THE UNIVERSITY OF MICHIGAN

COLLEGE OF LITERATURE, SCIENCE, AND THE ARTS
Department of Philosophy

Technical Report

TURING-MACHINES AND THE ENTSCHEIDUNGSPROBLEM

J. Richard Büchi

ORA Project 03105.

under contract with:

DEPARTMENT OF THE NAVY
OFFICE OF NAVAL RESEARCH
CONTRACT NO. Nonr 1224(21)
WASHINGTON, D.C.

administered through:

OFFICE OF RESEARCH ADMINISTRATION

ANN ARBOR

December 1961

ENGN UMR 1101

Turing-Machines and the Entscheidungsproblem*

by J. Richard Büchi

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 $S_{\mathbf{\xi}}X$, yields a decision as to whether or not S is satisfiable.

Church (1936) showed that [Q] is recursively unsolvable. Shortly thereafter Turing (1936) 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 over-all 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

^{*}The results of this paper were announced in the Notices, Am. Math. Soc., 8 (1961), 354. The work was supported by a grant from the National Science Foundation and contracts with the Office of Naval Research and U. S. Army Signal Corps.

individual variables x,u,y, monadic predicate letters Z,...., and 3 binary predicate letters S, K, and H, such that M&Hlt if and only if $Zo_{\Lambda}(\forall xy)\underline{M}(x,x',y)$ is satisfiable in the natural number system $\langle N,o,' \rangle$.

<u>Lemma</u> 3: For any matrices $\underline{Z}(x)$ and $\underline{M}(x,u,y)$, the sentence $(\exists x)\underline{Z}(x)\wedge(\forall x)(\exists u)$ $(\forall y)\underline{M}(x,u,y)$ is satisfiable if and only if $\underline{Z}(\circ)\wedge(\forall xy)\underline{M}(x,x',y)$ 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 EAVEV, such that M&Hlt if and only if S is satisfiable. Therefore, by lemma 1,

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

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 just means describing the operation of a Turing-machine M on the empty tape in the form $\underline{C}(Q,S,K,o,',x,y)$, whereby Qy = state at time y, $Kxy \equiv \text{position x}$ is scanned at time y, Sxy = tape-symbol at position x and time y. M&Hlt then means that no Q, P and S exist such that for all places x and all times y, $\underline{C}(Q,S,o,',x,y)$. As the functions Q and S are finite-valued, they can be coded as vectors of monadic and binary predicates on natural numbers. It remains to invent some tricks to put the matrix $\underline{C}(o,',x,y)$ into the form $\underline{C}(o)\wedge\underline{M}(x,x',y)$, 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 (Ξu) and a constant c for (Ξx). It remains to establish that $\underline{Z}(c)_{\Lambda}(\forall xy)\underline{M}(x,fx,y)$ is satisfiable if and only if it is satisfiable by predicates in N and c=0, fx=x'.

Our proof has the further advantage of directly yielding unsolvability for the very simple type EAVEV of sentences. By passing to the Skolem-form of VEV, theorem 1 also yields unsolvability of [EAVEAVAV]. Compare this with Bernays' (1958) analysis of Turing's proof, and note that such results are usually obtained by reduction of [Q] [see Suranyi (1959)]. Another feature of our proof is that, with slight modifications, it yields an improved version of Trachtenbrot'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 EAVEV are considered.

Corollary: The set of EAVEV 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 of lemma 2 has the further property: McCyl if and only if $Zo_{\Lambda}(\forall xy)\underline{M}(x,x',y)$ is satisfiable in $\langle N,o,' \rangle$ by periodic predicates.

Lemma III: Add to lemma 3: The sentence $(\exists x)\underline{Z}(x)\Lambda(\forall x)(\exists u)(\forall y)\underline{M}(x,u,y)$ is satisfiable in a finite domain, if and only if $\underline{Z}(o)\Lambda(\forall xy)\underline{M}(x,x',y)$ is satisfiable

in $\langle N, 0, ' \rangle$ by periodic predicates.

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

Proof of lemmas 2 and II: A (Turing-) machine we define to be a system $M = \langle D, A, L, R, P, Q, S \rangle$ consisting of a finite set D of elements called states; an AED called the <u>initial state</u>; three binary predicates L[X,Y], R[X,Y], P[X,Y], called <u>commands</u> of <u>left-move</u>, <u>right-move</u>, and <u>print</u>; a binary function Q[X,Y] with values in D, called the <u>new-state-function</u>; and a function S[X,Y] with values in T,F, called the <u>print-function</u>. All these predicates and functions have arguments T and T and T and T are to be exclusive and complementary. The <u>tape-symbols</u> are T and T; a <u>tape</u> is a one-way infinite sequence of tape-symbols, i.e., a predicate T and T. The

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 t it is in state X and scans position u of the tape, which now carries the symbol Y, then,

if L[X,Y], it moves to scan position u-1;

if R[X,Y], it moves to scan position u+l;

if P[X,Y], it prints S[X,Y] in place of Y at position u.

In all cases it goes into the new state Q[X,Y]. Note that, if u=0 and the command is 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 <u>halts</u> at time t+1, and that the tape I is <u>accepted</u> by M; in symbols H1(M,I). The set Hlt consists of all

machines M which eventually halt if put to work on the empty tape.

Now suppose that M is put to work on the empty tape, and never comes to a halt (i.e., M#Hlt). Then the functions

Qx = state of M at time x

Syx = tape-symbol at time x and position y

 $Kyx \equiv at time x position y is scanned by M$

Lx = at time x the command is left-move

Rx = at time x the command is right-move

Px = at time x the command is print

are defined for all x and y in N, and satisfy the conjunction \underline{C} of the following conditions:

$$Q_{O} \equiv A \wedge \sim Sy_{O} \qquad \qquad Koo \wedge \sim Ky' \circ$$

$$Kyx \supset Q_{X'} \equiv Q[Qx,Syx] \qquad Lx \supset Kyx' \equiv Ky'x$$

$$Kyx \wedge L[Qx,Syx] \supset Lx \wedge \sim Px \wedge \sim Rx \qquad Px \supset Kyx' \equiv Kyx$$

$$Kyx \wedge P[Qx,Syx] \supset Px \wedge \sim Lx \wedge \sim Fx \qquad Rx \supset Ky'x' \equiv Kyx$$

$$Kyx \wedge R[Qx,Syx] \supset Rx \wedge \sim Lx \wedge \sim Px \qquad Rx \supset \sim Kox'$$

$$[\sim Kyx \wedge Px] \lor Lx \lor Rx \supset Ky' \equiv Syx \qquad \sim [Kox \wedge Lx]$$

$$Kyx \wedge Px \supset Syx' \equiv S[Qx,Syx]$$

Conversely, the existence of Q, S, K, L, R, and P, which satisfy $(\forall yx)\underline{C}$, implies that M will not come to a halt if started on the empty tape. Thus (1) MHHt $.\equiv$. $(\forall xy)\underline{C}$ is satisfiable in $<\mathbb{N}$, o, '>. Note that the states of a machine may be coded as vectors of truth-values, so that the function-letter Q simply stands for a vector $<\mathbb{Q}_1$, ..., $\mathbb{Q}_n>$ of predicate-letters (n depending on the number of states of M), and \underline{C} therefore is a matrix of quantification

- theory. With the construction M o 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 C do not affect the validity of (1).
- <u>l</u>. Introduce an additional binary predicate-letter H. On the right side of <u>C</u> 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 $Zo\wedge Zx'$ and replace $Qo = A \wedge Syo$ by $Zx \supset Qx = A \wedge Syx$, $Koo\wedge Hyo$ by $Zx \supset Kxx\wedge Hyx$, Kox' by $Zy \supset Kyx'$, and $Kxx\wedge Lx$ by $Zy \supset Kyx\wedge Lx$. The resulting formula is of form $Zo\wedge M(x,x',y)$. $M\to M$ is the construction required in lemma 2. The same construction also satisfies lemma II, as will now be shown.

The machine M, if started on the tape I, goes into a p-cycle at time \mathcal{X} , if at the later time (\mathcal{X} +p) it is faced with an identical situation, i.e., at times \mathcal{X} and (\mathcal{X} +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 $\text{Cy}_p(\text{M},\text{I})$, if at some time it goes into a p-cycle. (It may be shown that for some p, $\text{Cy}_p(\text{M},\text{I})$ 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 <u>periodic</u> with <u>phase</u> \mathcal{X} and <u>period</u> p>0, if U(x+p) = Ux for all $x \ge \mathcal{X}$. A relation Vxy on N is called <u>periodic</u> with <u>phase</u> \mathcal{X} and period p>0, if $V(x+p)y \equiv Vxy$ for all $x \ge \mathcal{X}$ and all y, and $Vx(y+p) \equiv Vxy$ for all $x \ge \mathcal{X}$ and all $y \ge \mathcal{X}$. (Note that the entire line $Vx\mathcal{X}$ has to repeat at $Vx(\mathcal{X}+p)$, and not just from $x=\mathcal{X}$ on!)

Suppose now that MECyl, that is, M goes into a p-cycle at time Y, 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 Y and period p. Furthermore, if d is the maximum of all positions scanned by M before time (X+p), then at no time t a position y>d will be scanned. It follows that Y0 and Y1, and because Y2 and M never scans beyond d, also Y2 and Y3. Thus, also Y4 and Y5 are periodic (with phase Y4, and period p). In other words, the implication from left to right of (2) is valid.

(2) MacCyl .=. (Vyx)C is satisfiable by periodic predicates in $\langle \mathbb{N}, \circ, \cdot \rangle$. In the other direction (2) is trivially valid because the only solution of $(\forall yx)C$ 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 $\underline{1}$ and $\underline{2}$ of \underline{C} to \underline{C} t

The <u>block</u> of length 2 is the tape given by Iy \equiv (y<2). It is clear that one can effectively set up a <u>coding function</u> cd(M) which maps one-to-one all machines onto all blocks. A set \underline{X} of blocks is called <u>recursive</u> if there are machines M₁ and M₂ such that for all blocks I,

A set \underline{Y} of machines is called <u>recursive</u> if the set $\operatorname{cd}(\underline{Y})$ 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 either only to print or only to move in each atomic act.
- 3. We might have added another command predicate $\underline{H}[X,Y]$, to obtain haltsituations in addition to "running off the tape." But these can be eliminated by adding an additional state B, such that $\underline{H}[X,Y]$ 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 $H1(M,I) \equiv H1(M',I)$, but M' never 1-cycles. Similarly, one can modify a machine M to M' such that $H1(M,I) \equiv Cy_1(M',I)$ and M' does not halt on any block I. Thus in the definition of recursive sets of blocks one may replace (a) by

It now is possible to combine M_1 and M_2 into one machine M which 1-cycles on $I \not\in \underline{X}$ and halts on $I \not\notin \underline{X}$. Thus, to every recursive set \underline{X} of blocks there is a machine M_0 such that for all blocks I,

(c)
$$I \notin \underline{X} \quad :\equiv \quad Cy_1(M_O, I)$$

$$I \notin \underline{X} \quad :\equiv \quad Hl(M_O, I)$$

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

Suppose that \underline{Y} is a recursive set of machines and separates the sets of machines for which H1(M,cdM) respectively $Cy_1(M,cdM)$, i.e.,

H1 (M,cdM)
$$\supset M \varepsilon \underline{Y}$$

$$Cy_1(M,cdM) \supset M \notin \underline{Y}.$$

By (c) there is a machine $M_{\rm O}^{\ \ \ }$, such that

$$M \in \underline{Y} \supset Cy_1(M_O, cdM)$$

$$M \notin \underline{Y} \supset Hl (M_o, cdM).$$

Now $M_0 \not\in \underline{Y}$ implies $Cy_1(M_0, cdM_0)$ implies $M_0 \not\in \underline{Y}$, and $M_0 \not\in \underline{Y}$ implies $H1(M_0, cdM_0)$ implies $M_0 \in \underline{Y}$. This is contradictory, and therefore

(d) The sets $\underline{A} = \{M; Hl(M,cdM)\}$ and $B = \{M; Cy_1(M,cdM)\}$ are not separable by a recursive set.

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

$$Cy_1(M,cdM) \supset fM \in Cyl_1$$

it follows from (d) that also Hlt and Cyl₁ are not separable. Finally, because $\text{Cyl}_1 \subseteq \text{Cyl}$, 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 \mathfrak{D}_1 , $R_1 >$. By the axiom of choice it follows that there is an $a_1 \in D_1$ and a function $f_1 \colon D_1 \rightarrow D_2$, 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 a_2 , it follows that there is a homomorphism a_1 from a_2 , a_3 , a_4 , a_4 , a_5 . If we now define a_4 is a homomorphism a_4 is clear that a_4 is homomorphic image of a_4 a_5 . Again because a_5 is universal it therefore follows that a_5 , a_5 , a_5 is still a model of a_5 is universal it therefore follows that a_5 , a_5 , a_5 is still a model of a_5 . Thus,

(1) Σ is satisfiable . \supset . Σ^* is satisfiable in <N,0,'>.

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

$$hx = hy = x = y (x = x / y \ge x / x = y \pmod{p})$$

for some % and p>0. It follows that the relation R_3xy is periodic with phase % and period p. Thus we have shown

(2) Σ finitely satisfiable . \Im . Σ^* periodically satisfiable in \Im , \circ , \hookrightarrow 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 $\underline{D} = \langle \mathbb{N}, 0, ', \mathbb{R}_1 \rangle$ is a model of Σ^* (a, f, R), whereby \mathbb{R}_1 is periodic, say of phase 2 and period p>0. The relation

$x \sim y$.\equiv $x = y \vee [x \ge x \wedge y \ge x \wedge x \equiv y \pmod{p}]$

is clearly a congruence relation of $\langle \mathbb{N}, o, ' \rangle$, and because R_1 has phase \mathcal{X} 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 Σ^* (a, f, R) one obtains a model of Σ (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 $\langle \mathbb{N}, 0, ' \rangle$ appear the totally free algebras $\underline{F}_n^m 1, \cdots, m = \langle \mathbb{N}, 0_1, \ldots, 0_n, f_1, \ldots, f_k \rangle$ 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 $\Sigma^*(o_1, \ldots, o_n, f_1, \ldots, f_k, \mathbb{R})$ of an arbitrary sentence $\Sigma(\mathbb{R})$ 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-known manner (suggested by the axiom of choice). The general form of lemma III now is

<u>Lemma III</u>: 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,..., m_k .

(b) Σ is satisfiable in a finite domain if and only if Σ^* is satisfiable in \underline{F}_n 1,..., \underline{m} k by periodic relations.

The proof we gave (using the axiom of choice) simply carries one step further 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: $L_0 = \{o_1, \dots, o_n\}$, L_{k+1} is obtained by adding to L_k the elements fx...y whereby $x,...,y \in L_k$ and f is one of $f_1,...,f_m$. Let Σ be a sentence. Its Skolem-transform Σ^* is a universal sentence, say $(\forall x...y)\underline{A}(x,...,y)$. For any k we define Σ_k to be the conjunction of all $\underline{A}(u,...,v)$ whereby u,...,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 a new 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 syntatic version [X] $_{\text{O}}$. By Gödel's completeness theorem it follows that [X] and [X] $_{\text{O}}$ are equivalent, so that also $[\underline{\text{EAVEV}}]_{\text{O}}$ 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

proof clearly shows that [ENVEY] is of unsolvability degree 1. More directly

one can obtain a reduction from [Q] to [HAVHY] 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),

 Σ satisfiable .=. M \notin Hlt

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

M \notin Hlt .≡. \triangle satisfiable,

Prefix of length four: The unsolvability of [VVIV] 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 VEVV and those falling under EAVEV and Suranyi's (1959) VVEAVVV have a solvable decision problem. There remains the question whether [HAVEV] is unsolvable if one admits, besides monadic letters, only two (only one) binary predicate letters.

The prefix <u>VEV</u>: The really important outstanding question is to prove [VEV] 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.

<u>Problem:</u> To any Turing-machine M to construct a matrix $\underline{M}(x,u,y)$, with individual variables x,u,y, monadic predicate letters, and binary predicate letters, such that M \not Hlt if and only if $(\forall xy)\underline{M}(x,x',y)$ is satisfiable in the natural number system $\langle \mathbb{N}, ' \rangle$.

every generalized prenex type X either one of the following four alternatives holds:

 A_1 : Every conjunct of X is of form $\Xi^n V^m$

 A_2 : Every conjunct of X is of form $\exists V^2 \exists M$

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

B2: There are conjuncts ... \forall ...

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 [$\forall \exists \land \forall \forall \forall$] trivially reduces to [X].

It is well known (see Ackermann, 1954) that $[\exists^n V^m]$ and $[\exists^n V^m]$ 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, 1954) that $\Xi^{n}_{V} \Xi^{m}$ and $\Xi^{n}_{V} \Psi^{m}$ both have property Φ , while VEV and VEAVVV 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 EAVEV 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, ...

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 < N, o, '>.

 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 $A[Rxx, Rx'x, Rx'x', Rxy, Rx'y, Ryy] \land \underline{B}[Rxy, Ryx]$.
- 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

A[Rxx, Rxx', Rxy, Ryy] \land B[Rxy, Ryx] \land C[Rxy, Rx'y].

- $\underline{3}$. To $\underline{A} \wedge \underline{B} \wedge \underline{C}$ conjoin $[Rxy \equiv Syx] \wedge [Sx'y \equiv Txy]$ and make the proper substitutions in \underline{A} to obtain the new matrix of form $\underline{A}[Rxx, Rxy, Ryy] \wedge \underline{B}[Rxy, Ryx] \wedge \underline{C}[Rxy, Rx'y]$.
- $\underline{\underline{4}}$. To $\underline{\underline{A}}_{\Lambda} \underline{\underline{B}}_{\Lambda} \underline{\underline{C}}$ conjoin $[Sxx \equiv Rxx]_{\Lambda} [Sx'y \equiv Sxy]$ and in $\underline{\underline{A}}$ substitute Syx for Rxx, and Sxy for Ryy to obtain a new matrix of form $\underline{\underline{W}}[Rxx]_{\Lambda} \underline{\underline{B}}[Rxy, Ryx]_{\Lambda} \underline{\underline{C}}[Rxy, Rx'y]$.

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 <u>l'</u>: There is no recursive method for deciding satisfiability of sentences of form $(\exists v)\underline{Z}[Rvv]\wedge(\forall x)\underline{W}[Rxx]\wedge(\forall xy)\underline{B}[Rxy, Ryx]\wedge(\forall x)(\exists u)(\forall y)\underline{C}[Rxy, Ruy],$ 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 " $(\underline{T}v)\underline{Z}[Rvv]$ " 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

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

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

- (2) $(\forall x)[Qxx \equiv Pxx] \land (\forall xy)_{x \geq y} \underline{D}[Pxy, Qxy, Px'y] \land (\forall xy)_{x > y} \underline{D}[Qxy, Pxy, Qxy']$ Conversely, if Q and P satisfy (2) then the predicates R defined by Rxy $\equiv Pxy$, if $x \geq y$ and $Rxy \equiv Qyx$, if $x \leq y$ satisfy (1). Thus, (1) is satisfiable if and only if (2) is satisfiable. Note furthermore that the following formula uniquely defines the predicates $x \geq y$ and x > y:
- $(3) \qquad \qquad x \ge x \wedge [x > x] \wedge [x' > y] \equiv [x \ge y] \wedge [x > y] \supset [x \ge y]$

Thus, in case $\underline{D}[Rxy, Ryx, Rx'y]$ is of form $\underline{B}[Rxy, Ryx] \wedge \underline{C}[Rxy, Rx'y]$ one obtains an (as to satisfiability) equivalent formula of form $\underline{W}[Rxx] \wedge \underline{U}[Rxy, Rx'y] \wedge \underline{V}[Rxy, Rxy']$, 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 $\underline{Z}(o) \wedge (\forall x) \underline{W}(x) \wedge (\forall xy)$. $\underline{U}(x,x',y) \wedge \underline{V}(x,y,y')$ is satisfiable in $< \mathbb{N}, o, '>$. It therefore follows that also this problem is unsolvable, and by lemma 3, \underline{T} , there is no recursive method for deciding satisfiability of sentences of form $(\exists v)\underline{Z}[Rvv] \wedge (\forall x)\underline{W}[Rxx] \wedge (\forall x)(\exists u)(\forall y)$. $\underline{U}[Rxy, Ruy] \wedge \underline{V}[Ryx, Ryu]$.

Depending on the result of Kahr, Moore and Wang the conjunct \underline{Z} can be dropped. However, the question whether in this theorem both restraints on $(\underline{\exists v})\underline{Z}(v)$ and $(\underline{\forall x})\underline{W}(x)$ 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: $\mathbb{N} \times \mathbb{N} \times \underline{S}$ which satisfies the condition $(\mathbb{V} \times \mathbb{V})$. $\underline{U}[\mathbb{R} \times \mathbb{V}, \mathbb{R} \times \mathbb{V}] \wedge \underline{V}[\mathbb{R} \times \mathbb{V}, \mathbb{R} \times \mathbb{V}]$. 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 $\mathbb{N} \times \mathbb{N}$ 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 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 W[Rxx] is added.

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 $(\forall xy)$. $\underline{U}[Rxy, Rx'y]_{\Lambda} \underline{V}[Rxy, Rxy']$ 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 $(\forall x)(\exists u)(\forall y)$. $\underline{U}[Rxy, Ruy] \land \underline{V}[Ryx, Ryu]$, i.e., whether the set $\forall \exists V_0$, 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 [VEV], 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 one of the following initial restraints is added: \underline{l} . Distinguished initial state A, 2. Initially the tape is empty.

References

- A. Church, "A note on the Entscheidungsproblem," <u>Journal of Symbolic Logic</u>, <u>1</u> (1936), 40-41, 101-102.
- A M. Turing, "On computable numbers, with an application to the Entscheidungs-problem," Proc. London Math. Soc., ser. 2, 42 (1936-37), 230-265; 43 (1937), 544-546.
- J. Suranyi, Reduktionstheorie des Entscheidungsproblems, Budapest, 1959.
- W. Ackermann, Solvable cases of the decision problem, North-Holland, Amsterdam, 1954.
- B. A. Trachténbrot, "Névozmožnost' algorifma dlá problemy razrešimosti na konéčnyh klassah," Doklady Akadémii Nauk SSSR, n.s., 70 (1950), 569-572.
- P. Bernays, "Remarques sur les probleme de la décision en logique élémentaire," Edition de centre nat. de la rech. scient., 13 (1958), Paris, 39-44.
- H. Wang, "Proving theorems by pattern recognition II," <u>Bell System Technical</u>
 <u>Journal</u>, <u>40</u> (1961), 1-41.

DISTRIBUTION LIST

2

2

6

(One copy unless otherwise noted)

Asst. Sec. of Def. for Res. and Eng. Information Office Library Br. Pentagon Building Washington 25, D. C.

Armed Services Tech. Infor. Agcy. 10 Arlington Hall Station Arlington 12, Virginia

Chief of Naval Research
Department of the Navy
Washington 25, D.C.
Attn: Code 437, Inf. Syst. Br.

Chief of Naval Operations OP-07T-12 Navy Department Washington 25, D.C.

Director, Naval Res. Lab. Tech. Inf. Officer/Code 2000 Washington 25, D.C.

Commanding Officer, Officer of 10
Naval Research
Navy. No. 100, Fleet P. 0.
New York, New York

Commanding Officer, ONR Br. Office 346 Broadway
New York 13, New York

Commanding Officer, ONR Br. Office 495 Summer St. Boston 10, Massachusetts

Office of Technical Services Technical Reports Section Department of Commerce Washington 25, D.C. Bureau of Ships
Department of the Navy
Washington 25, D.C.
Attn: Code 671 NTDS

Bureau of Naval Weapons
Department of the Navy
Washington 25, D.C.
Attn: RAAV Avionics Division

Bureau of Ships
Department of the Navy
Washington 25, D.C.
Attn: Communications Br. Code 686

Naval Ordnance Laboratory White Oaks Silver Spring 19, Maryland Attn: Technical Library

David Taylor Model Basin Washington 7, D.C. Attn: Technical Library

Naval Electronics Laboratory San Diego 52, California Attn: Technical Library

University of Illinois Control Systems Laboratory Urbana, Illinois Attn: D. Alpert

University of Illinois Digital Computer Laboratory Urbana, Illinois Attn: Dr. J. E. Robertson

National Security Agency Fort Geo. G. Meade, Maryland Attn: Howard Campaigne 3

Technical Information Officer
US Army Signal Research and Dev. Lab.
Fort Monmouth, New Jersey
Attn: Data Equipment Branch

U. S. Naval Weapons Laboratory
Dahlgren, Virginia
Attn: Head, Compution Div.,
G. H. Gleissner

National Bureau of Standards Washington 25, D.C. Attn: Dr. S. N. Alexander

Aberdeen Proving Ground, BRL
Aberdeen Proving Ground, Maryland
Attn: J. H. Giese, Chief Compution Lab.

Office of Naval Research Resident Representative University of Michigan 146-B Temporary Classroom Bldg. Ann Arbor, Michigan

Commanding Officer
ONR, Branch Office
John Crerar Library Bldg.
86 East Randolph St.
Chicago 1, Illinois

Commanding Officer
ONR, Branch Office
1030 E. Green Street
Pasadena, California

Commanding Officer
ONR, Branch Office
1000 Geary Street
San Francisco 9, California

National Bureau of Standards Washington 25, D.C. Attn: Mr. R. D. Elbourn

Naval Ordnance Laboratory Corona, California Attn: H. H. Weider Massachusetts Inst. of Technology Cambridge, Massachusetts Attn: D. W. Baumann Dynamic Analysis and Control Lab.

Burroughs Corporation Research Center Paoli, Pennsylvania Attn: R. A. Tracey

Hermes Incorporated 75 Cambridge Parkway Cambridge 42, Massachusetts Attn: Mr. Reuben Wasserman

Lockheed Missiles and Space Div. 3251 Hanover Street
Palo Alto, California
Attn D. G. Willis

University of Michigan
Ann Arbor, Michigan
Attn: Dept. of Philosophy,
Prof. A. W. Burks

Census Bureau
Washington 25, D.C.
Attn: Office of Asst. Director for
Statistical Services, Mr. J. L.
McPherson

National Science Foundation Program Dir. for Documentation Res. Washington 25, D.C. Attn: Helen L. Brownson

University of California
Los Angeles 24, California
Attn: Dept. of Eng.,
Prof. Gerald Estrin

Columbia University
New York 27, New York
Attn: Dept. of Physics,
Prof. L. Brillouin

Hebrew University
Jerusalem, Israel
Attn: Prof. Y. Bar-Hillel

Massachusetts Inst. of Tech. Cambridge, Massachusetts
Attn: Prof. W. McCulloch

Atomic Energy Commission
Washington 25, D.C.
Attn: Div. of Research, John R. Pasta

Naval Research Laboratory Washington 25, D.C. Attn: Security Systems Code 5266, Mr. G. Abraham

Cornell University
Dept. of Mathematics
Ithaca, New York
Attn: Prof. Mark Kac

Dr. A. M. Uttley National Physical Laboratory Teddington, Middlesex England

Diamond Ordnance Fuze Laboratory Connecticut Ave. and Van Ness St. Washington 25, D.C. ORDTL-012, E. W. Channel

U.S. Army Signal Res. and Dev. Lab. Fort Monmouth, New Jersey Attn: M. Tenzer

Harvard University Cambridge, Massachusetts Attn: School of Applied Science Dean Harvey Brook

The University of Chicago
Institute for Computer Research
Chicago 37, Illinois
Attn: Mr. Nicholas C. Metropolis, Dir.

Wright Air Development Division Electronic Technology Laboratory Wright Patterson Air Force Base, Ohio Attn: WWRNEB Computer and Bionics Br.

Laboratory for Electronics, Inc. 1079 Commonwealth Ave. Boston 15, Massachusetts Attn: Dr. H. Fuller

Stanford Research Institute Computer Laboratory Menlo Park, California Attn: H. D. Crane

General Electric Company Schnectady 5, New York Attn: Library, L.M.E. Dept., Bldg. 28-501

The Rand Corporation 1700 Main Street Santa Monica, California Attn: Numerical Analysis Dept. Willis H. Ware

Hunter College
New York 21, New York
Attn: Dean Mina Rees.

General Electric Research Laboratory
P. O. Box 1088
Schenectady, New York
Attn: Information Studies Section
R. L. Shuey, Manager

Radio Corporation of America Moorestown, New Jersey Attn: Missile and Surface Radar Div. Sidney, Caplan

University of Pennsylvania Institute of Cooperative Research Philadelphia, Pennsylvania Attn: Dr. John O'Conner Stanford Research Institute Menlo Park, California Attn: Dr. Charles Rosen Applied Physics Group

Northeastern University 360 Huntington Avenue Boston, Massachusetts Attn: Prof. L. O. Dolansky

Marquardt Aircraft Company 16555 Saticoy Street P. O. Box 2013 - South Annex Van Nuys, California Attn: Dr. Basun Chang, Res. Sci.

Texas Technological College Lubbock, Texas Attn: Paul G. Griffith Dept. of Electrical Engineering

IBM Corporation
Military Products Division
Owego, New York
Attn: Dr. S. Winkler

Post Office Department
Office of Res. and Eng.
12th and Pennsylvania Avenue
Washington 25, D. C.
Attn: Mr. R. Kopp, Res. and Devel. Div.

Air Force Research Division, ARDC Computer and Mathemathical Sci. Lab., ARCRC L. G. Hanscom Field, CRBB, Bedford, Mass. Attn: Dr. H. H. Zschirnt

Office of Chief Signal Officer Department of the Army Washington D.C. Attn: R and D. Div. SIGRO-6D Mr L. H. Geiger

Bell Telephone Laboratories Murray Hill Laboratory Murray Hill, New Jersey Attn: Dr. Edward F. Moore National Biomedical Res. Found. Inc. 8600 16th St., Suite 310 Silver Spring, Maryland Attn: Dr. R. S. Ledley

National Bureau of Standards Washington 25, D. C. Attn: Mrs. Frances Neeland

University of Pennsylvania Moore School of Elec. Eng. 200 South 33rd Street Philadelphia 4, Pennsylvania Attn: Miss Anna Louise Campion

Varo Manufacturing Company 2201 Walnut Street Garland, Texas Attn: Fred P. Granger, Jr.

Data Processing Systems Staff
Department of State
Washington 25, D.C.
Attn: F. P. Diblasi

Dr. Saul Gorn, Director Computer Center University of Pennsylvania Philadelphia 4, Pennsylvania

Applied Physics Laboratory Johns Hopkins University 8621 Georgia Avenue Silver Spring, Maryland Attn: Supervisor of Tech. Rpts.

Chief, Bureau of Supplies and Accounts, Navy Department Washington, D.C. Attn: CDR. J. C. Busby, Code W3

Auerbach Electronics Corporation 1634 Arch St. Philadelphia 3, Pennsylvania National Aeronautics and Space Administration Goddard Space Flight Center Greenbelt, Maryland Attn: Chief, Data Systems, Div. C.V.L. Smith

Federal Aviation Agency Bureau of Research and Development' Washington 25, D.C. Attn: RD-375, Mr. Harry Hayman

Mr. Donald F. Wilson Code 5144 Naval Research Laboratory Washington 25, D. C.

David Taylor Model Basin Washington 7, D.C. Attn: Aerodynamics Laboratory, Code 628, Miss Cravens Lincoln Laboratory
Massachusetts Institute of Technology
Lexington 73, Massachusetts
Attn: Library

Dr. C. R. Porter Psychology Department Howard University Washington 1, D. C.

Electronics Research Laboratory University of California Berkeley 4, California Attn: Director

Institute for Defense Analysis Communications Research Division Von Neumann Hall Princeton, New Jersey 3 9015 02651 5034