# G. M. KORPELEVICH

MATHEMATICS

1963

SovietRxiv

## Abstract

## Full Text


# G. M. KORPELEVICH


## ON THE RELATION BETWEEN THE NOTIONS OF DECIDABILITY AND ENUMERABILITY FOR FINITE AUTOMATA


*(Presented by Academician P. S. Novikov, 29 X 1962)*

**MATHEMATICS**


1. In the theory of algorithms, the notions of an **enumerable** set and a **decidable** set ([1]) amount essentially to the following. A set is decidable if there exists an algorithm (which may be conceived as a machine with memory finite at every moment, but potentially unbounded) deciding this set, i.e. recognizing whether or not an object belongs to the given set. A set is enumerable if there exists an algorithm enumerating the given set, i.e. a machine producing the elements of the given set at the "output." In automata theory analogous notions are considered, but they are based not on the notion of an algorithm, but on the notion of a finite automaton, i.e. a machine with memory bounded in advance: the notions of a **finite-decidable** and **finite-enumerable** set.

In algorithmic theory all decidable sets are enumerable, but not all enumerable sets are decidable ([1]). In automata theory a crude analogue of this theorem turns out to be false, namely: it has been proved ([2]) that the class of finite-enumerable sets coincides with the class of finite-decidable sets. However, a subtler analogue turns out to be true (communicated to the author as a hypothesis by V. A. Uspenskii), namely: there exist finite-enumerable sets for whose decision automata with a "much larger" number of states are required than for their enumeration (the precise meaning of the expression "much larger" will be clarified below). This result constitutes the main content of the present note.

2. Let $\Sigma$ be a finite alphabet, and let $T$ be the free semigroup generated by it.

An automaton, according to ([2]), is a system

$$A = \langle S, M, s_0, F, O \rangle,$$

consisting of a finite set $S$, the "set of internal states," one of which $s_0$ is chosen as "initial" ; a subset $F \subseteq S$, the set of "marked" states; a "transition" function $M = M(s, \sigma)$, carrying out a mapping of $S \times \Sigma$ into $S$; and a "marking" function $O = O(s)$, carrying out a mapping of $S$ into $T$.

The function $M(s, \sigma)$ is naturally extended to all words of $T$, namely: if $x \in T$,

$x = \sigma_1\sigma_2 \ldots \sigma_n$, then

$$M(s, x) = s_1 s_2 \ldots s_n,$$

where

$$s_1 = M(s, \sigma_1), \quad s_2 = M(s_1, \sigma_2), \ldots, \quad s_n = M(s_{n-1}, \sigma_n)$$

($s_n$ will henceforth be denoted by $sx$); if $x = \Lambda$ ($\Lambda$ is the empty word), then $M(s, x) = s$. For those words $x$ under whose action the "automaton arrives" in one of the marked states, i.e. for which $s_0 x \in F$, we define the "output" word

$$A(x) = O(s_1)O(s_2) \ldots O(s_n).$$

If, however, $x$ is such that $s_0 x \notin F$, we shall regard the output as undefined. Of an automaton defined in this way we shall say that it decides the set

$$V_A = \{x : s_0 x \in F,\ x \in T\}$$

and enumerates the set

$$W_A = A(V_A) = \{y : y = A(x),\ x, y \in T\},$$

i.e. the set of all outputs.

A set is called **finite-decidable** (**finite-enumerable**) if there exists an automaton deciding (enumerating) the given set.

3. Among all automata that decide the set $V$, there exists at least one with the smallest number of states. The number of states of such an automaton will be called the deciding complexity of the set $V$ and denoted by $D(V)$.

For an arbitrary alphabet $\Sigma$ (containing at least two letters) the following holds.

**Theorem.** *Every set enumerable by an automaton with $r$ states has deciding complexity not exceeding $2^r$. However, whatever natural number $r \geqslant 4$ is taken, there exists a set $V$, enumerable by an automaton with number of states $\leqslant r$, whose deciding complexity satisfies*

$$D(V) \geqslant 2^{[r/2]}.$$

4. **Outline of the proof.** In the first part of the proof, conditions are derived on an automaton $A$ which are sufficient for the set $W_A$, enumerable by this automaton, to have deciding complexity

$$D(W_A) \geqslant 2^{[r/2]};$$

here $r$ is the number of states of the automaton $A$.

Let $A = \langle S, M, s_0, F, O \rangle$ be an automaton with $r$ states. Consider the equivalence relation ([3]) generated by the set $W_A$, namely: for $x, y \in T$ we shall say that $x$ and $y$ are $W_A$-equivalent (and denote this by $x \overset{W_A}{\sim} y$) if and only if, for any $z \in T$, the words $xz$ and $yz$ simultaneously either belong or do not belong to the set $W_A$. The partition of the set $T$ induced by the relation of $W_A$-equivalence will be called the $W_A$-partition. As follows from the proof of Nerode' s theorem ([3]), the deciding complexity of the set $W_A$ is equal to the number of classes in the $W_A$-partition.

Introduce one more equivalence relation: for $x, y \in T$, denote

$$\mathbf{A}^{-1}(x) = \{y : \mathbf{A}(y) = x\}$$

and

$$P(x) = \{s,\ s = s_0 y,\ y \in \mathbf{A}^{-1}(x)\}.$$

We shall say that $x$ and $y$ are $P$-equivalent ($x \overset{P}{\sim} y$) if and only if

$$P(x) = P(y).$$

It is easy to prove that if $x \overset{P}{\sim} y$, then $x \overset{W_A}{\sim} y$, and consequently the partition induced by $P$-equivalence (the $P$-partition) is a refinement of the $W_A$-partition. And since the number of equivalence classes in the $P$-partition is no more than $2^r$, it follows that $D(W_A) \leqslant 2^r$ (thereby the first part of the theorem is proved).

Suppose now that the automaton $A$ is such that:

1) $F = S$;
2) the range of the function $O(s)$ is $\Sigma$ (and not $T$, as in the general case);
3) there exists a set $S_1 \subseteq S$ all of whose subsets are "reachable," i.e., if $E \subseteq S_1$, then there exists a word $x$ such that $E = P(x)$.

In this case, to each subset $E \subseteq S_1$ one can naturally put in one-to-one correspondence a nonempty equivalence class of the $P$-partition in the domain

$$Q = \{x : \ P(x) \subseteq S_1\}.$$

(Here we shall assume that $W_A \neq T$, and the set $\{x : \ P(x) = \Lambda\}$ will be put in correspondence with the empty subset of states.) Then the domain $Q$ contains $2^{r_1}$ equivalence classes of the $P$-partition, where $r_1$ is the number of elements in $S_1$. Under a certain condition it turns out that the $P$-partition and the $W_A$-partition coincide in the domain $Q$; therefore the number of equivalence classes of the $W_A$-partition in this domain is equal to $2^{r_1}$, and, consequently,

$$D(W_A) \leqslant 2^{r_1}.$$

This condition is the following:

4) all states of the set $S_1$ are "distinguishable," i.e., for each $s_i \in S_1$ there exist words $x_i$ and $y_i$ such that, first, $M(s_i, x_i) = y_i$ and, second,

$$M(s, x) \neq y_i$$

for all $x \in T$, provided only that $s \neq s_i$.

In the second part of the proof, for an arbitrary natural number $r \geqslant 4$, an automaton satisfying conditions 1)–4) with $r_1 = [r/2]$ is constructed. This automaton is defined for even $r = 2\rho$ as follows: as ⋯

alphabet $\Sigma$ is taken to be the set $\{0, 1\}$; $S$ is a set of $r$ elements; $F = S$, and $s_1$ is the initial state.

We define the transition function by the following table (for brevity, instead of $s_i$ we shall write only the index $i$):

| $i$ | 0 | 1 |
|---|---|---|
| 1 | 1 | $\rho+1$ |
| 2 | 3 | $\rho+2$ |
| … | … | … |
| $k$ | $k+1$ | $k+\rho$ |
| … | … | … |
| $\rho$ | $2\rho$ | $2\rho$ |
| $\rho+1$ | 2 | $2\rho$ |
| $\rho+2$ | 3 | 3 |
| … | … | … |
| $\rho+l$ | $l+1$ | $l+1$ |
| … | … | … |
| $2\rho$ | 1 | 2 |

where $2 \leq k, l < \rho$.

Here the element of the table $a_{ij} = M(i, j)$, $1 \leq i \leq 2\rho$, $j = 1, 0$. The marking function is $O(s_i) = 0$ if $1 \leq i \leq \rho$; $O(s_i) = 1$ for $\rho < i \leq 2\rho$. For the particular case $r = 8$, the transition diagram of such an automaton has the form:

Transition diagram for $r = 8$:

- $1 \xrightarrow{0} 1$, $1 \xrightarrow{1} 5$;
- $5 \xrightarrow{0} 2$, $5 \xrightarrow{1} 8$;
- $8 \xrightarrow{0} 1$, $8 \xrightarrow{1} 2$;
- $2 \xrightarrow{1} 6$, $2 \xrightarrow{0} 3$;
- $6 \xrightarrow{1,0} 3$;
- $3 \xrightarrow{1} 7$, $3 \xrightarrow{0} 4$;
- $7 \xrightarrow{1,0} 4$;
- $4 \xrightarrow{1,0} 8$.

Moscow State University
named after M. V. Lomonosov

Received
26 X 1962

## REFERENCES

[1] E. L. Post, Bull. Am. Math. Soc., **50**, No. 5, 284 (1944).
[2] V. A. Kozmidiadi, DAN, **142**, No. 5, 1005 (1962).
[3] T. Robin, D. Scott, Intern. Business Mach., J. Res. and Development, **3**, No. 2, 114 (1959).

*Note: Figure translations are in progress. See original paper for figures.*