ON THE DECISION PROBLEM FOR THEORIES OF FINITE MODELS

BY
VERENA HUBER DYSON

ABSTRACT

An infinite extension of the elementary theory of Abelian groups is constructed, which is proved to be decidable, while the elementary theory of its finite models is shown to be undecidable. Tarski's proof of undecidability for the elementary theory of Abelian cancellation semigroups is presented in detail. Szmielew's proof of the decidability of the elementary theory of Abelian groups is used to prove the decidability of the elementary theory of finite Abelian groups, and an axiom system for this theory is exhibited. It follows that the elementary theory of Abelian cancellation semigroups, while undecidable, has a decidable theory of finite models.

In this note we shall frequently refer to concepts and results of [12]. Given a theory T with standard formalization, we denote by T_f the elementary theory of all finite models of T. Thus T_f is an extension of T with the same non-logical constants.

In all commonly known cases of theories T with arbitrarily large finite models, T and T_f are either both decidable or both undecidable. If, for instance, we take for T the elementary theory of relational structures with one discrete simple ordering relation, or with one equivalence relation, or of Boolean algebras, or of Abelian groups, then T is known to be decidable (see [6], [5], [11], and [8]), and it is not difficult to prove that T_f is decidable as well. However, we do not see in any of these cases an automatic method for deriving the decidability of T_f from that of T. In the case of Abelian groups the derivation will be given in the proof of Theorem 4 below. If, on the other hand, we take for T the first-order logic with a given set of non-logical constants (including at least one non-unary predicate), i.e., the elementary theory of all relational structures of a given similarity type, or the elementary theory of groups, or of rings, or of distributive lattices, then both T and T_f have been shown to be undecidable (cf. [12], where further references can be found, and [14], [1], [7] and [10]).

The question naturally arises whether the property of being decidable, or undecidable, always carries over from a theory T (with arbitrarily large finite

Received August 10, 1963.

models) to its extension T_f. The purpose of this note is to show that the answer is negative.(1)

In symbolic notation and terminology we shall, in general, adhere to [12]. We shall use, however, $\forall$ and $\exists$ as the universal and existential quantifiers. $\exists^n x\Phi$ will serve as the abbreviation of the formula expressing the fact that there are exactly n elements x satisfying the formula Φ. $\bigwedge_{i<n}\Phi_i$ and $\bigvee_{i<n}\Phi_i$ will respectively denote the conjunction and the disjunction of the n formulas $\Phi_0,\ldots,\Phi_{n-1}$. We shall also use expressions like $\bigwedge_{i\in I}\Phi_i$ to represent the conjunction of all formulas Φ_i indexed by the elements i of a finite set I (without indicating the order in which the formulas Φ_i occur in this conjunction, since the order is irrelevant for our purposes). Given a set X of sentences, we shall denote by $|X|$ the set of all disjunctions each term of which is either a sentence of X or the negation of such a sentence; by $[X]$ we shall denote the set of all conjunctions of members of $|X|$. N will stand for the set of natural numbers, p_n for the nth prime in natural order, and (m,n), as usual, for the greatest common divisor of m and n. By ${}^m n$ we shall denote the set of all m-termed sequences $r=\langle r_0,\ldots,r_{m-1}\rangle$ all terms of which are natural numbers $<n$, subject to the condition that at least one term differs from 0.

By the phrase "the sentence Φ is derivable in the theory T from the set S of sentences" we mean that Φ is logically derivable from the set consisting of all valid sentences of T and all sentences of S. Similar remarks apply to expressions such as "Φ is compatible (or incompatible) with S in T," "Φ and Ψ are compatible (or incompatible) in T," or, "Φ and Ψ are equivalent in T."

We shall be discussing certain theories closely related to the elementary theory AG of Abelian groups and therefore present first a brief account of a few pertinent results concerning this theory.

Theory AG has been thoroughly discussed by Szmielew in [8]. Since we shall frequently refer to [8], it should be pointed out that our symbolism deviates in some respects from that of [8]. In particular we use the multiplicative notation instead of the additive one. Thus we assume AG to be provided with the binary operation symbol $\cdot$ and the individual constant $\mathbf{1}$ as the only non-logical constants(2). For any term τ in the symbolism of AG and any $n\in N$ the symbolic expression τ^n will have its usual meaning.

One of the main results of [8] (cf. p. 269f.) is a proof of the decidability of AG. The method of proof can roughly be described as follows. A certain recursive

(1) This paper was prepared for publication while the author was working at the University of California on a research project in the foundations of mathematics sponsored by the U.S. National Science Foundation, Grant G19673. The main results were first stated (without proof) in [3]. For some related results see [4].

(2) Regarding the difference in use between symbols printed in bold and in ordinary type (e.g., between $\cdot$ and $\cdot$, or $=$ and $=$) see [12], p. 42.

set B of so-called *basic sentences* is singled out, it is proved that every sentence in the formalism of AG is equivalent to a sentence of $[B]$([3]); and finally a decision procedure for $[B]$ is established, i.e., it is shown that the set of all sentences of $[B]$ which are provable in AG is recursive. (What is actually discussed in [8] is not a set B of basic sentences, but the corresponding model-theoretic notion, the set C of basic arithmetical classes. While according to our conventions $|B|$ denotes the set of finite disjunctions of basic sentences and their negations, $|C|$ is the set of all finite unions of finite intersections—or, equivalently, of all finite intersections of finite unions—of basic arithmetical classes and their complements. Thus $|C|$ is the model theoretic object which exactly corresponds to our set $[B]$.)

In [8] the following sentences $K(m)$ and $R^{(i)}(q,k,m)$, where m and k are arbitrary positive integers, q is an arbitrary prime, and $i = 1,2,3$, are chosen as basic sentences:

$$K(m) = \forall x(x^m = \mathbf{1}),$$

$$R^{(1)}(q,k,m) = \exists x_0 \ldots \exists x_{m-1}[\bigwedge_{r \in m_q} \sim (x_0^{q^{k-1}r_0} \cdot \ldots \cdot x_{m-1}^{q^{k-1}r_{m-1}} = \mathbf{1}) \wedge \bigwedge_{i<m}(x_i^{q^k} = \mathbf{1})],$$

$$R^{(2)}(q,k,m) = \exists x_0 \ldots \exists x_{m-1}[\bigwedge_{r \in m_q} \forall x_m \sim (x_0^{q^{k-1}r_0} \cdot \ldots \cdot x_{m-1}^{q^{k-1}r_{m-1}} = x_m^{q^k})],$$

$$R^{(3)}(q,k,m) = \exists x_0 \ldots \exists x_{m-1}[\bigwedge_{r \in m_q} \forall x_m \sim (x_0^{q^{k-1}r_0} \cdot \ldots \cdot x_{m-1}^{q^{k-1}r_{m-1}} = x_m^{q^k}) \wedge \bigwedge_{i<m}(x_i^{q^k} = \mathbf{1})].$$

We find it more convenient for our purposes to use as basic sentences, instead of $K(m)$ and $R^{(i)}(q,k,m)$, the following closely related sentences $H(m)$ and $Q^{(i)}(q,k,n)$, where m, i, q, and k are as before and n is an arbitrary natural number,

$$H(1) = K(A1),$$

$$H(m+1) = [K(m+1) \wedge \bigwedge_{j<0\leqq m} \sim K(j)],$$

$$Q^{(i)}(q,k,0) = \sim R^{(i)}(q,k,1),$$

$$Q^{(i)}(q,k,m) = [\sim R^{(i)}(q,k,m+1) \wedge R^{(i)}(q,k,m)].$$

([3]) It is a widespread belief that, to justify the argument just described, it is necessary to know that every sentence in the formalism of the theory **AG** is *effectively* equivalent, and not just equivalent, to a sentence of $[B]$. It was pointed out by Tarski, however, that this is superfluous. In fact he formulated the following general theorem: *Assume that* (i) **T** *is an axiomatizable theory and S is the set of all sentences in the formalism of* **T**, (ii) *S′ is a recursively enumerable subset of S, and* (iii) *the set of all those sentences of S″ that are valid in* **T** *is recursive. If, under these assumptions, every sentence of S is equivalent in* **T** *to a sentence of S″, then* **T** *is decidable, i.e., the set of all sentences of S that are valid in* **T** *is recursive.* This generalises the well known theorem by which every complete axiomatizable theory is decidable (see [12] p. 14) and implies, e.g., that every axiomatizable theory which has only finitely many complete extensions is also decidable.

In connection with this theorem of Tarski we remark that it is an immediate consequence of the following principle: *If, under the assumptions* (i) *and* (ii), *every sentence of S is equivalent in* **T** *to some sentence of S′, then this equivalence relation is effective in the sense that there is a recursive function which correlates with every sentence of S an equivalent sentences of S″.* The proofs of both these observations are obvious.

Henceforth we shall denote by B the set of all sentences $H(m)$ and $Q^{(i)}(q,k,n)$. Since every basic sentence of [8] is logically equivalent to a sentence of $[B]$ we have as in [8], p. 270,

(*) *Every sentence in the formalism of AG is equivalent in AG to a sentence of* $[B]$.

This result will play a basic role in the proofs of Theorems 1 and 4.

The decision procedure for the set $[B]$ has not been presented in [8] with any details. We shall now give the details that are needed for our further discussion.

Obviously a conjunction of sentences is provable if and only if every one of its conjuncts is provable. Hence the decision problem for the whole set $[B]$ reduces to that for $|B|$. Thus we have to present a method that permits us to show for each particular sentence Φ of $|B|$, either that Φ is provable in AG or else that $\sim\Phi$ has an Abelian group as a model. It turns out that such models can always be found among finite direct products of the following *basic Ableian groups*:

$\mathfrak{R}_q$, *the additive group of all rationals of the form* n/m *with* $(m,q)=1$,
$\mathfrak{C}_q$, *the group of all rationals of the form* n/q^k *with addition modulo* 1 *as the group operation*,
$\mathfrak{C}_{q^h}$, *the group of all rationals of the form* n/q^h *with addition modulo* 1 *as the group operation*,
$\mathfrak{Z}$, *the trivial group*,

where q is an arbitrary prime and h an arbitrary positive integer. We shall call $\mathfrak{M}$ a *q-model of a sentence* Φ if and only if $\mathfrak{M}$ is a model of Φ and is either a direct product of finitely many groups $\mathfrak{R}_q$, $\mathfrak{C}_{q^h}$, or a direct product of finitely many groups $\mathfrak{C}_q$, $\mathfrak{C}_{q^h}$, i.e., if $\mathfrak{M}$ is a q-model, then $\mathfrak{M}=\mathfrak{M}(\alpha,n,r)$ for $\alpha=0$ or 1, some $n\in N$ and some $l(r)$-termed finite sequence r of natural numbers, where

$$\mathfrak{M}(\alpha,n,r) = \mathfrak{R}_q^{zn} \times \mathfrak{C}_q^{(1-\alpha)n} \times \prod_{0<h<l(r)} \mathfrak{C}_{q^h}^{r_h}.$$

We shall, for any group $\mathfrak{A}$, identify $\mathfrak{A}^0$ with $\mathfrak{Z}$. The set of all basic sentences $Q^{(i)}(q,k,n)$ with fixed q will be denoted by Q_q. Unless stated otherwise, q will range over primes, i over 1,2,3, n over N, and k,h,m over positive integers. We now present some lemmas, which are needed for the proofs of Theorems 1 and 4 and which yield a decision procedure for $|B|$.

LEMMA 1. *For any* i, q, k, n, n', m *and* m' *for which* $n'\neq n$, $m'\neq m$ *and* $(m,q)=1$, *the following are theorems of* AG:

(i) $Q^{(i)}(q,k,n) \rightarrow \sim Q^{(i)}(q,k,n')$,

(ii) $H(m) \rightarrow \sim H(m')$,

(iii) $Q^{(1)}(q,k,n) \leftrightarrow \bigvee_{j \leqq n}(Q^{(1)}(q,k+1,j) \wedge Q^{(3)}(q,k,n-j))$,

(iv) $Q^{(2)}(q,k,n) \leftrightarrow \bigvee_{j \leqq n}(Q^{(2)}(q,k+1,j) \wedge Q^{(3)}(q,k,n-i))$,

(v) $H(m) \rightarrow Q^{(i)}(q,1,0)$,

(vi) $H(q^k m) \rightarrow Q^{(1)}(q,k+1,0) \wedge Q^{(2)}(q,k+1,0) \wedge \sim Q^{(3)}(q,k,0)$.

This lemma is easily verified on the basis of well known properties of Abelian groups. Parts (iii) and (iv) are consequences of Theorem 1.7, p. 216, of [8], where the expression $\rho^{(i)}(q,k)\mathfrak{A} = n$ is to be interpreted as "$\mathfrak{A}$ is a model of $Q^{(i)}(q,k,n)$." Parts (i) and (ii), by the way, motivate our choice of basic sentences. The next lemma is an immediate consequence of our definitions and can be found in [8] as Theorem 1.9, p. 219. Because of Lemma 1 (i) and (ii), it lists all the basic sentences of which any given basic group is a model.

LEMMA 2. *For any two distinct primes q and q' the following table indicates for what values of i, k and m the basic groups listed in the first row are models of the basis sentences listed in the first column.*

	$\mathfrak{R}_q$	$\mathfrak{C}_q$	$\mathfrak{C}_{qh}$	$\mathfrak{Z}$
$Q^{(1)}(q,k,0)$	any k	no k	$k > h$	any k
$Q^{(2)}(q,k,0)$	no k	any k	$k > h$	any k
$Q^{(3)}(q,k,0)$	any k	any k	$k \neq h$	any k
$Q^{(1)}(q,k,1)$	no k	any k	$k \leqq h$	no k
$Q^{(2)}(q,k,1)$	any k	no k	$k \leqq h$	no k
$Q^{(3)}(q,k,1)$	no k	no k	$k = h$	no k
$Q^{(i)}(q',k,0)$	$i = 1, 2, 3$ and any k			
$H(m)$	no m	no m	$m = q^h$	$m = 1$

Our next lemma establishes the direct product formation as a tool for obtaining models for further basic sentences. The first part of it can be found as Theorem 1.10, p. 219, in [8]; the rest is easily checked.

LEMMA 3. (i) *If $\mathfrak{A}$ and $\mathfrak{A}'$ are models of $Q^{(i)}(q,k,n)$ and of $Q^{(i)}(q,k,n')$ respectively, then $\mathfrak{A} \times \mathfrak{A}'$ is a model of $Q^{(i)}(q,k,n+n')$.*

(ii) *If* $\mathfrak{A}$ *is a* q*-model of* $Q^{(1)}(q,k+1,0) \wedge Q^{(2)}(q,k+1,0) \wedge \sim Q^{(3)}(q,k,0)$, *then* $\mathfrak{A}$ *is a model of* $H(q^k)$.

(iii) *If* $\mathfrak{A}$ *and* $\mathfrak{A}'$ *are models of* $H(m)$ *and* $H(m')$ *respectively, then* $\mathfrak{A} \times \mathfrak{A}'$ *is a model of* $H(mm'/(m,m'))$.

It hardly needs mentioning that, when we speak of models here, we always mean models that are Abelian groups. As a marginal case of (ii) the following should be noted:

(ii') *If* $\mathfrak{A}$ *is a* q*-model of* $Q^{(1)}(q,1,0) \wedge Q^{(2)}q,1,0)$, *then* $\mathfrak{A}$ *is a model of* $H(1)$, *i.e.*, $\mathfrak{A} = \mathfrak{Z}$.

The next three lemmas finally are crucial for the decidability of $[B]$. The gist of the whole situation can be summarized as follows: Given any sentence Φ of $[B]$, then, either Φ is logically derivable from the set of sentences listed in Lemma 1, or else a direct product of finitely many q-models, which is a model of $\sim \Phi$, can effectively be constructed on the basis of Lemmas 2 and 3.

LEMMA 4. *If* $\Phi \in |Q_q|$, *then either* Φ *is provable in* AG *or else* $\sim \Phi$ *has a* q*-model.*

It is not difficult to show, using Lemmas 2 and 3(i), that, unless Φ is a consequence (in the sense of propositional logic) of the sentences (i), (iii) and (iv) of Lemma 1, $\sim \Phi$ has a q-model, say $\mathfrak{M}(\alpha,n,r)$ (see also Theorem 1.12 of [8], p. 220). The decidability of $|Q_q|$ is an immediate consequence of this. For, again by Lemmas 1(i), 2 and 3(i), we see that $\mathfrak{M}(\alpha,n,r)$ is the unique q-model of the sentence

$$\Psi(\alpha,n,r) = Q^{(1)}(q,l(r),(1-\alpha)n) \wedge Q^{(2)}(q,l(r),\alpha n) \wedge \bigwedge_{0<h<l(r)} Q^{(3)}(q,h,r_h).$$

Hence by Lemma 4, for any sentence $\Phi \in |Q_q|$:

either Φ *is provable in* AG, *or else* α,n,r *can be found such that* $\Psi(\alpha,n,r) \rightarrow \sim \Phi$ *is provable in* AG.

The next three lemmas reduce the decision problem for the set $|B|$ to its solution for the sets $|Q_q|$.

LEMMA 5. *Let* $\Phi = \bigvee_{j<h} \Phi_j$, *where* $\Phi_j \in |Q_{q_j}|$ *and all the* q_j*'s are distinct. If, for each* $j < h$, $\mathfrak{M}_j$ *is a* q_j*-model of* $\sim \Phi_j$, *then*

$$\prod_{j<h} \mathfrak{M}_j \text{ is a model of } \sim \Phi.$$

This lemma is an immediate consequence of Lemma 2 row 8 and Lemma 3(i). Together with Lemma 4 it clearly yields a decision-procedure for all sentences of $|B|$ that do not contain any subformulas of the form $H(m)$. For, as an obvious consequence of it we have

Φ *is provable in* AG *if and only if at least one* Φ_j *is provable in* AG.

LEMMA 6. *Let Φ be as in Lemma 5, and let $m = q_s^{k_s} \dots q_t^{k_t}$, where $s \leqq h \leqq t$, and all the primes $q_0, \dots, q_t$ are distinct. Set $\Phi' = \bigvee_{j<h} \Phi'_j$, where*

$$\Phi'_j = \Phi_j \vee \sim Q^{(1)}(q_j,1,0) \vee \sim Q^{(2)}(q_j,1,0) \text{ for } j < s, \text{ and}$$

$$\Phi'_j = \Phi_j \vee \sim Q^{(1)}(q_j,k_j+1,0) \vee \sim Q^{(2)}(q_j,k_j+1,0) \vee Q^{(3)}(q_j,k_j,0) \text{ for } s \leqq j < h.$$

If, for each $j < h$, $\mathfrak{M}_j$ is a q_j-model of $\sim \Phi'_j$, then

$$\prod_{j<h} \mathfrak{M}_j \times \prod_{h \leqq j \leqq t} \mathfrak{C}_{q_j k_j} \text{ is a model of } \sim (\Phi \vee \sim H(m)).$$

This lemma follows directly from Lemmas 2 (last row), 3(ii) and (iii). Together with Lemma 1(v) and (vi) we obtain from it:

$\Phi \vee \sim H(m)$ is provable in AG if and only if Φ' is.

Since Φ' is of the form considered in Lemma 5, and since obviously $\sim H(m)$ is not provable, and $\sim H(m) \vee \sim H(m')$, for $m \neq m'$, is provable, we again have the desired reduction.

LEMMA 7. *Let Φ and m be as in Lemma 6, let $\Psi = \bigvee_{j<n} H(m_j)$, where all the m_j's are different from m, and let q be prime to all the q_j's, $j < h$, and all the m_j's, $j < n$. Then*

(i) *if $\mathfrak{A}$ is any model of $\sim \Phi$, then $\mathfrak{A} \times \mathfrak{C}_{q1}$ is a model of $\sim (\Phi \vee \Psi)$,*

(ii) *if $\mathfrak{A}$ is any model of $\sim (\Phi \vee \sim H(m))$, then $\mathfrak{A}$ is a model of $\sim (\Phi \vee \sim H(m) \vee \Psi)$.*

Parts (i) and (ii) of this lemma are trivial consequences of Lemmas 1(v), 2 and 3(i), and of Lemma 1(ii) respectively. Clearly Ψ is not provable in AG ($\mathfrak{C}_{q1}$ is a model of $\sim \Psi$), and from our lemma we conclude that:

$\Phi \vee \Psi$ is provable in AG if and only if Φ is, and

$\Phi \vee \sim H(m) \vee \Psi$ is provable in AG if and only if $\Phi \vee \sim H(m)$ is.

This closes our discussion of the decidability of $[B]$ and gives us the tools we need. For further reference we state:

(**) *The set $[B]$ is decidable in AG, i.e., the set of all those sentences of $[B]$ which are provable in AG is recursive.*

We now proceed to construct a decidable theory T for which T_f is undecidable. Let g be a recursive function on and into the set N, such that its range $R(g)$ is not recursive. We extend AG to a theory $\overline{AG}$ by adding to the axioms of AG the sequence of sentences $A(n)$, $n \in N$, where

$$A(n) = [\sim Q^{(1)}(p_{n+1},1,0) \to Q^{(1)}(2,1,g(n))].$$

$A(n)$ states that, if there is an element of order p_{n+1}, then there are exactly

$2^{g(n)}-1$ elements of order 2. The next two theorems show that the theory $T=\overline{AG}$ has the desired properties.

THEOREM 1. *Theory $\overline{AG}$ is decidable.*

Proof. Since, by (*), every sentence in the formalism of AG is effectively equivalent to a sentence of $[B]$ in AG—and hence necessarily also in $\overline{AG}$—it suffices to establish a procedure for deciding whether or not a sentence of $[B]$ is provable in $\overline{AG}$. This will clearly be achieved once we have shown how to correlate effectively with every sentence $\Theta\in[B]$ a natural number $f(\Theta)$, such that Θ is provable in $\overline{AG}$ if and only if it is derivable in the decidable theory AG from the sentences $A(0),\dots,A(f(\Theta))$.

For every $\Theta\in[B]$ we define $f(\Theta)$ as the largest number h such that some subformula of Θ either belongs to Q or is of the form $H(mp_{h-1})$. Then,

(1) either Θ is provable in AG, or else $\Theta\vee\sim Q^{(1)}(q,1,0)$ is not provable for any prime $q>p_{f(\Theta)}$.

For, if Θ is not provable in AG, then, according to Lemmas 4–7, $\sim\Theta$ has a model $\mathfrak{M}$ which is a direct product of p_j-models, for $j\leqq f(\Theta)$. But, by Lemma 2 row 8 and Lemma 3(i), $\mathfrak{M}$ is a model of $Q^{(1)}(q,1,0)$ for any $q>p_{f(\Theta)}$.

Now let Θ be any given sentence of $[B]$ and assume that Θ is provable in $\overline{AG}$. Then there is an $n\in N$ such that

(2) $\qquad A(0)\wedge\dots\wedge A(n)\rightarrow\Theta$ is provable in AG.

Assume that m is the smallest number $n\geqq f(\Theta)$ for which (2) holds. Since

$$A(m)=[\sim Q^{(1)}(p_{m+1},1,0)\rightarrow Q^{(1)}(2,1,g(m))],$$

Proposition (2) obviously implies

(3) $\quad A(0)\wedge\dots\wedge A(m-1)\wedge\sim\Theta\rightarrow\sim Q^{(1)}(p_{m+1},1,0)$ is provable in AG.

Now suppose that $m>f(\Theta)$. Then we see by inspection that the negation of the hypothesis of the sentence in (3) is equivalent to a sentence Θ' of $[B]$ for which $f(\Theta')=m$. But then, by (1) and (3), Θ' is provable and hence

(4) $\qquad A(0)\wedge\dots\wedge A(m-1)\rightarrow\Theta$ must be provable in AG.

This however contradicts our assumptions concerning m. Therefore we have $m=f(\Theta)$, and $A(0)\wedge\dots\wedge A(f(\Theta))\rightarrow\Theta$ must be provable in AG whenever Θ is provable in $\overline{AG}$. The implication in the opposite direction being obvious, we obtain:

(5) a sentence $\Theta\in[B]$ is provable in $\overline{AG}$ if and only if $A(0)\wedge\dots\wedge A(f(\Theta))\rightarrow\Theta$ is provable in AG.

Since, by (*) and (**) AG is decidable and $f(\Theta)$ is effectively correlated with Θ, (5) yields our theorem.

THEOREM 2. Theory $\overline{AG}_f$ *is undecidable.*

Proof. Consider the set of sentences $B(n)$, $n \in N$, where

$$B(n) = [(\sim H(1) \wedge \sim H(2) \wedge Q^{(1)}(2,2,0)) \rightarrow \sim Q^{(1)}(2,1,n)].$$

Notice that hypothesis of $B(n)$ is equivalent to the sentence

$$\exists x \sim (x^2 = \mathbf{1}) \wedge \forall x(x^4 = \mathbf{1} \rightarrow x^2 = \mathbf{1}).$$

We first establish the following:

(1) if $m \notin R(g)$, then $B(m)$ is valid in $\overline{AG}_f$.

In fact, let $\mathfrak{A}$ be a finite model of $\overline{AG}$ satisfying the hypothesis of $B(m)$. Then $\mathfrak{A}$, being a finite Abelian group, must have an element of odd order and hence an element of order p_{n+1} for some $n \in N$, so that $\sim Q^{(1)}(p_{n+1},1,0)$ is valid in $\mathfrak{A}$. But then, since $\mathfrak{A}$ is a model of $\overline{AG}$ and therefore in particular of the axiom $A(n)$, the sentence $Q^{(1)}(2,1,g(n))$ must be valid in $\mathfrak{A}$. By $m \notin R(g)$ we have $m \neq g(n)$, and therefore the conclusion of $B(m)$ holds in $\mathfrak{A}$. Hence $B(m)$ holds in every finite model of $\overline{AG}$ and is thus valid in $\overline{AG}_f$. In turn we show:

(2) if $m \in R(g)$, then $B(m)$ is not valid in $\overline{AG}_f$.

Indeed, let $m = g(n)$ and set $\mathfrak{A} = \mathfrak{C}_{p_{n+1}1} \times \mathfrak{C}_{21}^{g(n)}$. Then, by Lemmas 2 and 3, $\mathfrak{A}$ is a model of $\overline{AG}_f$ in which the hypothesis of $B(m)$ holds while the conclusion fails. Hence $B(m)$ is not valid in $\overline{AG}_f$. From (1) and (2) we conclude that $B(m)$ is valid in $\overline{AG}_f$ if and only if m belongs to the complement of $R(g)$ with respect to N. But we have chosen g such that this complement is not recursive, and therefore theory $\overline{AG}_f$ is undecidable.

Along the pattern of our example, decidable theories T with undecidable T_f can be constructed at will, always using a recursive function g whose range is not recursive. For instance, we can take for T the extension of AG obtained by adjoining any one of the sequences $A'(n)$, $A''(n)$, $A'''(n)$, $n \in N$, where

$$A'(n) = [Q^{(1)}(2,1,n) \rightarrow Q^{(3)}(3,1,g(n))],$$

$$A''(n) = [Q^{(1)}(2,1,n+1) \rightarrow H(2g(n))],$$

$$A'''(n) = [H(2(n+1)) \rightarrow Q^{(1)}(2,1,g(n))].$$

We can also choose as bases for our constructions theories simpler than AG, e.g., the theory E of a single equivalence relation; we then take for T the extension of E by the sentences $C(n)$ expressing the fact that, if there are exactly n one-

element equivalence classes, then there are exactly $g(n)$ 2-element classes. One of the simplest constructions is obtained by starting with a theory in which the only non-logical constants are two unary predicates, say P and Q, and the only axiom is $\forall x(P(x) \to \sim Q(x))$; to construct T we adjoin as axioms all the sentences $\exists^n x P(x) \to \exists^{g(n)} x Q(x)$, $n \in N$. Finally it should be observed that if we allow theories with infinitely many non-logical constants the matter becomes still simpler. For, let R be a binary recursive relation for which the set of all m such that mRn holds for every n is not recursive, and let $T(R)$ be the elementary theory with the infinite set of sentential constants P_k, $k \in N$, based upon the axioms $A(m,n)$ where

$$A(m,n) = [\exists^{n+1} x(x = x) \to P_m] \text{ in case } mRn \text{ holds},$$

$$A(m,n) = [\exists^{n+1} x(x = x) \to \sim P_m] \text{ in case } mRn \text{ does not hold}.$$

Then $T(R)$ is clearly decidable while $(T(R))_f$ is clearly undecidable. Notice, by the way, that every theory T which is finitely axiomatizable or decidable and for which T_f is undecidable induces in a natural way a decidable theory of the type $T(R)$ with undecidable $(T(R))_f$.

However, in spite of the existence of such very simple examples, it may be of some interest that decidable extensions of the theory of Abelian groups can be found for which the theories of finite models are undecidable.

It should be observed that the success of our method rests heavily on the fact that we are working with infinite axiomatizations. The problem whether there are finitely aximatizable decidable theories T with undecidable T_f remains open.

We now turn to our second task and show that there is an undecidable theory T for which the Theory T_f of all finite models is decidable in a non-trivial way, i.e., in spite of having models with arbitrarily large number of elements. It turns out that such a T can be found among finitely axiomatizable theories. In fact, we can take for T the elementary theory $\boldsymbol{AS}$ of Abelian cancellation semigroups with (or without) unit. The symbolism of $\boldsymbol{AS}$ coincides with that of $\boldsymbol{AG}$; the axioms of $\boldsymbol{AS}$ are the commutative, associative, and cancellation laws, and the law expressing the idempotency of $\mathbf{1}$.

THEOREM 3. *The theory $\boldsymbol{AS}$ of Abelian cancellation semigroups is undecidable.*

Proof. This theorem was established independently by Taiclin in [9] and by Tarski in [13]. For the convenience of the reader we present here Tarski's proof, which was indicated briefly in his abstract.

We begin with the construction of a particular semigroup $\mathfrak{S}$, which is a subalgebra of the multiplicative semigroup $\mathfrak{M}$ of positive integers. To this end we define a binary operation $\bigcirc$ as follows:

$$m \bigcirc n = 2^{m+1}(2n+1) \quad \text{for all } m,n \text{ in } N.$$

Furthermore we denote by R the binary relation which holds between $m,n \in N$ if and only if, for some $k \in N$,

$$2^m(2k+1) \leqq n < 2^m(2k+2);$$

in other words, if and only if the $(m+1)$-st digit from the right in the binary expansion of n is 1. Hence it is easily seen that the relation R between natural numbers is isomorphic to the membership relation between sets of finite rank, i.e., between sets belonging to the smallest family containing the empty set and closed under the operation of forming singletons and finite unions. For our purpose, however, it suffices to know that R satisfies the following two conditions:

(1) there is an $n \in N$ (in fact $n = 0$) such that mRn does not hold for any $m \in N$;

(2) for all $m,n \in N$ there is a $p \in N$ (namely n or $n + 2^m$ depending on whether mRn holds or not) such that, for every $q \in N$, qRp holds if and only if $q = m$ or qRn holds.

We now define $\mathfrak{S}$ as the semigroup of $\mathfrak{M}$ generated by the set G consisting of all primes p_{2n+1}, as well as all numbers $p_{2m+1}^3 p_{mon}$ and $p_{2n+1}^2 p_{mon}$ for any $m,n \in N$ for which mRn holds. Let P be the set of all primes p_{2n+1} and let E be the relation that holds between p_{2m+1} and p_{2n+1} if and only if mRn holds. In view of (1) and (2) the definition of E implies:

(1′) there is an $x \in P$ such that yEx does not hold for any $y \in P$;

(2′) for all $x,y \in P$ there is a $z \in P$ such that, for every $u \in P$, uEz if and only if $u = x$ or uEy.

It can be shown without difficulty that G, P and E can be characterized intrinsically within the semigroup $\mathfrak{S}$ by means of the following conditions:

(3) $x \in G$ if and only if x is an element of $\mathfrak{S}$ different from 1 and, for all elements w and z of $\mathfrak{S}$, the formula $x = w \cdot z$ implies that $w = 1$ or $z = 1$,

(4) $x \in P$ if and only if $x \in G$ and $x^3 \cdot u = y^2 \cdot v$ for some $y,u,v \in G$,

(5) xEy if and only if $x,y \in G$ and $x^3 \cdot u = y^2 \cdot v$ for some $u,v \in G$.

Let $T(S)$ be the elementary theory of the semigroup $\mathfrak{S}$. We shall show that this theory is hereditarily undecidable, i.e., that not only $T(\mathfrak{S})$ but also every subtheory of $T(\mathfrak{S})$ with the same constants is undecidable. For this purpose we consider another formalized theory F which is a fragment of the theory of sets. F has one non-logical constant, the binary predicate $\mathbf{E}$, denoting the membership relation, and is based upon the following two axioms:

$$A = \exists x \forall y \sim E(y,x),$$

$$B = \forall x \forall y \exists z \forall u(E(u,z) \leftrightarrow (u = x \vee E(u,y))).$$

It is known that:

(6) Theory F is essentially undecidable[4].

Finally we form a third theory $\overline{T}$ by adding a unary predicate **P** and a binary predicate **E** to the non-logical constants of $T(\mathfrak{S})$, and by stipulating that a sentence be valid in $\overline{T}$ and if only if it is derivable from the set of all valid sentences of $T(\mathfrak{S})$ together with the following two sentences:

$$C = [\mathbf{P}(x) \leftrightarrow (G(x) \wedge \exists y\, \exists u\, \exists v(G(y) \wedge G(u) \wedge G(v) \wedge x^3 \cdot u = y^2 \cdot v))],$$

$$D = [\mathbf{E}(x,y) \leftrightarrow (G(x) \wedge G(y) \wedge \exists u\, \exists v(G(u) \wedge G(v) \wedge x^3 \cdot u = y^2 \cdot v))],$$

where $G(x)$ is an abbreviation for the formula

$$\sim (x = \mathbf{1}) \wedge \forall w \forall z(x = w \cdot z \rightarrow (w = \mathbf{1} \wedge z = \mathbf{1})).$$

Since $T(\mathfrak{S})$ is obviously consistent, and C and D are respectively possible definitions of **P** and **E**, we have:

(7) $\overline{T}$ is a consistent extension of $T(\mathfrak{S})$.

From (1′) and (2′) we can conclude, because of (3)-(5), that the sentences $A^{(P)}$ and $B^{(P)}$, which are obtained by relativizing the axioms A and B of F to the predicate P (see [12] p. 24f.) are valid in $\overline{T}$. Consequently

(8) $\overline{T}$ is an extension of $F^{(P)}$.

By (7) and (8) we see that

(9) F is relatively interpretable in $\overline{T}$.

From (6)–(9) follows that the finitely axiomatizable and essentially undecidable theory F is relatively weakly interpretable in $T(\mathfrak{S})$. Hence, applying Theorems 8-10 of [12], pp. 23 ff. (cf. in particular the remarks at the end of section 1.5 p. 29 f.), we find that $T(\mathfrak{S})$ is indeed hereditarily undecidable. This immediately implies the undecidability of Theory AS and thus completes the proof.

This proof of Theorem 3 actually yields a stronger conclusion. Since the elementary theory of a particular subsemigroup of the multiplicative semigroup $\mathfrak{M}$ of positive integers has been proven hereditarily undecidable, the elementary theory of the class of all subsemigroups of $\mathfrak{M}$ is also hereditarily undecidable (see [13]).

Finally we arrive at the decidability of the theory of finite Abelian semigroups by exhibiting an axiomatization for the theory of finite Abelian groups.

---

(4) The fact that Theory F with an additional axiom, the law of extensionality for E, is essentially undecidable was stated without proof in [12] p. 34 as a joint result of Szmielew and Tarski. Vaught in [15] p. 21 shows that the result can be improved by omitting the additional axiom.

THEOREM 4. (i) *The theory AG_f of finite Abelian groups coincides with the extension of AG obtained by adjoining all sentences $D(q,k,n)$, for any prime $q, 0 < k \in N$, and $n \in N$, where*

$$D(q,k,n) = [Q^{(1)}(q,k,n) \leftrightarrow Q^{(2)}(q,k,n)].$$

(ii) *The theory AS_f of finite Abelian cancellation semigroups coincides with AG_f and is decidable*([5]).

Proof. (i) Let D be the set of all sentences $D(q,k,n)$, let AG_D be the extension obtained from AG by adjoining the sentences of D, and let AG_p be the elementary theory of periodic groups, i.e., of Abelian groups in which one of the sentences $H(m)$ is valid (groups of the first kind in the sense of [8]). Then

(1) AG_D is a subtheory of AG_p, i.e., every sentence provable on AG_D is valid in AG_p.

For, from Lemma 1 (v) and (vi) follows that for every m and every q there is an h such that

$$H(m) \rightarrow (Q^{(1)}(q,h,0) \wedge Q^{(2)}(q,h,0))$$

is provable in AG. But, for any q, h, k, and n the sentence

$$Q^{(1)}(q,h,0) \wedge Q^{(2)}(q,h,0) \rightarrow D(q,k,n)$$

is derivable from the sentences listed in Lemma 1 (iii) and (iv). Therefore all the sentences of D are valid in every periodic Abelian group and hence in AG_p. Furthermore, since every finite group is periodic, we obtain as an immediate consequence of (1)

(2) AG_D is a subtheory of AG_f.

To prove the converse, consider any sentence Θ which is not provable in AG_D, so that

(3) $\sim \Theta$ is compatible in AG with D.

We shall show by cases that

(4) $\sim \Theta$ has a finite Abelian group as a model.

Case (a): $\Theta \in |Q_q|$ for some fixed q. Now, if for some k and n, and for $j = 1$ or 2, the sentence $\sim Q^{(j)}(q,k,n)$ is a disjunct of Θ, then

(5) $\sim \Theta$ is compatible in AG with $Q^{(1)}(q,k,n) \wedge Q^{(2)}(q,k,n)$;

for, by our assumption (3), $\sim \Theta$ is compatible with $D(q,k,n)$. But then, by Lemma

([5]) The decidability of AG_f was established independently by Eršov and by the author (using different methods of proof); see [2] and [3].

4, the sentence $\sim\Theta \wedge Q^{(1)}(q,k,n) \wedge Q^{(2)}(q,k,n)$ must have a q-model. Inspection of Lemma 2, and Lemma 3(i), however, show that a q-model of the sentence $Q^{(1)}(q,k,n) \wedge Q^{(2)}(q,k,n)$ cannot have any direct factors $\mathfrak{R}_q$ or $\mathfrak{C}_q$ (by definition a q-model never has both groups as factors) and hence is finite. Thus

(6) $\sim\Theta$ has a finite q-model.

Suppose, on the other hand, that no disjunct of Θ is of the form $\sim Q^{(j)}(q,h,n')$ for $j=1$ or 2, any positive integer h and any $n' \in N$. Then let $k-1$ be the largest positive integer h such that some subformula of Θ is of the form $Q^{(i)}(q,h,n')$, $i=1,2$ or 3. Then, since, by assumption (3) and Lemma 4, $\sim\Theta$ has a q-model, there must be a k-termed sequence r of natural numbers such that $\Theta' = \bigwedge_{0<h<k} Q^{(3)}(q,h,r_h)$ and $\sim\Theta$ are compatible in AG. Now let $n-1$ be the largest $n' \in N$ such that some subformula of Θ is of the form $Q^{(i)}(q,h,n')$, $i=1,2$, or 3. Since, by assumption, Θ does not have any disjuncts $\sim Q^{(j)}(q,h,n')$ with $j=1$ or 2, we find, by Lemmas 1(i), 2 and 3(i), that the finite group $\mathfrak{M}(0,0,r) \times C^n_{qk}$ is a model of $\Theta' \wedge \sim\Theta$ whence (6) (and (5) too) is established again. Hence (4) holds in case (a).

Case (b): $\Theta = \Phi = \bigvee_{j<h} \Phi_j$ where the Φ_j's are as in Lemma 5. Then, by (3), each sentence $\sim\Phi_j$ is compatible in AG with D. Hence, by case (a), each sentence $\sim\Phi_j$ has a finite q_j-model, and this, by Lemma 5, implies (4).

Case (c): Let $\Theta = \Phi \vee \sim H(m)$ where Φ and m are as in Lemma 6, and let Φ' too be as in Lemma 6. Then, since by Lemma 1 (v) and (vi) the sentence $\sim\Theta \rightarrow \sim\Phi'$ is provable in AG, we find that, because of (3), $\sim\Phi'$ is compatible in AG with D. Thus, by case (b), $\sim\Phi'$ has a finite model, the direct product of which with another finite model as in Lemma 6 is, by Lemma 6, a model of $\sim\Theta$. And thus (4) proves to hold again.

Case (d): Θ is an arbitrary sentence in $|B|$. By Lemma 7, this case reduces to the previous cases.

Case (e): Θ is an arbitrary sentence in the formalism of AG. But then, (see (*)), Θ is equivalent in AG to a sentence of $[B]$, i.e., to some sentence Θ' which is a conjunction of some sentences Θ'_j of $|B|$. By (3) and cases (a)–(d), at least one of the sentences $\sim\Theta'_j$ must have a finite Abelian group as a model, and this group will then, of course, also be a model of $\sim\Theta$.

We have thus shown that (3) always implies (4). Consequently every sentence that is valid in AG_f is derivable in AG from D, i.e.,

(7) AG_f is a subtheory of AG_D,

and in view of (2) our proof of (i) is complete.

As a byproduct of this proof we mention that, by (1) and (7), *the elementary theories of periodic Abelian groups and of finite Abelian groups coincide.*

(ii) It is well known and easy to show that every finite cancellation semi-group is a group; hence AG_f and AS_f coincide. Furthermore, part (i) of our theorem

implies that the set of sentences which are valid in AG_f is recursively enumerable. On the other hand a sentence is not valid in AG_f if and only if its negation has a finite model which is an Abelian group. Using the fact that AG is finitely axiomatizable (or that it is decidable) we can effectively enumerate all finite Abelian groups. Thus, if a sentence $\sim\Theta$ has a finite Abelian group as a model, it can effectively be found. Therefore the set of all sentences in the formalism of AG, which are not valid in AG_f, is also recursively enumerable. This completes the proof of part (ii) of our theorem.(6)

We conclude with the remark that the extension $\overline{AG_f}$ obtained from AG_f by adjoining all the sentences $A(n)$ would have served as well as $\overline{AG}$ for an example of a decidable theory whose theory of finite models—namely $\overline{AG}_f(=(\overline{AG_f})_f)$—is undecidable.

References

1. Cobham, A., 1962, Undecidability in group theory, *Amer. Math. Soc. Notices*, **9**, 406.

2. Eršov, U., 1963, Razrešimost' èlementarnyh, teorii nekotoryh klassov abelevyh grupp (Decidability of certain classes of Abelian groups). *Algebra i Logika Seminar*, **1**, 37–41.

3. Huber Dyson, V., 1963, A decidable theory for which the theory of finite models is undecidable, *Amer. Math. Soc. Notices*, **10**, 453.

4. Huber Dyson, V., 1963, A decidable theory for which the theory of infinite models is undecidable, *Amer. Math. Soc. Notices*, **10**, 491.

5. Janiczak, A., 1953, Undecidability of some simple formalized theories, *Fund Math.*, **40**, 131–139.

6. Langford, C., 1927, On a type of completeness characterizing the general laws for separation of pointpairs, *Trans. Amer. Math. Soc.*, **29**, 96–110.

7. Mal'cev, A., 1961, Effective inseparability of the set of identically true from the set of finitely refutable formulas of certain elementary theories, *Soviet Mathematics*, **2**, 1005–1008. (Original in Russian: *Doklady Akadémii Nauk*, **139**, (1961) 802–805).

8. Szmielew, W., Elementary properties of Abelian groups. *Fund. Math.*, **41** 1955, pp. 203–271.

9. Taiclin, M. Nerazresimost' èlementarnoi teorii kommutativnyh polygrupp so sokrascenem (Undecidability of the elementary theory of commutative semigroup with cancellation). *Sibirskii Matematiceskii Zhurnal*, **3**, (1962), pp. 308–309.

10. Taiclin, M., 1962, Effektivnaya neotdelimost' množestva toždestvenno istinnyh i množestva konečno oproveržimyh formul èlementarnoi teorii struktur (Effective inseparability of the set of identically true and the set of finitely refutable formulas of the elementary theory of lattices). *Algebra i Logika Seminar*, **1**, 24–38.

11. Tarski, A., 1949, Arithmetical classes and types of Boolean algebras, *Bull. Amer, Math. Soc.*, **55**, 64.

12. Tarski, A., Robinson, R.M. and Mostowski, A., 1953, *Undecidable Theories*, North Holland Publ. Co., Amsterdam.

(6) The argument just outlined applies of course to an arbitrary theory T and leads to the conclusion that *for every theory T which is finitely axiomatizable or decidable, the set of sentences that are not valid in T_f is recursively enumerable.*

13. Tarski, A., 1962, Solution of the decision problem for the elementary theory of commutative semigroups, *Amer. Math. Soc. Notices*, **9**, 205.

14. Trahtènbrot, B., 1950, Nevozmožnost' algorifma dlya problemy razešiomstina konečnyh klassah (Impossibility of an algorithm for the decision problem in finite classes). *Doklady Akadémii Nauk, SSSR*, **70**, 569–572.

15. Vaught, R., 1962, On a theorem of Cobham concerning undecidable theories, *Proceedings of the* 1960 *International Congress on Logic, Methodology and Philosophy of Science*, Stanford pp. 14–25.

ADELPHI COLLEGE
GARDEN CITY, LONG ISLAND, NEW YORK