BÜCHI, R.
Math. Annalen 148, 201—213 (1962)

Turing-Machines and the Entscheidungsproblem*

By

J. RICHARD BÜCHI in Ann Arbor and Mainz

Let Q be the set of all sentences of elementary quantification theory (without equality). In its semantic version Hilbert's Entscheidungsproblem for a class $X \subseteq Q$ of sentences is,

$[X]$: To find a method which for every $S \in X$ yields a decision as to whether or not S is satisfiable.

CHURCH [3] showed that $[Q]$ is recursively unsolvable. Shortly thereafter TURING [6] obtained this result more directly by reducing to $[Q]$ an unsolvable problem on Turing-machines. This reduction however is rather involved, and requires much detailed attention of the kind which does not add to one's overall understanding of the situation. We will show in this paper that the connection between Turing-machines and quantification theory is really a rather simple one. The key to it is lemma 3, which is closely related to the Skolem-Gödel-Herbrand work on quantification theory. As a result we obtain the first really elegant proof of unsolvability of $[Q]$. It can be outlined thus:

Lemma 1: *The set* Hlt, *consisting of all Turing-machines which eventually halt, if started on the empty tape, is not recursive.*

Lemma 2: *To any Turing-machine M one can construct a matrix $\underline{M}(x,u,y)$, with individual variables x, u, y, monadic predicate letters, and 3 binary predicate letters, such that $M \notin$ Hlt if and only if $Zo \wedge (\forall xy)\ \underline{M}(x, x', y)$ is satisfiable in the natural number system $\langle N, o, '\rangle$*[1].

Lemma 3: *For any matrices $\underline{Z}(x)$ and $\underline{M}(x, u, y)$, the sentence $(\exists x)\ \underline{Z}(x) \wedge \wedge (\forall x)\ (\exists u)\ (\forall y)\ \underline{M}(x, u, y)$ is satisfiable if and only if $\underline{Z}(o) \wedge (\forall xy)\ \underline{M}(x,x',y)$ is satisfiable in $\langle N, o, '\rangle$.*

By lemmas 2 and 3, to any Turing-machine M one can construct a sentence S of form $\exists \wedge \forall\exists\forall$, such that $M \notin$ Hlt if and only if S is satisfiable. Therefore, by lemma 1,

Theorem 1: *The problem $[\exists \wedge \forall\exists\forall]$ is not recursively solvable, even if restricted to sentences in which, besides monadic letters, only three binary predicate letters occur.*

---

* The results of this paper were announced in the Notices, Am. Math. Soc. 8, 354 (1961), and appeared as University of Michigan Technical Report, December, 1961. The work was supported by grants from the National Science Foundation and the U. S. Army Signal Corps, and by a contract with the Office of Naval Research.

1) The expression "satisfiable in $\langle N, o, '\rangle$" is not to be confused with "satisfiable in N". Here as in other places we prefer a somewhat abbreviated terminology, so as not to drown the main ideas in a formalistic flood. With a bit of good will the reader will find it possible to supply the details.

To stress the simplicity of this argument we wish to claim that the following hints suffice to prove the three lemmas: Lemma 1 is well known and immediately follows from the basic unsolvability result on Turing-machines (machine halting on the tape carrying its description). Proving lemma 2 is just an exercise on Turing-machines. One first describes the operation of a machine M on the empty tape in the form of a matrix $\underline{C}(Q, S, K, o, ', x, y)$, whereby $Qx =$ state at time x, $Kyx \equiv$ position y is scanned at time x, $Syx =$ tape-symbol at position y and time x. It is important to note that the functions Q and S are finite-valued, and therefore can be considered to be vectors of monadic and binary predicates on natural numbers. $M \in$ Hlt now means that no Q, K and S exist such that for all places y and all times x, $\underline{C}(Q, S, K, o, ', x, y)$. It remains to invent some tricks to put the matrix $\underline{C}(o, ', x, y)$ into the form $Z(o) \wedge \underline{M}(x, x', y)$, by adding auxiliary predicates. Lemma 3 is trivial in the "if-direction". In the other direction one might use the axiom of choice to introduce a monadic Skolem-function fx for $(\exists u)$ and a constant c for $(\exists x)$. It remains to note that $\underline{Z}(c) \wedge (\forall xy)\ \underline{M}(x, fx, y)$ is satisfiable if and only if it is satisfiable by predicates in N and $c = o$, $fx = x'$.

This proof has the further advantage of directly yielding unsolvability for the very simple type $\exists \wedge \forall\exists\forall$. The unsolvability of $[\exists \wedge \forall\exists \wedge \forall\forall\forall]$ follows, by replacing the part $\forall\exists\forall$ by its Skolem-form $\forall\exists \wedge \forall\forall\forall$. (Compare these results with Bernays' (1958) analysis of Turing's proof.) More important is, that our method of using lemma 3, for the first time provides real hope of settling the decision problem for the only remaining prefix-types $\forall\exists\forall$ and $\forall\exists \wedge \forall\forall\forall$. Furthermore, with slight modifications we obtain an improved version of TRACHTÉNBROT's (1950) result about satisfiability in finite domains:

Theorem 2: *There is no recursive set which separates the not-satisfiable sentences from those satisfiable in a finite domain; even if only sentences of form* $\exists \wedge \forall\exists\forall$ *are considered.*

Corollary: *The set of* $\exists \wedge \forall\exists\forall$ *sentences, which are finitely satisfiable, is not recursive.*

Clearly theorem 2 follows from the following stronger versions of lemmas 1, 2, and 3:

Lemma I: *Let* Cyl *be the set of all Turing-machines which eventually cycle, if started on the empty tape. The sets* Hlt *and* Cyl *are not recursively separable.*

Lemma II: *The construction* $M \rightarrow \underline{M}$ *of lemma 2 has the further property:* $M \in$ Cyl *if and only if* $Zo \wedge (\forall xy)\ \underline{M}(x, x', y)$ *is satisfiable in* $\langle N, o, '\rangle$ *by periodic predicates.*

Lemma III: *Add to lemma 3: The sentence* $(\exists x)\ \underline{Z}(x) \wedge (\forall x)\ (\exists u)\ (\forall y)\ \underline{M}(x, u, y)$ *is satisfiable in a finite domain, if and only if,* $\underline{Z}(o) \wedge (\forall xy)\ \underline{M}(x, x', y)$ *is satisfiable in* $\langle N, o, '\rangle$ *by periodic predicates.*

We will now indicate the proofs of the lemmas, and add some additional discussion at the end of the paper.

Proof of lemmas 2 and II: A (Turing-) *machine* we define to be a system $M = \langle \underline{D}, A, \underline{L}, \underline{R}, \underline{P}, \underline{Q}, \underline{S}\rangle$ consisting of a finite set $\underline{D}$ of elements called *states;*

an $A \in \underline{D}$ called the *initial state;* three binary predicates $\underline{L}[X, Y]$, $\underline{R}[Y, X]$, $\underline{P}[X, Y]$, called *commands* of *left-move*, *right-move*, and *print;* a binary function $\underline{Q}[X, Y]$ with values in $\underline{D}$, called the *new-state-function;* and a function $\underline{S}[X, Y]$ with values in $\{T, F\}$, called the *print-function.* All these predicates and functions have arguments $X \in \underline{D}$ and $Y \in \{T, F\}$, furthermore $\underline{L}$, $\underline{R}$, $\underline{P}$ are to be exclusive and complementary. The *tape-symbols* are T and F, a *tape* is a one-way infinite sequence of tape-symbols, i.e. a predicate Ix on N. The tape $Ix \equiv F$ is called the *empty tape.*

The *operation of a machine* M, set to work on a tape I, is as follows. M is started in its initial state A, scanning the zero-position of the tape I. If at any time x it is in state X and scans position y of the tape, which now carries the symbol Y, then,

if $\underline{L}[X, Y]$ it moves to scan position $y - 1$

if $\underline{R}[X, Y]$ it moves to scan position $y + 1$

if $\underline{P}[X, Y]$ it prints $\underline{S}[X, Y]$ in place of Y at position y.

In all cases it goes into the new state $\underline{Q}[X, Y]$. Note that if $y = o$ and the command is $\underline{L}[X, Y]$, then M will next scan position -1, i.e., it *runs off the tape.* In this case we say that the machine *halts* at time $x + 1$, and that the tape I is *accepted* by M; in symbols $\mathrm{Hl}(M, I)$. The set Hlt consists of all machines M which eventually halt if put to work on the empty tape.

Now let $M = \langle \underline{D}, A, \underline{L}, \underline{R}, \underline{P}, \underline{Q}, \underline{S} \rangle$ be any machine. From it we construct the formula $\underline{C}(Q, S, K, L, R, P, x, y)$ as conjunction of the following parts,

$$
\text{(i)}\quad
\begin{array}{ll}
Qo = A \wedge \sim Syo & Koo \wedge \sim Ky'o \\
Kyx \supset \cdot\, Qx' = \underline{Q}[Qx, Syx] & Lx \supset \cdot\, Kyx' \equiv Ky'x \\
Kyx \wedge \underline{L}[Qx, Syx] \cdot\!\supset\!\cdot\, Lx \wedge \sim Px \wedge \sim Rx & Px \supset \cdot\, Kyx' \equiv Kyx \\
Kyx \wedge \underline{P}[Qx, Syx] \cdot\!\supset\!\cdot\, Px \wedge \sim Lx \wedge \sim Rx & Rx \supset \cdot\, Ky'x' \equiv Kyx \\
Kyx \wedge \underline{R}[Qx, Syx] \cdot\!\supset\!\cdot\, Rx \wedge \sim Lx \wedge \sim Px & Rx \supset \cdot \sim Kox' \\
\sim Kyx \vee Lx \vee Rx \quad \cdot\!\supset\!\cdot\, Syx' \equiv Syx & \sim [Kox \wedge Lx] \\
\qquad Kyx \wedge Px \quad \cdot\!\supset\!\cdot\, Syx' \equiv \underline{S}[Qx, Syx] &
\end{array}
$$

and we claim that[1]),

$$\text{(1)}\qquad M \notin \mathrm{Hlt} \cdot\!\equiv\!\cdot (\forall xy)\underline{C} \quad \text{is satisfiable in } \langle N, o, {}' \rangle.$$

Suppose first that $M \notin \mathrm{Hlt}$, i.e., M put to work on the empty tape does never halt. Then clearly the functions and predicates

$$
\text{(j)}\quad
\begin{array}{rl}
Qx = & \text{state of } M \text{ at time } x \\
Syx \equiv & \text{tape-symbol at time } x \text{ and position } y \text{ is } T \\
Kyx \equiv & \text{at time } x \text{ position } y \text{ is scanned by } M \\
Lx \equiv & \text{at time } x \text{ the command is left-move} \\
Rx \equiv & \text{at time } x \text{ the command is right-move} \\
Px \equiv & \text{at time } x \text{ the command is print}
\end{array}
$$

are defined for all x and y. Furthermore, because M is started on the empty tape and never runs off the tape, these Q, S, K, L, R, P will satisfy $Qo = A$, $Koo \wedge \sim Ky'o$, $\sim Syo$ and $\sim [Kox \wedge Lx]$, for any x and y. Referring to our description of the operation of a machine, one easily verifies that also the remaining formulas of (i) are satisfied for all x and y. In other words, $(\forall xy)\underline{C}$ becomes true in $\langle N, o, ' \rangle$, if its variables are given the values (j). Thus, (1) is established in the left-right direction.

Suppose next that $(\forall xy)\underline{C}$ is satisfiable in $\langle N, o, ' \rangle$. Then there are a function $Q : N \to \underline{D}$ and predicates S, K, L, R, P, such that for all x and y in N the formulas (i) hold. Now suppose M is put to work on the empty tape, and refer back to our description of the operation of a machine. By induction on x and the use of (i) one then shows that Q, S, K, L, R, P must satisfy (j), for all x and y[2]). It follows that at no time x, the machine M halts, if started on the empty tape, i.e., $M \notin$ Hlt. This completes the proof of (1).

Note that the states of a machine $M = \langle \underline{D}, A, \underline{L}, \underline{R}, \underline{Q}, \underline{S} \rangle$ may be coded as vectors of truth-values, so that A stands for a vector $(A_1, \ldots, A_n)$ of truth-values, and $\underline{Q}$ for a vector $(\underline{Q}_1, \ldots, \underline{Q}_n)$ of formulas of propositional calculus (n depending on the number of states of M). Furthermore, the expressions $Qo = A$ and $Qx' = \underline{Q}[Qx, Syx]$ stand for conjunctions of terms of the form $Q_i o \equiv A_i$ and $Q_i x' \equiv \underline{Q}_i [Q_1 x, \ldots, Q_n x, Syx]$. $\underline{C}$ therefore is a matrix of quantification-theory. With the construction $M \to \underline{C}$, and the established (1), we thus are pretty close to a proof of lemma 2. All that remains to be done is to note that the following modifications of $\underline{C}$ do not affect the validity of (1).

1. Introduce an additional binary predicate-letter H. On the right side of $\underline{C}$ replace $Ky'o$ by Hyo, $Ky'x$ by Hyx, $Ky'x'$ by Hyx', and conjoin $Hxy \equiv Kx'y$. The resulting matrix is of form $\underline{C}^*(o, x, x', y)$.

2. Introduce an additional monadic predicate-letter Z. To $\underline{C}^*$ conjoin $Zo \wedge \sim Zx'$ and replace $[Qo{=}A] \wedge \sim Syo$ by $Zx \supset \cdot [Qx{=}A] \wedge \sim Syx$, $Koo \wedge \wedge \sim Hyo$ by $Zx \supset \cdot Kxx \wedge \sim Hyx$, $\sim Kox'$ by $Zy \supset \sim Kyx'$, and $\sim [Kox \wedge Lx]$ by $Zy \supset \sim [Kyx \wedge Lx]$. The resulting formula is of form $Zo \wedge \underline{M}(x, x', y)$. $M \to \underline{M}$ is the construction required in lemma 2. That the same construction also satisfies lemma II, will now be shown.

The machine M, if started on the tape I, *goes into a p-cycle* at time l, if at the later time $(l + p)$ it is faced with an identical situation, i.e., at times l and $(l + p)$ M is in the same state and scans identical tapes in the same position. We will say that M (eventually) *p-cycles on I*, in symbols $\mathrm{Cy}_p(M, I)$, if at some time it goes into a p-cycle. (It may be shown that for some p, $\mathrm{Cy}_p(M, I)$ holds if and only if M never runs off the tape and scans only in a bounded part of the tape.) The set Cyl is defined to consist of all those machines M which eventually cycle, if put to work on the empty tape.

A predicate Ux on N is called *periodic* with *phase* l and *period* $p > o$, if $U(x + p) \equiv Ux$ for all $x \geqq l$. A relation Vxy on N is called *periodic* with *phase* l and period $p > o$, if $V(x + p)y \equiv Vxy$ for all $x \geqq l$ and all y, and

[2]) The details are best left to the reader. It should be noted that, by our definition of machines, $\underline{L}$, $\underline{R}$, $\underline{P}$ are mutually exclusive.

$Vx(y+p) \equiv Vxy$ for all x and all $y \geqq l$. (Note that the entire line Vxl has to repeat at $Vx(l+p)$, and not just from $x = l$ on!)

Suppose now that $M \in$ Cyl, that is, M goes into a p-cycle at time l, if started on the empty tape. Then clearly the functions Q, L, R, P are periodic and Syx and Kyx are periodic in the time-argument x, all of them with phase l and period p. Furthermore, if d is the maximum of all positions scanned by M before time $(l+p)$, then at no time t a position $y > d$ will be scanned. It follows that $Kyx \equiv F$, for all x and all $y > d$, and because $Syo \equiv F$ and M never scans beyond d, also $Syx \equiv F$ for all x and all $y > d$. Thus, also K and S are periodic (with phase $\geqq l, d$ and period p). In other words, the implication from left to right of (2) is valid.

(2) $M \in \mathrm{Cyl} \cdot\equiv\cdot (\forall yx)\underline{C}$ is satisfiable by periodic predicates in $\langle N, o, {}' \rangle$.

In the other direction (2) is trivially valid because the only solution of $(\forall yx)\underline{C}$ are the predicates Q, S, K, L, R, P describing the operation of M; and to say that Q, S, K, are periodic (in the time argument) just means that M eventually cycles. Because the modifications 1. and 2. of $\underline{C}$ to C^* to $Zo \wedge \underline{M}$ clearly do not affect the validity of (2), this ends the proof of lemma II.

Proof of lemma I: We omit giving a direct proof of lemma 1, as it is well known from the literature. Of the proof of lemma I we present an intuitive sketch:

The *block* of length l is the tape given by $Iy \equiv (y < l)$. It is clear that one can effectively set up a *coding function* $\mathrm{cd}(M)$ which maps one-to-one all machines onto all blocks. A set X of blocks is called *recursive* if there are machines M_1 and M_2 such that for all blocks I,

$$\text{(a)} \qquad \begin{aligned} I \in X &\cdot\equiv\cdot \mathrm{Hl}\,(M_1, I) \\ I \notin X &\cdot\equiv\cdot \mathrm{Hl}\,(M_2, I)\,. \end{aligned}$$

A set Y of machines is called *recursive* if the set $\mathrm{cd}(Y)$ of blocks is recursive. As to the equivalence of this to other definitions of "recursive sets" we remark:

1. It is well known that the restriction to two tape-symbols (one of them the blank) and one-way infinite tapes is not a serious one, 2. Machines which print and move at the same time can, by adding new states, easily be modified so as to either only print or only move in each atomic act, 3. We might have added another command predicate $H[X, Y]$, to obtain halt-situations in addition to "running off the tape". But these can be eliminated by adding an additional state B, such that $H[X, Y]$ implies that the next state is B, and B requires M to stay in B and move left.

Note that for a machine M to 1-cycle simply means that it keeps scanning at the same position. Thus, one can find a predicate $\underline{C}_1[X, Y]$ such that M at time t goes into a 1-cycle just in case $\underline{C}_1[X, Y]$ holds for the state X and scanned symbol Y. Let now M' be obtained by adding a new state B with $\underline{Q}[B, Y] = B$, and conjoining $\underline{C}_1$ to the right-move condition $\underline{R}$. Then clearly

$\mathrm{Hl}(M, I) \equiv \mathrm{Hl}(M', I)$, but M' never 1-cycles. Similarly one can modify a machine M to M' such that $\mathrm{Hl}(M, I) \equiv \mathrm{Cy}_1(M', I)$ and M' does not halt on any block I. Thus in the definition of recursive sets of blocks one may replace (a) by

(b)
$$I \in X \cdot\equiv\cdot \mathrm{Cy}_1(M_1, I) \text{ and } M_1 \text{ does not halt on blocks}$$
$$I \notin X \cdot\equiv\cdot \mathrm{Hl}(M_2, I) \text{ and } M_2 \text{ never 1-cycles}.$$

It now is possible to combine M_1 and M_2 into one machine M which 1-cycles on $I \in X$ and halts on $I \notin X$. Thus, to every recursive set X of blocks there is a machine M_0 such that for all blocks I,

(c)
$$I \in X \cdot\equiv\cdot \mathrm{Cy}_1(M_0, I)$$
$$I \notin X \cdot\equiv\cdot \mathrm{Hl}(M_0, I).$$

By the usual diagonal-argument we now can prove lemma I:

Suppose that Y is a recursive set of machines and separates the sets of machines for which $\mathrm{Hl}(M, \mathrm{cd}\,M)$ respectively $\mathrm{Cy}_1(M, \mathrm{cd}M)$, i.e.,

$$\mathrm{Hl}(M, \mathrm{cd}\,M) \supset M \in Y$$
$$\mathrm{Cy}_1(M, \mathrm{cd}M) \supset M \notin Y.$$

By (c) there is a machine M_0, such that

$$M \in Y \supset \mathrm{Cy}_1(M_0, \mathrm{cd}M)$$
$$M \notin Y \supset \mathrm{Hl}(M_0, \mathrm{cd}M).$$

Now $M_0 \in Y$ implies $\mathrm{Cy}_1(M_0, \mathrm{cd}M_0)$ implies $M_0 \notin Y$, and $M_0 \notin Y$ implies $\mathrm{Hl}(M_0, \mathrm{cd}M)$ implies $M_0 \in Y$. This is contradictory, and therefore,

(d) The sets $A = \{M; \mathrm{Hl}(M, \mathrm{cd}\,M)\}$ and $B = \{M; \mathrm{Cy}_1(M, \mathrm{cd}M)\}$ are not separable by a recursive set.

Because there is a recursive mapping f from machines to machines such that

$$\mathrm{Hl}(M, \mathrm{cd}\,M) \supset fM \in \mathrm{Hlt}$$
$$\mathrm{Cy}_1(M, \mathrm{cd}\,M) \supset fM \in \mathrm{Cyl}_1$$

it follows from (d) that also Hlt and Cyl_1 are not separable. Finally, because $\mathrm{Cyl}_1 \subseteq \mathrm{Cyl}$, we conclude that Hlt and Cyl are inseparable.

Proof of lemma 3 and III: We will assume that the matrices $\underline{Z}$ and $\underline{M}$ contain only one predicate-letter R, which is binary. The general case does not present any new problems. Let $\Sigma(R)$ stand for the sentence $(\exists x)\,\underline{Z}(x) \wedge (\forall x)\,(\exists u)\,(\forall y)\,\underline{M}(x, u, y)$, and $\Sigma^*(a, f, R)$ for its Skolem-transform $\underline{Z}(a) \wedge (\forall xy)\,\underline{M}(x, fx, y)$.

Now suppose that $\Sigma(R)$ is satisfiable, i.e., has a model $\langle D_1, R_1\rangle$. By the axiom of choice it follows that there is an $a_1 \in D_1$ and a function $f_1\colon D_1 \to D_1$, such that $\underline{D}_1 = \langle D_1, a_1, f_1, R_1\rangle$ is a model of $\Sigma^*(a, f, R)$. Let D_2 be the smallest subset of D_1 which contains a_1 and is closed under f_1, let $a_2 = a_1$, $f_2 =$ restriction of f_1 to D_2, $R_2 =$ restriction of R_1 to D_2. Because Σ^* is a universal sentence it follows that $\underline{D}_2 = \langle D_2, a_2, f_2, R_2\rangle$ still is a model of Σ^*. Next we note that

$\langle N, o, {}' \rangle$ is the free algebra with one generator and one monadic function. Because $\langle D_2, a_2, f_2 \rangle$ is generated by a_2 and f_2, it follows that there is a homomorphism h from $\langle N, o, {}' \rangle$ onto $\langle D_2, a_2, f_2 \rangle$. If we now define $R_3xy \equiv \equiv R_2(hx)(hy)$, then it is clear that $\underline{D}_2$ is strong homomorphic image of $\langle N, o, {}', R_3 \rangle$. Again because Σ^* is universal it therefore follows that $\langle N, o, {}', R_3 \rangle$ is still a model of $\Sigma^*(a, f, R)$[3]. Thus,

(1) Σ is satisfiable $\cdot \supset \cdot$ Σ^* is satisfiable in $\langle N, o, {}' \rangle$.

Suppose now further, that the model $\langle D_1, R_1 \rangle$ of Σ is finite. Then clearly the algebra $\langle D_2, a_2, f_2 \rangle$ is finite. It follows that the congruence relation $hx = hy$ on $\langle N, o, {}' \rangle$ is of finite index, and therefore must be of form

$$hx = hy \cdot \equiv \cdot x = y \vee [x \geqq l \wedge y \geqq l \wedge x \equiv y \ (\mathrm{mod}\, p)],$$

for some l and $p > o$. It follows that the relation R_3xy is periodic with phase l and period p. Thus we have shown,

(2) Σ finitely satisfiable $\cdot \supset \cdot \Sigma^*$ periodically satisfiable in $\langle N, o, {}' \rangle$.

The converse to (1) is trivial, so that lemma 3 is established. To establish lemma III it remains only to prove the converse to (2). This goes as follows:

Suppose $\underline{D} = \langle N, o, {}', R_1 \rangle$ is a model of $\Sigma^*(a, f, R)$, whereby R_1 is periodic, say of phase l and period $p > o$. The relation

$$x \sim y \cdot \equiv \cdot x = y \vee [x \geqq l \wedge y \geqq l \wedge x \equiv y (\mathrm{mod}\, p)]$$

is clearly a congruence relation of $\langle N, o, {}' \rangle$, and because R_1 has phase l and period p, it is also a congruence relation of R_1. Consequently one can form the factor $\underline{D}/\!\sim$ of the relational system $\underline{D}$. Because Σ^* is universal and $\underline{D}/\!\sim$ is homomorphic image of $\underline{D}$, it follows that $\underline{D}/\!\sim$ is still a model of Σ^*. Furthermore, $\underline{D}/\!\sim$ is finite, because $\sim$ is of finite index. But from any model of $\Sigma^*(a, f, R)$ one obtains a model of $\Sigma(R)$, if one just omits the interpretations of a and f. Thus Σ has a finite model.

This concludes the proof of the lemmas. We add some further discussion of the results.

General form of lemma III: Without any essential change in the presented proof, one can establish the result for general sentences of Q. In place of $\langle N, o, {}' \rangle$ appear the *totally free* algebras $\underline{F}_n^{m_1, \ldots, m_k} = \langle N, o_1, \ldots, o_n, f_1, \ldots, f_k \rangle$ with n generators and k operations, f_i having m_i arguments. A *periodic relation on* $\underline{F}$ is one which admits a congruence of $\underline{F}$ of finite index. A *Skolem-transform* $\Sigma^*(o_1, \ldots, o_n, f_1, \ldots, f_k, R)$ of an arbitrary sentence $\Sigma(R)$ in Q is obtained by first writing Σ as a conjunction of prenex sentences, and next replacing existential quantifiers by individual-letters and function letters, in the well

[3]) A strong homomorphism h of $\underline{D} = \langle D, f, R \rangle$ onto $\underline{D}^* = \langle D^*, f^*, R^* \rangle$ is characterized by $h(fxy) = f^*(hx)(hy)$ and $Rxy \equiv R^*(hx)(hy)$. There seems to be a widespread prejudice that h^{-1} does not preserve the validity of universal sentences S. Of course, this is justified in case S contains the equality-sign, and one demands that it must be interpreted as equality. In the other case, a bit of reflection will show the prejudice to be faulty.

known manner (suggested by the axiom of choice). The general form of lemma III now is,

Lemma III: *Let $\Sigma(R_1, \ldots, R_s)$ be any sentence of Q, let $\Sigma^*(o_1, \ldots, o_n, f_1, \ldots, f_k, R_1, \ldots, R_s)$ be a Skolem-transform of Σ.*

(a) *Σ is satisfiable, if and only if, Σ^* is satisfiable in the totally free algebra $\underline{F}_n^{m_1, \ldots, m_k}$.*

(b) *Σ is satisfiable in a finite domain, if and only if, Σ^* is satisfiable in $\underline{F}_n^{m_1, \ldots, m_k}$ by periodic relations.*

The proof we gave (using the axiom of choice) simply carries one step farther Skolem's first proof of Löwenheim's theorem. A more elementary proof of part (a) actually is contained in Skolem's second proof. It may be outlined thus.

The free algebra $\underline{F}$ can be built up by levels: $L_0 = \{o_1, \ldots, o_n\}$, L_{k+1} is obtained by adding to L_k the elements $fx \ldots y$ whereby $x, \ldots, y \in L_k$ and f is one of $f_1, \ldots, f_m$. Let Σ be a sentence. Its Skolem-transform Σ^* is a universal sentence, say $(\forall x \ldots y)\, A(x, \ldots, y)$. For any k we define Σ_k to be the conjunction of all $A(u, \ldots, v)$ whereby $u, \ldots, v$ range over L_k. By a quite elementary argument one shows,

(c) If Σ is satisfiable, then for every k, Σ_k is satisfiable in L_k.

Furthermore, by König's infinity lemma,

(d) If for every k, Σ_k is satisfiable in L_k, then Σ^* is satisfiable in $\underline{F}$.

Because the "if-part" is trivial, this yields another proof of (a). It makes use of the infinity lemma, while the first proof uses the axiom of choice! We have not analyzed whether (b) also can be obtained in this second way.

Syntactic version of the Entscheidungsproblem: If in the statement of problem $[X]$ one replaces "satisfiable" by "formally consistent" one obtains the syntactic version $[X]_0$. By GÖDEL's completeness theorem it follows that $[X]$ and $[X]_0$ are equivalent, so that also $[\exists \wedge \forall\exists\forall]_0$ is not recursively solvable. However, one can prove this more directly by using HERBRAND's theorem. It can be stated thus,

(c′) Σ is formally consistent, if and only if, for any k, Σ_k is satisfiable in L_k.

Now (c′) and the infinity lemma (d) yield,

(a′) Σ is formally consistent, if and only if, Σ^* is satisfiable in $\underline{F}$.

From lemmas 1, 2, and (a′) the unsolvability of $[\exists \wedge \forall\exists\forall]_0$ follows.

Reduction: To the one who does not accept CHURCH's thesis, theorem 1 is of less interest. But our method also yields that $\exists \wedge \forall\exists\forall$ is a reduction-type, i.e., the problem $[Q]$ is effectively reducible (in fact $1-1$-reducible) to the problem $[\exists \wedge \forall\exists\forall]$. This can be seen by using a theorem of MYHILL's, because our proof clearly shows that $[\exists \wedge \forall\exists\forall]$ is of unsolvability degree 1. More directly one can obtain a reduction from $[Q]$ to $[\exists \wedge \forall\exists\forall]$ as follows.

To the sentence Σ in Q construct a Turing-machine M which, if started on the empty tape, begins by checking Σ_0 for satisfiability in L_0. M halts if it finds Σ_k not to be satisfiable in L_k, and it proceeds to Σ_{k+1} in case it has found a model of Σ_k. Thus by (c),

$$\Sigma \text{ satisfiable} \cdot\equiv\cdot M \notin \text{Hlt}.$$

The construction of lemma 2 now yields a matrix $\underline{\underline{M}}(x, u, y)$, which by lemma 2 and 3 is such that,

$$M \notin \text{Hlt} \cdot\equiv\cdot \Delta \text{ satisfiable},$$

whereby Δ is the sentence $(\exists x)Zx \wedge (\forall x)(\exists u)(\forall y)\underline{\underline{M}}$. Thus, the effective construction $\Sigma \to \Delta$, reduces $[Q]$ to $[\exists \wedge \forall\exists\forall]$.

Prefix of length four: The unsolvability of $[\forall\exists\forall\forall]$ does not follow from theorem 1, but it can be proved by the same method. (However, to obtain the necessary modified version of lemma 2, the author had to make use of ternary predicate letters.) We note that all prenex-types with prefix of length 4 are now settled; all except $\forall\exists\forall\forall$ and those falling under $\exists \wedge \forall\exists\forall$ and SURANYI's (1959) $\forall\forall\exists \wedge \forall\forall\forall$, have a solvable decision problem. There remains the question whether $[\exists \wedge \forall\exists\forall]$ is unsolvable if one admits, besides monadic letters, only two (only one) binary predicate letters.

The prefix $\forall\exists\forall$: The really important outstanding question is to prove $[\forall\exists\forall]$ unsolvable. For the first time there now is hope of obtaining this result. All that is missing is the following stronger form of lemma 2,

Problem: To any Turing-machine M to construct a matrix $\underline{\underline{M}}(x, u, y)$, with individual variables x, u, y, monadic predicate letters, and binary predicate letters, such that $M \notin \text{Hlt}$ if and only if $(\forall xy)\,\underline{\underline{M}}(x, x', y)$ is satisfiable in the natural number system $\langle N, '\rangle$.

In our proof of lemma 2 we fell short of obtaining this stronger result, because, in describing the action of M on the empty tape we used special constraints on two axes, namely the tape-axis and the time-axis. It is important to realize that also in conditions of form $(\forall xy)\,\underline{\underline{M}}(x, x', y)$ one still has use of one axis, namely one can formulate special restraints on the diagonal! In September 61 the author explained this situation to HAO WANG. He now claims, in collaboration with A. S. KAHR and E. F. MOORE, to have found a construction $M \to \underline{\underline{M}}$ as required in the above problem. Thus, even $[\forall\exists\forall]$ seems to be unsolvable, and the unsolvability of $[\forall\exists \wedge \forall\forall\forall]$ follows by passing to Skolem-form. These results settle (up to detailed questions, like number of binary predicate-letters) the Entscheidungsproblem for all generalized prenex types (conjunctions of prenex sentences). It is easy to see that for every generalized prenex type X either one of the following four alternatives holds:

A_1: Every conjunct of X is of form $\exists^n \forall^m$

A_2: Every conjunct of X is of form $\exists^n \forall^2 \exists^m$

B_1: There is a conjunct of form $\ldots \forall \ldots \exists \ldots \forall \ldots$ in X.

B_2: There are conjuncts $\ldots \forall \ldots \exists \ldots$ and $\ldots \forall \ldots \forall \ldots \forall \ldots$ in X.

Thus, there are just two cases,

A: $[X]$ trivially reduces to $[\exists^n \forall^m]$ or $[\exists^n \forall^2 \exists^m]$

B: Either $[\forall \exists \forall]$ or $[\forall \exists \wedge \forall \forall \forall]$ trivially reduces to $[X]$.

It is well known (see ACKERMANN [1]) that $[\exists^n \forall^m]$ and $[\exists^n \forall^2 \exists^m]$ are solvable. Thus, in case A, $[X]$ is solvable, while in case B, depending on the result of KAHR, MOORE, and WANG, $[X]$ is unsolvable.

Let us say that a set X of sentences has property Φ, if every sentence of X which is satisfiable also is finitely satisfiable. In other words $\sim \Phi X$ means that X contains an "infinity-axiom". It is well known (see ACKERMANN [1]) that $\exists^n \forall^2 \exists^m$ and $\exists^n \forall^m$ both have property Φ, while $\forall \exists \forall$ and $\forall \exists \wedge \forall \forall \forall$ do not. The trivial reductions mentioned preserve property Φ, so that the cases A and B also divide those generalized prenex types X having property Φ from those which do not.

Matrices of special form: We will show now that if in theorem 1 one drops the remark concerning the number of binary predicate-letters, one can in turn add very strong restrictions on the form of the matrices in the $\exists \wedge \forall \exists \forall$-sentences. We note that monadic letters can be eliminated (replace Sv by Svv) without changing satisfiability of a sentence. In the following discussion $R, S, \ldots$ will stand for vectors of binary predicate-letters. By lemmas 1 and 2 the following is an undecidable problem,

(D) For any matrices $\underline{Z}[Roo]$ and $\underline{M}[Rxx, Rxx', Rxy; Rx'x, Rx'x', Rx'y; Ryx, Ryx', Ryy]$ to decide whether $\underline{Z}(o) \wedge (\forall xy)\, \underline{M}(x, y)$ is satisfiable in $\langle N, o, {}' \rangle$.

The following modifications of $\underline{M}$ do clearly not affect satisfiability of $\underline{Z}(o) \wedge (\forall xy)\, \underline{M}(x, y)$:

1. To $\underline{M}$ conjoin $Sxy \equiv Ryx$ and make the proper substitutions in $\underline{M}$ to obtain a new matrix of form $\underline{A}[Rxx, Rx'x, Rx'x', Rxy, Rx'y, Ryy] \wedge \wedge \underline{B}[Rxy, Ryx]$.

2. To $\underline{A} \wedge \underline{B}$ conjoin $Sxy \equiv Rx'y$ and make the proper substitutions in $\underline{A}$ to obtain a new matrix of form $\underline{A}[Rxx, Rxx', Rxy, Ryy] \wedge \underline{B}[Rxy, Ryx] \wedge \wedge \underline{C}[Rxy, Rx'y]$.

3. To $\underline{A} \wedge \underline{B} \wedge \underline{C}$ conjoin $[Rxy \equiv Syx] \wedge [Sx'y \equiv Rxy]$ and make the proper substitutions in A to obtain the new matrix of form $\underline{A}[Rxx, Rxy, Ryy] \wedge \wedge \underline{B}[Rxy, Ryx] \wedge \underline{C}[Rxy, Rx'y]$.

4. To $\underline{A} \wedge \underline{B} \wedge \underline{C}$ conjoin $[Sxx \equiv Rxx] \wedge [Sx'y \equiv Sxy]$ and in A substitute Syx for Rxx, and Sxy for Ryy to obtain a new matrix of form $\underline{W}[Rxx] \wedge \wedge \underline{B}[Rxy, Ryx] \wedge \underline{C}[Rxy, Rx'y]$.

It therefore follows that the following is still an undecidable problem, (D′) For any matrices $\underline{Z}[Roo]$, $\underline{W}[Rxx]$, $\underline{B}[Rxy, Ryx]$ and $\underline{C}[Rxy, Rx'y]$ to decide whether $\underline{Z}(o) \wedge (\forall x)\, \underline{W}(x) \wedge (\forall xy)\, \underline{B}(x, y) \wedge (\forall xy)\, \underline{C}(x, x', y)$ is satisfiable in $\langle N, o, {}' \rangle$.

By lemma 3 one now obtains,

Theorem 1′: *There is no recursive method for deciding satisfiability of sentences of form* $(\exists v)\, \underline{Z}[Rvv] \wedge (\forall x)\, \underline{W}[Rxx] \wedge (\forall xy)\, \underline{B}[Rxy, Ryx] \wedge \wedge (\forall x)(\exists u)(\forall y)\, \underline{C}[Rxy, Ruy]$, *whereby* R *is a vector of binary predicate letters.*

Depending on the mentioned result of Kahr, Moore, and Wang the initial condition $\underline{Z}[Roo]$ may be dropped without making (D) decidable. Correspondingly theorem 1′ remains true if "$(\exists v)\, \underline{Z}[Rvv]$" is dropped. The question, whether in addition the axial restraint $\underline{W}[Rxx]$ can be avoided, remains unanswered.

Domino problems: The reduction (D) to (D′) discussed in the previous section can be carried one step further by the following observation. Suppose that the predicates Rxy on N satisfy

$$(\forall xy)\, \underline{D}[Rxy, Ryx, Rx'y]\,. \tag{1}$$

Then clearly the predicates $Pxy \equiv Rxy$ and $Qxy \equiv Ryx$ satisfy

$$\begin{aligned}(\forall x)\,[Qxx \equiv Pxx] \wedge (\forall xy)_{x \geqq y}\, \underline{D}[Pxy, Qxy, Px'y] \wedge \\ \wedge (\forall xy)_{x \geqq y}\, \underline{D}[Qxy, Pxy, Qxy']\end{aligned} \tag{2}$$

Conversely, if Q and P satisfy (2) then the predicates R defined by $Rxy \equiv Pxy$, if $x \geqq y$ and $Rxy \equiv Qyx$, if $x \leqq y$ satisfy (1). Thus, (1) is satisfiable if and only if (2) is satisfiable. Note furthermore that the following formula uniquely defines the predicates $x \geqq y$ and $x > y$:

$$x \geqq x \cdot\!\wedge\!\cdot \sim [x > x] \cdot\!\wedge\!\cdot [x' > y] \equiv [x \geqq y] \cdot\!\wedge\!\cdot [x > y] \supset [x \geqq y]\,. \tag{3}$$

Thus, in case $\underline{D}[Rxy, Ryx, Rx'y]$ is of form $B[Rxy, Ryx] \wedge \underline{C}[Rxy, Rx'y]$ one obtains an (as to satisfiability) equivalent formula of form $\underline{W}[Rxx] \wedge \wedge \underline{U}[Rxy, Rx'y] \wedge \underline{V}[Rxy, Rxy']$, by conjoining (3) to (2). Consequently the problem (D′) reduces to the following,

(D″) For any matrices $\underline{Z}[Roo]$, $\underline{W}[Rxx]$, $\underline{U}[Rxy, Rx'y]$, $\underline{V}[Rxy, Rxy']$ to decide whether $\underline{Z}(o) \wedge (\forall x)\, \underline{W}(x) \wedge (\forall xy) \cdot \underline{U}(x, x', y) \wedge \underline{V}(x, y, y')$ is satisfiable in $\langle N, o, {}' \rangle$.

It therefore follows that also this problem is unsolvable, and by lemma 3,

Theorem 1″: *There is no recursive method for deciding satisfiability of sentences of form* $(\exists v)\, \underline{Z}[Rvv] \wedge (\forall x)\, \underline{W}[Rxx] \wedge (\forall x)(\exists u)(\forall y) \cdot \underline{U}[Ruy, Ruy] \wedge \wedge \underline{V}[Ryx, Ryu]$.

Depending on the result of Kahr, Moore and Wang the conjunct $(\exists v)\underline{Z}$ can be dropped. However, the question whether in this theorem both restraints $(\exists v)\, \underline{Z}(v)$ and $(\forall x)\, \underline{W}(x)$ may be dropped, is a challenging unsolved problem. It can be stated thus, *Problem* 1: Is there an effective method which applies to any $\langle \underline{S}, \underline{U}, \underline{V} \rangle$, $\underline{U}$ and $\underline{V}$ binary relations on the finite set $\underline{S}$, and decides whether or not there is a valuation $R: N \times N \to \underline{S}$ which satisfies the condition $(\forall xy) \cdot \underline{U}[Rxy, Rx'y] \wedge \wedge \underline{V}[Rxy, Rxy']$.

In a slightly different form this was first stated by WANG (1961), and called the domino problem. $\underline{U}$ and $\underline{V}$ may be interpreted as sets of bars of length one, whose ends are marked with colors from a finite set $\underline{S}$. The problem then takes the following rather appealing form: To decide whether the lattice $N \times N$ can be filled with bars from $\underline{U}$ along the x-direction and bars from $\underline{V}$ along the y-direction, such that the ends of all bars meeting at any lattice point carry the same color.

The domino problem 1 is distinguished from other decision-problems by the complete lack of "initial restraints". This seems to make it very hard to reduce to it any one of the standard unsolvable problems, which all contain initial conditions of one kind or another (empty or finite initial tapes, initial states, axioms = initial theorems). In contrast, such a reduction was possible in the case (D″), which is the domino problem 1 with initial restraints $\underline{Z}[Roo]$ and $W[Rxx]$ added. In fact, the claim of KAHR, MOORE and WANG is that the domino problem becomes unsolvable even in case only the axial-restraint $\underline{W}[Rxx]$ is added[4]).

Related to the domino problem is the following, also unanswered, question:

Problem 2: Is there a finite set $\underline{S}$ and binary relations $\underline{U}$ and $\underline{V}$ on $\underline{S}$ such that $(\forall xy)$. $\underline{U}[Rxy, Rx'y] \wedge \underline{V}[Rxy, Rxy']$ has a solution R, but none which is periodic?

By lemma III this is simply the question whether or not there still is an infinity-axiom of form $(\forall x)(\exists u)(\forall y)$. $\underline{U}[Rxy, Ruy] \wedge \underline{V}[Ryx, Ryu]$, i.e., whether the set $\forall\exists\forall_0$, consisting of all these sentences, has property Φ. As noted by WANG (1961), a negative answer to problem 2 would mean solvability of the domino problem 1. (This corresponds to the well known fact that ΦX implies solvability of $[X]$.) However, we rather expect problem 1 to be unsolvable (possibly not of maximal degree 1, which would explain the mentioned difficulties in setting up reductions of standard unsolvable problems).

An unsolved problem on Turing-machines: We will now present a very natural halting problem on Turing-machines. It came up in connection with $[\forall\exists\forall]$, but seems to be of interest in its own right.

(T_2) To find an effective method, which for every Turing-machine M decides whether or not, for all tapes I (finite and infinite) and all states B, M will eventually halt if started in state B on the tape I.

This problem also displays the feature of lack of initial restraints. STANLEY TENNENBAUM has shown to the author that (T_2) becomes unsolvable if either

[4]) While the present paper was in print the author was informed that the mentioned results of KARR, MOORE and WANG are to be published in the February issue of the Proc. Nat. Ac. of Sc. U.S.A. 1962.

one of the following initial restraints is added: 1. Distinguished initial state A, 2. Initially the tape is empty.

Bibliography

[1] ACKERMANN, W.: Solvable cases of the decision problem. North-Holland, Amsterdam 1954.

[2] BERNAYS, P.: Remarques sur les problème de la décision en logique élémentaire. Edition de centre nat. de la rech. scient. **13**, 39—44 (1958), Paris.

[3] CHURCH, A.: A note on the Entscheidungsproblem. J. Symbolic Logic **1**, 40—41, 101—102 (1936).

[4] SURANYI, J.: Reduktionstheorie des Entscheidungsproblems. Budapest 1959.

[5] TRACHTÉNBROT, B. A.: Névozmožnost′ algorifma dlá problemy razréšimosti na konéčnyh klassah. Doklady Akadémii Nauk SSSR, n. s., **70**, 569—572 (1950).

[6] TURING, A. M.: On computable numbers, with an application to the Entscheidungsproblem. Proc. London Math. Soc. ser. 2, **42**, 230—265 (1936—7); **43**, 544—546 (1937).

[7] WANG, H.: Proving theorems by pattern recognition II. Bell System Technical J. **40**, 1—41 (1961).

(Received November 30, 1961)