[c_1, \dots, c_n]$ obtained from \mathcal{M} by the addition of a_1, \dots, 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, \dots, p_k , L_1 another language (not necessarily distinct from L) and let c_1, \dots, c_n be constants not in L_1 . Let $\delta(x)$ and $q_1(x, y), \dots, q_k(x, y)$ be formulas of $L_1[c_1, \dots, c_n]$. Given a structure \mathcal{M}_1 of L_1 with universe M_1 and $a_1, \dots, a_n \in M_1$ we define a *structure of L* – denoted by $\mathcal{M}_1(\delta, q_1, \dots, q_k; a_1, \dots, a_n)$ – induced by δ, q_1, \dots, q_k as follows:

$$\mathcal{M}_1(\delta, q_1, \dots, q_k; a_1, \dots, a_n) = \langle D; R_1, \dots, R_k \rangle$$

where

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

and

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

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 Taitlin (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, \dots, c_n not in L_1 and formulas $\delta(x), q_1(x, y), \dots, q_k(x, y)$ of $L_1[c_1, \dots, c_n]$ 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, \dots, a_n of \mathcal{M}_1 such that the induced structure $\mathcal{M}_1(\delta, q_1, \dots, q_k; a_1, \dots, a_n) \cong \mathcal{N}$, and*
- (2) *for every model \mathcal{M}_1 of T_1 and for every $a_1, \dots, a_n \in M_1$, the induced structure $\mathcal{M}_1(\delta, q_1, \dots, q_k; a_1, \dots, a_n)$ 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 Π_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 $Th(\mathcal{P})$ 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. *$Th(\mathcal{P})$ is recursively inseparable.*

Proof. Let T' be the theory of two equivalence relations. It is shown in Lavrov [13] that T' and T'_f are recursively inseparable. Letting ξ 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 $\text{Atom}(x)$, $\text{Coatom}(x)$ and $\text{Max}(x)$ 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 $\text{Config}(x)$ 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).

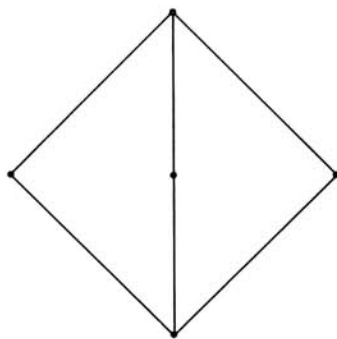


Fig. 1.

Let $\mathcal{N} = \langle A, R_1, R_2 \rangle$ be a model of T , and we choose $\mathcal{M}_1 = \Pi_A$. Let π_{R_1} and π_{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 $x = x \wedge y$:

$$\begin{aligned} \delta(x) \stackrel{\text{def}}{\leftrightarrow} & \text{Coatom}(x) \ \& \ \forall y \forall z [(y \neq z \ \& \ \text{Atom}(y) \ \& \ \text{Atom}(z) \ \& \\ & \ \& \ \text{Max}(x \vee y) \ \& \ \text{Max}(x \vee z)) \rightarrow \text{Config}(y \vee z)], \end{aligned}$$

and for $i=1, 2$,

$$\varrho_i(x, y) \stackrel{\text{def}}{\leftrightarrow} \delta(x) \ \& \ \delta(y) \ \& \ [x \neq y \rightarrow \exists z(\text{Atom}(z) \ \& \ z \leq c_i \ \& \ \text{Coatom}(z \vee (x \wedge y)) \ \& \ \neg \delta(z \vee (x \wedge y)))].$$

Given $a \in A$ we define a partition π_a on A by $\pi_a = \{\{a\}, A - \{a\}\}$ which is clearly a coatom (i.e. maximal element $\neq 1$) in Π_A . We want to single out precisely the coatoms of the form π_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. $\Pi_A \models \delta(\pi)$ iff π is of the form π_a for some $a \in A$. To prove this, let $a \in A$ and we first show that $\Pi_A \models \delta(\pi_a)$. Since $\xi \in T$ it follows that $|A| \geq 4$ (as \mathcal{N} is a model of T). Let π_1 and π_2 be any two distinct atoms in Π_A such that $\pi_a \vee \pi_1 = 1 = \pi_a \vee \pi_2$ (where 1 denotes the largest partition). It is clear that we can write π_1 and π_2 as

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

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

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

Observe that the elements below $\pi_1 \vee \pi_2$ are precisely 0, π_1 , π_2 , π_3 and $\pi_1 \vee \pi_2$, 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 $[0, \pi_1 \vee \pi_2] \cong M_3$, proving that $\Pi_A \models \delta(\pi_a)$. Conversely, suppose $\Pi_A \models \delta(\pi)$. 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 :

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

These are both atoms in Π_A and $\pi \vee \pi_i = 1$, $i=1, 2$. Since $\pi_1 \vee \pi_2 = \{\{f_1, g_1\}, \{f_2, g_2\}\} \cup \{\{b\} : b \in A, b \neq f_1, f_2, g_1, g_2\}$, it follows that $|[0, \pi_1 \vee \pi_2]| = 4$ and hence $[0, \pi_1 \vee \pi_2]$ is not isomorphic with \mathcal{M}_3 , implying that $\Pi_A \not\models \delta(\pi)$ which is a contradiction – hence claim 1 is proved.

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

CLAIM 2. For $a, b \in A$, $\langle a, b \rangle \in R_i$ iff $\langle \Pi_A; \pi_{R_1}, \pi_{R_2} \rangle \models \varrho_i(\pi_a, \pi_b)$, $i=1, 2$. The case $a=b$ is trivial, so let $\langle a, b \rangle \in R_i$, $a \neq b$. Define a partition π on A by $\pi = \{\{a, b\}\} \cup \{\{h\} : h \in A, h \neq a, b\}$. Then, for $i=1, 2$, π is an atom and $\pi \leq \pi_{R_i}$. Also $\pi \vee (\pi_a \wedge \pi_b) = \{\{a, b\}, A - \{a, b\}\}$ which is a coatom and is not of the form π_h , $h \in A$. This shows that $\langle \Pi_A;$

$\pi_{R_1}, \pi_{R_2} \models \varrho_i(\pi_a, \pi_b)$, $i=1, 2$. Conversely, suppose $\varrho_i(\pi_a, \pi_b)$ is true in $\langle \Pi_A; \pi_{R_1}, \pi_{R_2} \rangle$. Then there is an atom partition $\pi = \{\{c, d\}\} \cup \{\{h\}: h \in A, h \neq c, d\}$, $c, d \in A$ such that $\pi \leq \pi_{R_1}$ and $\pi \vee (\pi_a \wedge \pi_b)$ is a coatom which does not satisfy δ . From this it follows that $\{c, d\} = \{a, b\}$, and since $\pi \leq \pi_{R_1}$, we conclude that $\langle a, b \rangle \in R_i$, proving the claim.

From claims 1 and 2 it is immediate that if $D = \{\pi_a \in \Pi_A: a \in A\}$ and $Eq_i = \{\langle \pi_a, \pi_b \rangle: \langle \Pi_A; \pi_{R_1}, \pi_{R_2} \rangle \models \varrho_i(\pi_a, \pi_b)\}$, $i=1, 2$, then $\langle D, Eq_1, Eq_2 \rangle \cong \langle A, R_1, R_2 \rangle$. Thus (1) of Theorem 2.1 holds, and (2) is easily checked, hence the theory of all Π_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_{fin} are distinct. Hence there exists a sentence σ 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 $\mathcal{M}_1 = \langle \Pi_A; \pi_{R_1}, \pi_{R_2} \rangle$ 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 σ into L_1 , whereby the quantifiers are relativized to $\delta(x)$, P_i is replaced by ϱ_i , and the (inessential) constants c_1, c_2 are replaced by universally quantified variables, fails in Π_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_ω 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 Π_m , $m \in \omega$, is isomorphic to a subinterval of Π_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 Π_ω , 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 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:

$$p(x_1, x_2, \dots, x_n) = \sum_{a_1, \dots, a_n} \frac{\prod_{1 \leq i \leq n} (x_i - y)}{\prod_{1 \leq i \leq n} (a_i - y)} \cdot f(a_1, \dots, a_n).$$

It is straightforward to verify that $f(a_1, \dots, a_n) = p(a_1, \dots, a_n)$ for $a_1, \dots, a_n \in Z_p$, 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 $R \cong Z_p$ 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 χ_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 $\sum c_i \chi_{A_i}$ 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 θ_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 $\chi_{A_i} = \prod_{j \notin A_i} \theta_j f$, we have that $\chi_{A_i} \in R$.

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 $E(R_1) \supseteq E(R_2)$, and if E_1, E_2 are equivalence relations on n then $E_1 \subseteq E_2$ implies $R(E_1) \supseteq R(E_2)$. 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 Π_n .*

THEOREM 4.6 *Let K be a class of rings with unity such that $Z_{p_i}^{n_i} \in K$ for p prime and for infinitely many distinct n_i . 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 \mathcal{A}^n where \mathcal{A} is a primal algebra is isomorphic to the dual of Π_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 τ

The notation is taken from Grätzer [7]. A type τ of algebras is a sequence $\langle n_0, n_1, \dots, n_\gamma, \dots \rangle$ 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_γ -ary operation symbol f_γ . If τ is a type, the multiplicity type μ associated with τ is $\mu = \langle m_0, m_1, \dots, m_i, \dots \rangle_{i < \omega}$ where m_i is the number of i -ary operations. We denote by $\mathcal{L}(\tau)$ the lattice of varieties of type τ (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 $m_1 \geq 2$ or $m_j \geq 1$ for some $j \geq 2$. Then $\mathcal{L}(\tau)$ contains the dual of Π_ω 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 $Th(\langle \omega, \leq \rangle)$ is decidable.*

THEOREM 5.5. (Mostowski [15]). *$Th(\langle \omega - \{0\}, | \rangle)$ 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 $Th(\langle L, \leq \rangle)$ is decidable then $Th(\langle L, \vee, \wedge \rangle)$ is decidable.*

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

$$J(x, y, z) \stackrel{\text{def}}{\leftrightarrow} x \leq z \ \& \ y \leq z \ \& \ \forall w((x \leq w \ \& \ y \leq w) \rightarrow z \leq w).$$

DEFINITION. Let $\mathcal{P} = \langle P, \leq \rangle$ be a poset. We define \mathcal{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 \mathcal{P}_* 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. *$Th(\mathcal{P})$ is decidable implies $Th(\mathcal{P}^*)$ and $Th(\mathcal{P}_*)$ are decidable.*

Proof. Enrich the language of posets by adding 1 as a constant and consider the following conversion process: if a formula ψ is of the form $\exists x \phi(x, \bar{y})$ then define ψ_1 as $\exists x(\phi(1, \bar{y}) \vee ((x \neq 1) \ \& \ \phi(x, \bar{y})))$ and if it is of the form $\forall x \phi(x, \bar{y})$ then define ψ_1 as $\forall x(\phi(1, \bar{y}) \ \& \ ((x \neq 1) \rightarrow \phi(x, \bar{y})))$. Now let σ be an arbitrary sentence and we may

suppose that σ 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:

$$f^i(x) = f^{i+j}(x);$$

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 $\langle L(\langle 1 \rangle), \leq \rangle \cong (\langle \omega, \leq \rangle \times (\langle \omega - \{0\}, \mid \rangle)_*)^*$, 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 $\mathcal{B} = \langle \{ \langle a, b \rangle \in A \times A : A \models \phi(a, b) \}, R \rangle$. 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

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

or

$\{f^m(x)=f^t(a)\}$ 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 $k=0 \leftrightarrow r=0$. 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 $m \leq m'$, $k \mid_* k'$, $t \leq t'$ 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

$$\mathcal{L}_2 = \langle \{ \langle k, r \rangle : r \mid_* k \text{ \& } (k=0 \leftrightarrow r=0) \}, \mid_* \rangle.$$

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

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

§6. The theory of congruence lattices of semilattices

By a semilattice we mean a \wedge -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 $x \wedge a = y \wedge a$. 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

$$\text{Dense}(x) \stackrel{\text{def}}{\leftrightarrow} \forall y (\neg \text{Min}(y) \rightarrow \neg \text{Min}(x \wedge y)).$$

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 $Th(\mathcal{C})$ 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_f 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 $\wedge : S \times S \rightarrow S$ 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 $R = \{\langle a, b \rangle, \langle a, c \rangle, \langle b, c \rangle, \langle c, d \rangle, \langle b, a \rangle, \langle c, a \rangle, \langle c, b \rangle, \langle d, c \rangle\}$.

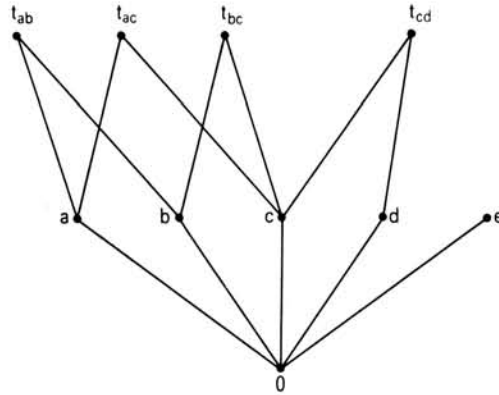


Fig. 2.

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

$$\stackrel{\text{def}}{\delta(x)} \leftrightarrow \text{Coatom}(x) \ \& \ \text{Dense}(x),$$

$$\stackrel{\text{def}}{\varrho(x, y)} \leftrightarrow \delta(x) \ \& \ \delta(y) \ \& \ \exists z (\text{Dense}(z) \ \& \ \text{Coatom}(z) \ \& \ z > x \wedge y).$$

CLAIM 1: $\text{Con } \mathcal{S} \models \delta(\theta)$ iff $\theta = \hat{a}$ for some $a \in A$. To prove claim 1, we suppose $a \in A$ and show that $\text{Con } \mathcal{S} \models \delta(\hat{a})$. 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 $\text{Con } \mathcal{S} \models \delta(\hat{a})$. Conversely, let $\text{Con } \mathcal{S} \models \delta(\theta)$. Since θ is a coatom, θ 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 θ has two congruence classes, viz. $\{t_{ab}\}$ and $S - \{t_{ab}\}$, which implies that θ is dense in $\text{Con } \mathcal{S}$, 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. $[a] \in I$. 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 $\text{Con } \mathcal{S} \models \varrho(\hat{a}, \hat{b})$.

Proof of claim 2. Suppose $\langle a, b \rangle \in R$ and let α be a congruence with just two classes $\{t_{ab}\}$ and $S - \{t_{ab}\}$. Then clearly α 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 $\hat{a} \wedge \hat{b} = \hat{t}_{ab}$. Observe that $\alpha \geq \hat{t}_{ab}$, 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 $\text{Con } \mathcal{S} \models \varrho(\hat{a}, \hat{b})$. To prove the converse, suppose $\text{Con } \mathcal{S} \models \varrho(\hat{a}, \hat{b})$. 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 $\langle a, b \rangle \notin R$; then $[a] \cap [b]$ is empty and hence we see that the congruence classes of $\hat{a} \wedge \hat{b}$ are $[a]$, $[b]$ and $S - ([a] \cup [b])$. Then we assert that if θ is any congruence on \mathcal{S} such that $\theta > \hat{a} \wedge \hat{b}$ then $\theta = \hat{a}$ or $\theta = \hat{b}$ or θ 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 θ has just one class, so θ is the greatest congruence;

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

(iii) $\langle b, f \rangle \in \theta$ for some $f \in S - ([a] \cup [b])$ 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 $\{\langle \hat{a}, \hat{b} \rangle : \text{Con } \mathcal{S} \models \varrho(\hat{a}, \hat{b})\}$ 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 coatomistic, 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 $(\alpha): x(yz) = (xy)z$;

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 \mathcal{S} and hence the congruence lattice of \mathcal{S} is isomorphic with the partition lattice on the universe of \mathcal{S} . Hence by Theorem 3.1 the theory of the congruence lattices of semigroups in Z_b , or Z_r 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 Π_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 $\mathcal{L}(\langle 1 \rangle)$, hence decidable.

§8. Varieties of unary algebras

Let \mathcal{V} be a non-trivial variety of unary algebras of type τ , i.e. $\tau = \langle 1, 1, \dots \rangle$ and for some $\mathcal{A} \in \mathcal{V}$, $\mathcal{A} \not\models x = y$. $\mathcal{F}_{\mathcal{V}}(\omega)$ denotes the free algebra in \mathcal{V} on the generators x_0, x_1, \dots . Let \mathbf{P} denote the set of polynomials of type τ . Define a subset \mathbf{T} of \mathbf{P} by

$$\mathbf{T} = \{p(x_0) \in \mathbf{P} : \text{for } g \in \mathbf{P}, \mathcal{F}_{\mathcal{V}}(\omega) \not\models gp(x) = x\}$$

and let $T = \{\langle p(x_i), p(x_j) \rangle : p \in \mathbf{T}\} \cup \Delta$ where Δ is the diagonal relation on $\mathcal{F}_{\mathcal{V}}(\omega)$. It is easily verified that T is a congruence on $\mathcal{F}_{\mathcal{V}}(\omega)$. For $\pi \in \Pi_{\omega}$ define a congruence $\theta(\pi)$ on $\mathcal{F}_{\mathcal{V}}(\omega)$ by

$$\theta(\pi) = \{\langle p(x_i), p(x_j) \rangle : p \in \mathbf{P}, \{i, j\} \subseteq A \text{ for some } A \in \pi\}.$$

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

LEMMA 8.1. *Π_{ω} is isomorphic to a subinterval of $\text{Con}(\mathcal{F}_{\mathcal{V}}(\omega))$, the congruence lattice of $\mathcal{F}_{\mathcal{V}}(\omega)$.*

Proof. It is straightforward to verify that the mapping $\pi \rightarrow \theta(\pi) \vee T$ is the desired isomorphism of Π_{ω} onto the subinterval $[T, \theta(1)]$ of $\text{Con}(\mathcal{F}_{\mathcal{V}}(\omega))$, where 1 is the maximum element of Π_{ω} .

THEOREM 8.2 *$\text{Th}(\text{Con}(\mathcal{F}_{\mathcal{V}}(\omega)))$ 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

- [1] S. Burris, *On the structure of the lattice of equational classes $\mathcal{L}(\tau)$* , Alg. Univ. 1. (1971), 39–45.
- [2] S. Burris and E. Nelson, *Embedding the dual of Π_m in the lattice of equational classes of commutative semigroups*, Proc. Amer. Math. Soc. 30 (1971), 37–39.
- [3] S. Burris and E. Nelson, *Embedding the dual of Π_∞ in the lattice of equational classes of semigroups*, Alg. Univ. 1 (1971), 248–253.
- [4] T. Evans, *The lattice of semigroup varieties*, Semigroup Forum 2 (1971), 1–43.
- [5] Y. L. Ershov, I. A. Lavrov, A. D. Taimanov, and M. A. Taitlin, *Elementary theories*, Russian Math. Surveys 20 (1965), 35–105.
- [6] S. Feferman and R. L. Vaught, *The first order properties of products of algebraic systems*, Fund. Math. 47 (1959), 57–103.
- [7] G. Grätzer, 'Universal Algebra', Van Nostrand, Princeton, New Jersey, 1968.
- [8] G. Grzegorzcyk, *Undecidability of some topological theories*, Fund. Math. 38 (1951), 137–152.
- [9] E. Jacobs and R. Schwabauer, *The lattice of equational classes of algebras with one unary operation*, Amer. Math. Monthly 71 (1964), 151–155.
- [10] J. Kalicki and D. Scott, *Equational completeness of abstract algebras*, Nederl. Akad. Wetensch. Proc. Ser. A 58 (1955), 650–659.
- [11] M. I. Kargapolov, *On the elementary theory of lattices of subgroups*, Algebra i Logika 1 (1962), 46–53.
- [12] G. T. Kozlov, *The undecidability of the theory of lattices of subgroups of finite abelian p -groups*, Algebra and Logic 9 (1970), 167–171.
- [13] I. A. Lavrov, *Effective inseparability of the sets of identically true formulae and finitely refutable formulae for certain elementary theories*, Algebra i Logika 2 (1963), 39–45.
- [14] R. McKenzie, *Negative solution of the decision problem for sentences true in every subalgebra of $\langle N, + \rangle$* , J. Symbolic Logic 36 (1971), 607–609.
- [15] A. Mostowski, *On direct products of theories*, J. Symbolic Logic 17 (1952), 1–31.
- [16] J. B. Nation, *Congruence lattices of relatively free unary algebras*, (preprint).
- [17] D. Papert, *Congruence relations in semilattices*, J. London Math. Soc. 39 (1964), 723–729.
- [18] M. Presburger, *Über die Vollständigkeit eines gewissen systems der Arithmetik ganzer Zahlen, in welchen die Addition als einzige operation hervortritt*, Comptes-rendus du I Congres des Mathematiciens des Pays Slaves, Warsaw 1930, 92–101, 395.
- [19] M. O. Rabin, *A simple method for undecidability proofs and some applications*, Logic, Methodology and Philosophy of science, Proceedings of the 1964 International Congress, Bar Hillel ed., Amsterdam 1965, 58–68.
- [20] M. O. Rabin, *Decidability of second-order theories and automata on infinite trees*, Trans. Amer. Math. Soc. 141 (1964), 1–34.
- [21] M. A. Taitlin, *Elementary lattice theories for ideals in polynomial rings*, Algebra and Logic 7 (1968), 127–129.
- [22] M. A. Taitlin, *On simple ideals in polynomial rings*, Algebra and Logic 7(1968), 394–395.
- [23] M. A. Taitlin, *On elementary theories of lattices of subgroups*, Algebra and Logic 9 (1970), 285–290.
- [24] A. Tarski, R. M. Robinson, and A. Mostowski, 'Undecidable Theories', Amsterdam 1953.
- [25] A. Tarski, *Undecidability of the theories of lattices and projective geometries*, J. Symbolic Logic 14 (1949), 77–78.

University of Waterloo,
Waterloo, Ontario
Canada