# THE UNDECIDABILITY OF THE WORD PROBLEMS FOR PROJECTIVE GEOMETRIES AND MODULAR LATTICES([1])

BY

## L. LIPSHITZ

ABSTRACT. We show that the restricted word problems for finite-dimensional projective geometries and finite modular lattices and the word problem for modular lattices are undecidable.

1. **Introduction.** In this paper we shall show the undecidability of the restricted word problem (see definitions below) for (i) modular lattices, (ii) finite-dimensional projective geometries (over any field), and (iii) finite modular lattices. From (i) it then follows that there is a finitely presented modular lattice with undecidable word problem. I would like to thank my adviser, Simon Kochen, who suggested these problems to me.

These results should be compared with the following results. In [9] Whitman gave a decision procedure for the restricted word problem for lattices and in [6] McKinsey showed that the open theory of lattices is the same as the open theory of finite lattices, which immediately gives a decision procedure for this open theory. Eršov [2] has shown that the elementary theory of relatively complemented distributive lattices is decidable.

The main tool which we shall use to establish these results is the von Neumann coordinatization theorem, which we shall describe briefly in the next section.

For the definitions of terms used but not defined in this paper the reader is referred to any standard texts, such as [5] and [8].

1.1. **Definitions.** (i) Let $A$ be a finitely generated algebraic structure, with generators $x_1, \cdots, x_n$. The word problem for $A$ is the decision problem for formulas of the form $w_1 = w_2$ in $A$, where $w_1, w_2$ vary over words in $x_1, \cdots, x_n$.

(ii) Let $T$ be an algebraic theory. We shall say that the restricted word problem for $T$ is undecidable if there are words $r_i, s_i, i = 1, \cdots, k$. in the variables $x_1, \cdots, x_n$ such that the decision problem for formulas of the form

$$r_1 = s_1 \wedge \cdots \wedge r_k = s_k \rightarrow r = s$$

is undecidable in $T$, where $r$ and $s$ vary over words in $x_1, \cdots, x_n$.

(iii) If $\mathfrak{M}$ is a class of algebraic structures then by the restricted word problem for $\mathfrak{M}$ we mean the restricted word problem for $\mathrm{Th}(\mathfrak{M})$, the theory of $\mathfrak{M}$.

Notice that if the class of models of $T$ is closed under substructures and the formation of products then the undecidability of the restricted word problem for $T$ implies that there is a finitely presented model of $T$ with undecidable word problem.

2. In this section we describe the von Neumann coordinatization theorem. A good reference for the proof of this theorem is [10, pp. 93–209]. We shall use $\cup$ and $\cap$ to denote the lattice operations of join and meet.

2.1. **Definitions.** (a) A lattice $L$ is (i) modular if it satisfies the partial distributive law

$$c \cap (a \cup b) = a \cup (c \cap b) \quad \text{whenever } a \subset c,$$

and (ii) complemented if it contains a least element $0$, a greatest element $1$ and for all $x$ there exists a $y$ such that $x \cap y = 0$ and $x \cup y = 1$.

(b) If $L$ is a lattice and $a, b \in L$ $(a \subset b)$ then $L(a, b)$ denotes the sublattice of all $x \in L$ with $a \subset x \subset b$. Notice that $L(a, b)$ has least element $a$ and greatest element $b$.

(c) A set of nonzero elements $\{a_i : i = 1, \cdots, n\} \subset L$ is independent if, for any subset $I \subset \{1, \cdots, n\}$, $\bigcup_{i \in I} a_i \cap \bigcup_{i \notin I} a_i = 0$.

(d) A normalized frame of order $n$ in a complemented modular lattice $L$ is a set $a_i$, $i = 1, \cdots, n$; $c_{ij}$, $i, j = 1, \cdots, n$, $i \neq j$ such that:
  (i) the $a_i$ are independent and $\bigcup_{i=1}^{n} a_i = 1$;
  (ii) $c_{ij} = c_{ji}$;
  (iii) $a_i \cup a_j = a_i \cup c_{ij} = a_j \cup c_{ji}$ $\forall i, j$, $i \neq j$;
  (iv) $(c_{ij} \cup c_{jk}) \cap (a_i \cup a_k) = c_{ik}$ for any distinct triple $i, j, k$.

If $L$ has a normalized frame of order $n$, $L$ is said to have homogeneous order $n$. If $L$ has a normalized frame $a_i$, $c_{ij}$ we define $L_{ij} = \{x \in L: x \cap a_j = 0$ and $x \cup a_j = a_i \cup a_j\}$.

(e) If $b \in L_{ij}$, $d \in L_{jk}$ we define $b \otimes d = (b \cup d) \cap (a_i \cup a_k)$.

(f) If $L$ has a normalized frame $a_i$, $c_{ij}$ then an $L$-number $B = (b_{ij})$ is an array $b_{ij}$, $i, j = 1, \cdots, n$, $i \neq j$ such that:
  (i) $b_{ij} \in L_{ij}$;
  (ii) $b_{hk} = b_{ij} P\binom{i\ \ j}{h\ \ k}$ for any 2 distinct pairs $i, j$ and $h, k$, where $P\binom{i\ \ j}{h\ \ k}$ is a projective isomorphism of $(a_i \cup a_j) \rightarrow (a_h \cup a_k)$ defined via the axes of

perspectivity $c_{ih}$ and $c_{jk}$. For the definition and properties of the $P(\begin{smallmatrix} i & j \\ b & k \end{smallmatrix})$ see [10, pp. 117–129]. Since we shall give a different definition of $L$-numbers we shall not describe the $P(\begin{smallmatrix} i & j \\ b & k \end{smallmatrix})$.

(g) Multiplication of $L$-numbers $B = (b_{ij})$ and $D = (d_{ij})$ is defined as follows. $BD = (f_{ij})$ where $f_{ij} = b_{ik} \otimes d_{kj}$. This definition is independent of $k \neq i$, $j$, and $BD$ is an $L$-number. We shall verify this later after we have given an alternative definition of $L$-numbers (see Lemma 2.6). Addition of $L$-numbers $B = (b_{ij})$ and $D = (d_{ij})$ is defined by $B + D = (g_{ij})$ where

$$g_{ij} = [\{(b_{ij} \cup c_{ik}) \cap (a_j \cup a_k)\} \cup \{(d_{ij} \cup a_k) \cap (a_j \cup c_{ik})\}] \cap (a_i \cup a_j).$$

This also is independent of $k$ and is an $L$-number; see [10, pp. 136–147]. We shall not use this definition in the following.

(h) A ring $R$ is called regular (in the sense of von Neumann) if it satisfies the condition $\forall x \exists y (xyx = x)$.

(i) If $S$ is a ring then $M_n(S)$ is the ring of $n \times n$ matrices over $S$.

Let $L$ be a complemented modular lattice of homogeneous order $n \geq 4$ with a normalized frame $a_i$, $c_{ij}$. Let $S$ be the set of $L$-numbers with respect to this frame, with addition and multiplication defined as above, and with $0$ the $L$-number $(0_{ij}) = (a_i)$ and $1$ the $L$-number $1_{ij} = c_{ij}$. Then

**2.2. Theorem** (von Neumann [10, p. 157]). *The set $S$ with $+$, $\times$, $0$, $1$ defined as above is a regular ring. $M_n(S)$ is also a regular ring.*

**2.3. Theorem** (von Neumann [10, pp. 104, 108, 208]). *$L$ is isomorphic with the lattice of principal right ideals of $M_n(S)$, and this correspondence between the lattice $L$ and the ring $M_n(S)$ is unique.*

Notice that the statement "$a_i$, $c_{ij}$ is a normalized frame" is an open lattice relation among the $a_i$, $c_{ij}$ ($0 = \bigcap_{i=1}^n a_i$ and $1 = \bigcup_{i=1}^n a_i$). If $B$, $D$, $E$ are $L$-numbers then the statement $B \cdot D = E$ is an open lattice relation among the $b_{ij}$, $d_{ij}$, $e_{ij}$ and the $a_i$ and $c_{ij}$. Our first aim is to give a different definition of $L$-numbers from (f) above, so that the statement that $B = (b_{ij})$ is an $L$-number is an open relation among the $b_{ij}$, $a_i$ and $c_{ij}$.

**2.4. Lemma.** *Let $b_{ij} \in L_{ij}$ for $i$, $j = 1, \cdots, n$, $i \neq j$. Then $B = (b_{ij})$ is an $L$-number if and only if $B \cdot 1 = B = 1 \cdot B$; i.e.*

(1)
$$b_{ij} = b_{ik} \otimes c_{kj} \quad and \quad b_{ij} = c_{ik} \otimes b_{kj}$$

*for all distinct triples $i$, $j$, $k$.*

**Proof.** If $B$ is an $L$-number then, by Theorem 2.2, $B \cdot 1 = 1 \cdot B = B$. Conversely suppose that $B \cdot 1 = 1 \cdot B = B$. Then

$$b_{ik} = (b_{ij} \cup c_{jk}) \cap (a_i \cup a_k) = b_{ij} P \begin{pmatrix} i & j \\ i & k \end{pmatrix}$$

by the definition of $P(\begin{smallmatrix} i & j \\ i & k \end{smallmatrix})$. (See [10, p. 117].) Similarly,

$$b_{hj} = b_{ij} P \begin{pmatrix} i & j \\ h & j \end{pmatrix}.$$

If follows now that $b_{hk} = b_{ij} P(\begin{smallmatrix} i & j \\ h & k \end{smallmatrix})$ since $P(\begin{smallmatrix} i & j \\ h & k \end{smallmatrix}) = P(\begin{smallmatrix} i & j \\ i & u \end{smallmatrix}) P(\begin{smallmatrix} i & k \\ h & k \end{smallmatrix})$. (See [10, p. 117].) Hence $B$ is an $L$-number.

We can now make the new

2.5. **Definition.** Let $L$ have normalized frame $a_i, c_{ij}$; then $B = (b_{ij})$ is an $L$-number if (i) $b_{ij} \in L_{ij}$, and (ii) formulas (1) above hold for all distinct triples $i, j, k$.

Notice that the statement that $B$ is an $L$-number is an open relation among the $a_i, c_{ij}$ and the $b_{ij}$.

In order that our results should extend to (not necessarily complemented) modular lattices we need the following:

2.6. **Lemma.** *Let $L$ be a modular lattice with least element $0$, greatest element $1$ and normalized frame $a_i, c_{ij}$.*

(a) (i) *If $b_{ij} \in L_{ij}, d_{jk} \in L_{jk}$ ($i, j, k$ distinct) then $b_{ij} \otimes d_{jk} \in L_{ik}$.* (ii) $\otimes$ *is associative.*

(b) *If $B = (b_{ij})$, $D = (d_{ij})$ are $L$-numbers according to Definition 2.5 and if $i, j, h, k$ are distinct then $b_{ik} \otimes d_{kj} = b_{ih} \otimes d_{hj}$, i.e. multiplication of $L$-numbers is well defined in any modular lattice with a normalized frame.*

(c) *If $B, D, E$ are $L$-numbers then $B \cdot D = E$ holds if and only if $b_{ij} \otimes d_{jk} = e_{ik}$ holds for some distinct triple $i, j, k$.*

**Proof.** (a) (i) We must show that $(b_{ij} \otimes d_{jk}) \cap a_k = 0$ and that $(b_{ij} \otimes d_{jk}) \cup a_k = a_i \cup a_k$.

$$(b_{ij} \otimes d_{jk}) \cap a_k = (b_{ij} \cup d_{jk}) \cap (a_i \cup a_k) \cap a_k$$

$$= (b_{ij} \cup d_{jk}) \cap a_k \subset a_k$$

$$\subset (b_{ij} \cup d_{jk}) \cap (a_j \cup a_k)$$

$$= [b_{ij} \cap (a_j \cup a_k)] \cup d_{jk} \quad \text{since } d_{jk} \subset a_j \cup a_k.$$

Since $d_{jk} \cap a_k = 0$ it is sufficient to show that $b_{ij} \cap (a_j \cup a_k) = 0$.

$$b_{ij} \cap (a_j \cup a_k) \subset (b_{ij} \cup a_j) \cap (a_j \cup a_k)$$

$$= (a_i \cup a_j) \cap (a_j \cup a_k) = a_j.$$

Since $a_j \cap b_{ij} = 0$, we have $b_{ij} \cap (a_j \cup a_k) = 0$. Next consider

$$(b_{ij} \otimes d_{jk}) \cup a_k = [(b_{ij} \cup d_{jk}) \cap (a_i \cup a_k)] \cup a_k$$

$$= (b_{ij} \cup d_{jk} \cup a_k) \cap (a_i \cup a_k)$$

$$= (b_{ij} \cup a_j \cup a_k) \cap (a_i \cup a_k)$$

$$= (a_i \cup a_j \cup a_k) \cap (a_i \cup a_k)$$

$$= (a_i \cup a_k).$$

This completes the proof of (i).

(ii) We must show that if $b_{ij} \in L_{ij}$, $d_{jk} \in L_{jk}$ and $e_{kl} \in L_{kl}$ then $(b_{ij} \otimes d_{jk})$ $\otimes e_{kl} = b_{ij} \otimes (d_{jk} \otimes e_{kl})$.

$$(b_{ij} \otimes d_{jk}) \otimes e_{kl} = \{[(b_{ij} \cup d_{jk}) \cap (a_i \cup a_k)] \cup e_{kl}\} \cap (a_i \cup a_l)$$

$$= \{[(b_{ij} \cup d_{jk}) \cap (a_i \cup a_k \cup a_l)] \cup e_{kl}\} \cap (a_i \cup a_l)$$

$$= (b_{ij} \cup d_{jk} \cup e_{kl}) \cap (a_i \cup a_k \cup a_l) \cap (a_i \cup a_l)$$

$$= (b_{ij} \cup d_{jk} \cup e_{kl}) \cap (a_i \cup a_l).$$

By symmetry we also have $b_{ij} \otimes (d_{jk} \otimes e_{kl}) = (b_{ij} \cup d_{jk} \cup e_{kl}) \cap (a_i \cup a_l)$ and this completes the proof of (ii).

(b)
$$b_{ik} \otimes d_{kj} = (b_{ij} \otimes c_{jk}) \otimes (c_{kb} \otimes d_{bj})$$

$$= [b_{ij} \otimes (c_{jk} \otimes c_{kb})] \otimes d_{bj}$$

$$= (b_{ij} \otimes c_{jb}) \otimes d_{bj}$$

$$= b_{ib} \otimes d_{bj}.$$

(c) Suppose that $b_{ij} \otimes d_{jk} = e_{ik}$. Then

$$b_{bj} \otimes d_{jk} = (1_{bi} \otimes b_{ij}) \otimes (d_{jk} \otimes 1_{kl})$$

$$= 1_{bi} \otimes (b_{ij} \otimes d_{jk}) \otimes 1_{kl}$$

$$= 1_{bi} \otimes c_{ik} \otimes 1_{kl} = e_{bl}.$$

We have already seen in (a) that this is independent of $j$.

**3. The undecidability results.** In order to apply the above to get the undecidability of the restricted word problem for modular lattices we need to know that any countable semigroup can be obtained as a subsemigroup of the multiplicative semigroup $S$, of $L$-numbers of a suitable modular lattice $L$ with fixed homogeneous order $n \geq 4$.

Let $V$ be an infinite dimensional vector space (over $Q$ say) with algebraic basis $\{e_i: i \in \mathbb{N}\} = E$. Let $L$ be the lattice of all subspaces of $V$. It is well known that $L$ is a complemented modular lattice. Let $R$ be the ring of all linear transformations of $V$. Then

**3.1. Lemma.** (i) *$R$ is a regular ring and any countable semigroup is a subsemigroup of $R$.* (ii) *There is a normalized frame of order 4 in $L$.* (iii) *If $S$ is the ring of $L$-numbers relative to this frame then the multiplicative semigroup of $R$ is a subsemigroup of $S$.*

**Proof.** (i) Let $M \in R$. Let $N \in R$ such that for all $x \in \text{Range}(M)$, $N(x) \in M^{-1}(x)$. It is clear that such $N$ exist. Then $MNM = M$, so $R$ is regular.

Let $C$ be a countable semigroup. Without loss of generality we may assume $C$ has an identity, since if not $C$ can be extended to a semigroup with identity. Then the right regular representation faithfully represents $C$ as a semigroup of endomorphisms of the set $C$, by $C \ni x \rightarrow$ right multiplication by $x$. We can now take any 1-1 mapping of $C$ onto $E$, and represent $C$ in the ring of endomorphisms of $V$.

(ii) Let $A_\alpha$, $\alpha = 1, \cdots, 4$, be the subspace of $V$ generated by $E_\alpha = \{e_{\alpha+4i}: i \in \mathbb{N}\}$. Let $R_\alpha$ be the ring of endomorphisms of $A_\alpha$. Then since $V_\alpha \simeq V$, $R_\alpha \simeq R$. Also $V = \bigoplus_{\alpha=1}^4 A_\alpha$. Let $C_{\alpha\beta}$ $(\alpha \neq \beta)$ be the subspace of $V$ generated by $E_{\alpha\beta} = \{e_{\beta+4i} - e_{\alpha+4i}: i \in \mathbb{N}\}$. Then the $A_\alpha$, $C_{\alpha\beta}$ form a normalized frame of order 4 in $L$. This is obvious, except perhaps for the equation $C_{\alpha\beta} \otimes C_{\beta\gamma} = C_{\alpha\gamma}$, which is easily verified as follows, where $[F]$ denotes the subspace of $V$ generated by $F \subset V$.

$$C_{\alpha\beta} \otimes C_{\beta\gamma} = (C_{\alpha\beta} \cup C_{\beta\gamma}) \cap (A_\alpha \cup A_\gamma)$$

$$= [\{e_{\beta+4i} - e_{\alpha+4i}: i \in \mathbb{N}\} \cup \{e_{\gamma+4i} - e_{\beta+4i}: i \in \mathbb{N}\}] \cap (A_\alpha \cup A_\gamma)$$

$$= [\{e_{\gamma+4i} - e_{\alpha+4i}: i \in \mathbb{N}\} \cup \{e_{\alpha+4i} + e_{\gamma+4i} - 2e_{\beta+4i}: i \in \mathbb{N}\}] \cap (A_\alpha \cup A_\gamma)$$

$$= (C_{\gamma\alpha} \cup [\{e_{\alpha+4i} + e_{\gamma+4i} - 2e_{\beta+4i}\}]) \cap (A_\alpha \cup A_\gamma)$$

$$= C_{\gamma\alpha} = C_{\alpha\gamma}.$$

Let $\phi_{\alpha\beta}: A_\alpha \rightarrow A_\beta$ be defined by $\phi(e_{\alpha+4i}) = e_{\beta+4i}$. Let $r \in R_1$ and let $[r]$ be the subspace of $V$ generated by $E'_{12} = \{e_{1+4i} - \phi_{12} \circ r(e_{1+4i}): i \in \mathbb{N}\}$. Then

certainly $[r] \in L_{12}$. Extend $[r]$ to the $L$-number $(r)$ by defining $(r)_{ij} = C_{i1} \otimes [r]$ $\otimes C_{2j}$, etc. We claim that the mapping $r \rightarrow (r)$ is an embedding of the multiplicative semigroup of $R \simeq R_1$ into $S$. Clearly if $r \neq s$ then $[r] \neq [s]$ and so $(r) \neq (s)$. We must show that $(r)(s) = (rs)$. Notice that it is sufficient to show that $(r)_{12} \otimes (s)_{23} = (rs)_{13}$ in the light of part (c) of Lemma 2.6. First we show that for any $t \in R_1$

(2) $(t)_{\alpha\beta} = [\{e_{\alpha+4i} - \phi_{1\beta} \circ t(e_{1+4i}) : i \in \mathbf{N}\}].$

$$(t)_{\alpha\beta} = C_{\alpha1} \otimes [t] \otimes C_{2\beta}$$

$$= [\{e_{1+4i} - e_{\alpha+4i}, e_{1+4i} - \phi_{12} \circ t(e_{1+4i}), e_{\beta+4i} - e_{2+4i} : i \in \mathbf{N}\}] \cap (A_\alpha \cup A_\beta)$$

(as in the proof of (a)(ii) of Lemma 2.6)

$$\supseteq [\{e_{\alpha+4i} - \phi_{12} \circ t(e_{1+4i}), e_{\beta+4i} - e_{2+4i} : i \in \mathbf{N}\}] \cap (A_\alpha \cup A_\beta)$$

$$\supseteq [\{e_{\alpha+4i} - \phi_{12} \circ t(e_{1+4i}),$$

$$\phi_{1\beta} \circ t \circ \phi_{\beta1}(e_{\beta+4i}) - \phi_{1\alpha} \circ t \circ \phi_{21}(e_{2+4i}) : i \in \mathbf{N}\}] \cap (A_\alpha \cup A_\beta)$$

$$= [\{e_{\alpha+4i} - \phi_{12} \circ t(e_{1+4i}),$$

$$\phi_{1\beta} \circ t(e_{1+4i}) - \phi_{12} \circ t(e_{1+4i}) : i \in \mathbf{N}\}] \cap (A_\alpha \cup A_\beta)$$

$$\supseteq [\{e_{\alpha+4i} - \phi_{1\beta} \circ t(e_{1+4i}) : i \in \mathbf{N}\}] \in L_{\alpha\beta}.$$

(2) now follows from the easy observation that if $b, b' \in L_{ij}$ and $b \subset b'$ then $b = b'$. So

$$(r)_{12} \otimes (s)_{23} = [\{e_{1+4i} - \phi_{12} \circ r(e_{1+4i}), e_{2+4i} - \phi_{13} \circ s(e_{1+4i}) : i \in \mathbf{N}\}] \cap (A_1 \cup A_3)$$

$$\supseteq [\{e_{1+4i} - \phi_{12} \circ r(e_{1+4i}),$$

$$\phi_{12} \circ r \circ \phi_{21}(e_{2+4i}) - \phi_{13} \circ r \circ \phi_{31} \circ \phi_{13} \circ s(e_{1+4i}) : i \in \mathbf{N}\}] \cap (A_1 \cup A_3)$$

$$= [\{e_{1+4i} - \phi_{12} \circ r(e_{1+4i}), \phi_{12} \circ r(e_{1+4i}) - \phi_{13} \circ (rs)(e_{1+4i}) : i \in \mathbf{N}\}] \cap (A_1 \cup A_3)$$

$$\supseteq [\{e_{1+4i} - \phi_{13} \circ (rs)(e_{1+4i}) : i \in \mathbf{N}\}]$$

$$= (rs)_{13}.$$

Hence $(r)_{12} \otimes (s)_{23} = (rs)_{13}$ by the above observation and this completes the proof.

Now let $S'$ be a finitely presented semigroup with unsolvable word problem (see Davis [1]). Let $S'$ have generators $x_1, \cdots, x_n$ and relations $r_\nu = s_\nu$, $\nu = 1, \cdots, k$. Let $\psi$ be the conjunction of the following open formulas in the language of lattices

(i) $a_i$, $c_{ij}$, $i$, $j = 1, \cdots, 4$, $i \neq j$, form a normalized frame in $L(\bigcap_{i=1}^4 a_i, \bigcup_{i=1}^4 a_i)$ $= L'$,

(ii) $x_\alpha^{ij}$, $i$, $j = 1, \cdots, 4$, $i \neq j$, $\alpha = 1, \cdots, n$, are $L'$-numbers relative to this frame,

(iii) $r_\nu(x_\alpha^{ij}) = s_\nu(x_\alpha^{ij})$, $\nu = 1, \cdots, k$.

Notice that each equation in (iii) is actually a set of 12 equations, but in the light of Lemma 2.6(c), the truth of all of these equations follow from any one of them, so we may regard each of these equations to be just one equation. Similarly for any words $r$ and $s$ we shall let $r(x_\alpha^{ij}) = s(x_\alpha^{ij})$ denote any one of the possible (equivalent) equations.

If $\phi$ is the open formula $\bigwedge_{\nu=1}^k r_\nu = s_\nu \to r = s$ in the language of semigroups, let $\phi^*$ be the open formula $\psi \to r(x_\alpha^{ij}) = s(x_\alpha^{ij})$ in the language of lattices. It follows immediately from Lemma 3.1 that $\phi$ is true in the theory of semigroups if and only if $\phi^*$ is true in the theory of (complemented) modular lattices. Hence we have

**3.2. Theorem.** *The restricted word problem for the theory of (complemented) modular lattices is undecidable.*

**3.3. Corollary.** *There exists a finitely presented modular lattice with undecidable word problem.*

**3.4. Remark.** It follows that the restricted word problem for modular lattices is different from the restricted word problem for finite modular lattices and hence that there is a finitely presented modular lattice which is not residually finite.

Next we shall prove that the restricted word problems for finite-dimensional projective geometries and for finite modular lattices are undecidable. To do this we shall use the result of Gurevič [3] that the restricted word problem for finite semigroups is undecidable, instead of the Post result on the word problem for semigroups.

A projective geometry is an irreducible, complemented modular lattice. The dimension of a projective geometry is the cardinality of a maximal set of independent (nonzero) elements. (Often the dimension is taken to be 1 less than this number.) It is well known that corresponding to any $n$-dimensional projective geometry $P$, with $n > 3$, is a division ring $\mathfrak{D}$ such that $P$ is isomorphic with the lattice of subspaces of $V_n(\mathfrak{D})$—the $n$-dimensional right vector space over $\mathfrak{D}$. For a modern treatment of this and other elementary results about projective geometries see Hartshorne [4]. We shall denote this geometry by $P_n(\mathfrak{D})$. It is also well known that $P_n(\mathfrak{D})$ is isomorphic with the lattice of (principal) right ideals of the regular ring $M_n(\mathfrak{D})$. (See [10, p. 90].)

The proof of Lemma 3.1 shows that $P_{4n}(\mathfrak{D})$ has homogeneous order 4. Consequently if we fix a normalized frame of order 4 in $P_{4n}(\mathfrak{D})$, and if $S$ is the corresponding ring of $P_{4n}(\mathfrak{D})$-numbers then $M_4(S) \simeq M_{4n}(\mathfrak{D})$. From this it follows that $S \simeq M_n(\mathfrak{D})$.

We also remark that if $H$ is a semigroup of cardinality $n$ then the right regular representation, as in the proof of Lemma 3.1, shows that $H$ is a subsemigroup of the multiplicative semigroup of $M_{n+1}(F)$, for any field $F$.

Let $T$ be the open theory of finite semigroups and let $T_F$ denote the open theory of the multiplicative semigroups $M_n(F)$, $n \in \mathbf{N}$.

**3.5. Lemma.** *For any field* $F$, $T \equiv T_F$.

**Proof.** We have just remarked that $T \subseteq T_F$. Now if $F$ is finite then certainly $T_F \subseteq T$, and thus $T \equiv T_F$. Let $F_p$ denote the prime field of characteristic $p$, and let $\overline{F}_p$ denote the algebraic closure of $F_p$. Then $\overline{F}_p$ is the union of finite fields so each $M_n(\overline{F}_p)$ is the union of finite semigroups. Hence if an open formula $\phi$ is refutable in $M_n(\overline{F}_p)$ then it is refutable in $M_n(F)$ for some finite $F$. Hence $T \equiv T_{\overline{F}_p}$. From the completeness of the theory of algebraically closed fields of characteristic $p$ we have that if $F$ is an algebraically closed field of characteristic $p$ then $M_n(F) \equiv M_n(\overline{F}_p)$. The lemma then follows for fields of characteristic $p$ from the observations that if $F_1 \subset F_2$ then $T_{F_2} \subset T_{F_1}$ and that any field is contained in an algebraically closed field. To extend this proof to fields of characteristic zero we need only observe that if $\phi$ is refutable in $M_n(\overline{\mathbf{Q}})$ then by the compactness theorem $\phi$ is refutable in $M_n(\overline{F}_p)$ for large enough $p$.

We can repeat the above construction of $\phi^*$ using the result of Gurevič instead of Post. Observe that $\phi^*$ is true in $P_n(F)$ if and only if $\phi$ is true in $M_k(F)$ for all $k \leq [n/4]$, and hence that $\phi^*$ is true in the class of finite-dimensional projective geometries over $F$ if and only if $\phi$ is true in the class of finite semigroups. Hence we have

**3.6. Theorem.** *The restricted word problem for finite-dimensional projective geometries over any class of fields is undecidable.*

**3.7. Corollary.** *The restricted word problem for finite projective geometries is undecidable.*

**3.8. Remarks.** Notice that if $T$ is a decidable theory of fields then the theory of the rings $\{M_n(F): F \vDash T\}$ for fixed $n$ is decidable and hence the theory of the geometries $\{P_n(F): F \vDash T\}$ is decidable. It follows easily from the methods of Scott [7] that for a decidable theory of fields, $T$, the theory of the

geometries $\{P_n(F): n \in N, F \vDash T\}$ with variables constrained to vary over sub-objects of dimension $< N$ for fixed $N$, is decidable.

**3.9. Theorem.** *The restricted word problem for finite (complemented) modular lattices is undecidable.*

**Proof.** We know that relative to a normalized frame in any modular lattice $L$, $L$-number multiplication is a well-defined semigroup operation. If $L$ is finite this semigroup is certainly finite and, conversely, we have seen that any finite semigroup is a subsemigroup of $M_n(F_2)$ for large enough $n$ and that $P_n(F_2)$ is certainly a finite modular lattice.

**3.10. Corollary.** *The theory of finite commutative idempotent semigroups is undecidable.*

**Proof.** Any finite lattice becomes such a semigroup under the operation $a \cdot b = a \cap b$. The lattice structure can be recovered from the semigroup structure since $a \subset b$ if and only if $a \cdot b = (a \cap b) = a$.

**Added in proof.** It has been brought to my attention (July 1973) that a proof of the undecidability of the word problem for modular lattices has also been given by George Hutchinson, *Recursively unsolvable word problems of modular lattices and diagram-chasing*, J. Algebra (to appear).

## REFERENCES

1. M. Davis, *Computability and unsolvability*, McGraw-Hill Series in Information Processing and Computers, McGraw-Hill, New York, 1958. MR 23 #A1525.

2. Ju. L. Eršov, *Decidability of the elementary theory of relatively complemented lattices and of the theory of filters*, Algebra i Logika Sem. 3 (1964), no. 3, 17–38. (Russian) MR 31 #4725.

3. Ju. S. Gurevič, *The problem of equality of words for certain classes of semigroups*, Algebra i Logika Sem. 5 (1966), no. 5, 25–35. (Russian) MR 34 #5904.

4. R. Hartshorne, *Foundations of projective geometry*, Lecture Notes, Harvard University, 1966/67, Benjamin, New York, 1967. MR 36 #5801.

5. J. Lambek, *Lectures on rings and modules*, Blaisdell, Waltham, Mass., 1966. MR 34 #5857.

6. J. C. C. McKinsey, *The decision problem for some classes of sentences without quantifiers*, J. Symbolic Logic 8 (1943), 61–76. MR 5, 85.

7. D. Scott, *Convergent sequences of complete theories*, Ph.D. Thesis, Princeton University, Princeton, N. J., 1958.

8. J. R. Shoenfield, *Mathematical logic*, Addison-Wesley, Reading, Mass., 1967. MR 37 #1224.

9. P. M. Whitman, *Free lattices*, Ann. of Math. (2) 42 (1941), 325–330. MR 2, 244.

10. J. von Neumann, *Continuous geometry. Foreword by Israel Halperin*, Princeton Math. Series, no. 25, Princeton Univ. Press, Princeton, N. J., 1960. MR 22 #10931.

DIVISION OF MATHEMATICAL SCIENCES, PURDUE UNIVERSITY, WEST LAFAYETTE, INDIANA 47907