ESTIMATES OF THE NUMBER OF STATES OF FINITE AUTOMATA

MATHEMATICS

1970

SovietRxiv

Abstract

Full Text

UDC 519.95

MATHEMATICS

A. N. MASLOV

ESTIMATES OF THE NUMBER OF STATES OF FINITE AUTOMATA

(Presented by Academician A. N. Kolmogorov on 27 III 1970)

In the present paper we consider operations on sets of words representable in finite automata. An important characteristic of the complexity of these sets is the number of states of the minimal representing automaton.

Kleene proved (^{1,2}) that a set of words is representable in a finite automaton if and only if it is obtained from $\{\Lambda\}$ and $\{\sigma_i\}$ (where Λ is the empty word, and σ_i are letters of the input alphabet Σ) by applying the operations of union ($\cup$), product ($\cdot$), and iteration ($*$).

Further, $S_i x = S_k$ means that, upon receiving the word x as input, an automaton in state S_i passes into state S_k; the index 0 corresponds to the initial state, unless otherwise stipulated; $[x^\circ]$ denotes the length of the word x; $T(A)$ denotes the set of words representable in the automaton A. In what follows, by representability of events we shall always mean representability in a finite automaton.

It is known that if $T(A)$ and $T(B)$ are representable in automata A and B with m and n states, respectively ($m \geq 1,\ n \geq 1$), then

1) $T(A) \cup T(B)$ is representable in an automaton with $m \cdot n$ states,
2) $T(A) \cdot T(B)$ is representable in an automaton with $(m-1) \cdot 2^n + 2^{n-1}$ states ($n \geq 3$),
3) $T(A)^*$ is representable in an automaton with $\frac{3}{4} \cdot 2^m - 1$ states ($m \geq 2$).

We have constructed examples of automata over the alphabet $\Sigma = \{0, 1\}$ on which these estimates are attained.

1. **Union:** A has states $\{S_0, \dots, S_{m-1}\}$ and transitions $S_{m-1}1 = S_0,\ S_i 1 = S_{i+1}$ for $i \neq m-1,\ S_i 0 = S_i,\ S_{m-1}$ is the final state; B has states $\{P_0, \dots, P_{n-1}\}$ and transitions $P_i 1 = P_i,\ P_{n-1}0 = P_0,\ P_i 0 = P_{i+1}$ for $i \neq n-1,\ P_{n-1}$ is the final state.
2. **Product:** B has states $\{P_0, \dots, P_{n-1}\}$ and transitions $P_{n-1}1 = P_{n-2},\ P_{n-2}1 = P_{n-1},\ P_i 1 = P_i$ for $i < n-2,\ P_{n-1}0 = P_{n-1},\ P_i 0 = P_{i+1}$ for $i \neq n-1,\ P_{n-1}$ is the final state; the automaton A is the same as for union.

3. **Iteration:** A has states $\{S_0, \dots, S_{m-1}\}$ and transitions $S_{m-1}1 = S_0$, $S_i1 = S_{i+1}$ for $i \neq m-1$, $S_{00} = S_0$, $S_i0 = S_{i-1}$ for $i > 0$, S_{m-1} is the final state.

From A and B we construct the corresponding automata, as in (2,4), and find the necessary number of attainable and distinct states, which proves the minimality (3).

The general formulation of problems of this kind is as follows: there are events $T(A_i)$ $(1 \leq i \leq k)$, representable in automata A_i with n_i states, respectively, and a k-ary operation f on events preserving representability in finite automata. What can be the maximal number of states of the minimal automaton representing $f(T(A_1), \dots, T(A_k))$, for given n_i?

The problems considered above belong to this class. Earlier a result was obtained (2,5) that reversal of words from a set representable

in an automaton with m states is representable in an automaton with 2^m states, and this estimate is attainable over the alphabet $\Sigma = \{a, b, c\}$.

From the results of (8) it follows that, for a set T (representable in an automaton A with n states), the set

$$\{xz \mid \exists y(xy \cdot z \in T \& [x^\theta] = [y^\theta] = [z^\theta])\}$$

may be nonrepresentable. We shall prove that the sets

$$\frac{p}{q}T = \{x \mid \exists y(x \cdot y \in T \& \frac{[x^\theta]}{[y^\theta]} = \frac{p}{q})\}$$

and $\sqrt{T} = \{x \mid xx \in T\}$ are always representable. We shall be interested in estimates of the complexity of these sets.

4. To represent $\frac{p}{q}T$, we first construct a nondeterministic automaton A_1, whose states will be the states of A, and whose transition matrix for all input letters is constructed as follows: $a_{ij} = 1 \leftrightarrow \exists x([x^\theta] = p \& S_{jx} = S_i)$. The set of initial states P_0 consists of the final states of A. From (5) it is known that, upon determinization, an automaton A_2 is obtained having no more than $2^{c\sqrt{n}\ln n}$ reachable states. The desired automaton has states $(S_i \mid l \mid P_j)$, where S_i is a state of A, P_j is a state of A_2, and $0 \leq l < q$ is an integer. The transitions are defined by the formula:

   $$(S_i \mid l \mid P_j)\sigma = (S_i\sigma \mid l + 1 (\operatorname{mod} q) \mid P_j\sigma^{-\operatorname{sign} l})$$

   $(S_0 \mid 0 \mid P_0)$ is the initial state. A state is final if $l = 0$ and $S_i \in P_j$. The number of states of this automaton is

   $$N(p, q, n) \leq qn2^{c\sqrt{n}\ln n}.$$

   A lower estimate for $\log_2 N(p, q, n)$ can be obtained using the example in (5), but it will differ by a multiplicative constant.

Next we shall need estimates of the number of congruence classes of a representable event (2).

5. To each word Z there corresponds a mapping of states $Z : S_i \to S_{iZ}$. Obviously, if the words x and y correspond to identical mappings, then they are congruent; that is, there are no more than n^n congruence classes. Consider the automaton from (7). This is the automaton B^n over the alphabet $\Sigma = \{a, b, c\}$ with states $\{Q_0, \dots, Q_{n-1}\}$ and transitions $Q_{n-1}a = Q_0,\ Q_{ia} = Q_{i+1}$ for $i \neq n-1,\ Q_0 b = Q_1,\ Q_1 b = Q_0,\ Q_{ib} = Q_i$ for $i > 1,\ Q_0 c = Q_0,\ Q_1 c = Q_0,\ Q_{ic} = Q_i$ for $i > 1$; Q_0 is final. B^n has exactly n^n congruence classes.

6. Over the alphabet $\Sigma = \{0, 1\}$ there cannot be an automaton with n states and n^n congruence classes. The exact value of the maximum number of congruence classes in this case is unknown; however, one can construct an automaton B_1^n having no fewer than $(n-1)^{n-1}$ of them. Its states are $\{P_0, \dots, P_{n-1}\}$, and the transitions are $P_{n-1}1 = P_1,\ P_{01} = P_2,\ P_i 1 = P_{i+1}$, for $i \neq 0,\ n-1,\ P_i 0 = P_0,\ P_{00} = P_2,\ P_{20} = P_1,\ P_i 0 = P_i$ for $i > 2$; P_1 is simultaneously the initial and final state.

Let us note that the states $P_1, \dots, P_{n-1}$, by the words $a' = 1,\ b' = 001^{n-1}$ and $c' = 01^{n-1}$, are mapped in the same way as the states of the automaton B^{n-1} by the words a, b, and c. Consequently, the set $(a' \cup b' \cup c')^*$ contains $(n-1)^{n-1}$ incongruent words.

7. The set $\sqrt{T}$ is representable in an automaton whose states are mappings or ordered n-tuples of states of A of length n; the transitions are given by the formula
$$(S_{i_1}, \dots, S_{i_n})\sigma = (S_{i_1}\sigma, \dots, S_{i_n}\sigma),$$
$(S_0, S_1, \dots, S_{n-1})$ is the initial state. A state is final if the tuple has a coordinate S_{i_1} that is a final state of A. The lower estimates n^n and $(n-1)^{n-1}$ are given by the automata B^n and B_1^n.

8. In (4) it is shown that permutations of letters in words from a representable set may form a nonrepresentable set. If only cyclic permutations are allowed, i.e.
$$T' = \{x \mid x = \sigma_{i_1} \dots \sigma_{i_k} \& \exists l (\sigma_{i_l} \dots \sigma_{i_k} \sigma_{i_1} \dots \sigma_{i_{l-1}} \in T)\}$$

(where T is representable in an automaton A with n states), then it can be proved that T' is also representable in an automaton B with $(n2^n - 2^{n-1})^n$ states. Indeed, let B_i have the same states and transitions as A, S_i being its initial state, and the final states the same as in the automaton A. Let C_i have the same states and transitions as A, S_0 its initial state, and S_i the only final state. Then
$$T' = \bigcup_{i=0}^{n-1} (T(B_i) \cdot T(C_i))$$

and, consequently (see 1) and 2)), it is representable in an automaton with $(n \cdot 2^n - 2^{n-1})^n$ states. Below we give an example yielding the lower estimate $((n-2) \cdot 2^{n-2})^{n-2}$ for $n > 3$. Here, however, the input alphabet grows together with the growth of n. $\Sigma = \{a_0, \dots, a_{n-2}, b_0, \dots, b_{n-2}\}$. The states of the automaton are $\{S_0, \dots, S_{n-1}\}$, and the transitions are $S_i a_i = S_{n-1}$, $S_{n-1} a_i = S_i$, $S_j a_i = S_j$ for $i \neq j$, $S_0 b_i = S_i$, $S_j b_i = S_j$ for $i \neq j$; S_{n-1} is the final state.

The author expresses his gratitude to A. A. Muchnik for his guidance.

Moscow State University
named after M. V. Lomonosov

Received
18 III 1970

REFERENCES

1. S. C. Kleene, in: *Automata*, Moscow, 1956.
2. M. O. Rabin, D. Scott, *Cybernetics Collection*, issue 4, 58 (1962).
3. E. F. Moore, in: *Automata*, Moscow, 1956.
4. V. M. Glushkov, *Uspekhi Mat. Nauk*, 16, issue 5 (101), 3 (1961).
5. Yu. I. Lyubich, *Siberian Mathematical Journal*, 5, No. 2, 337 (1964).
6. B. G. Mirkin, *Cybernetics*, No. 1, 7 (1966).
7. A. Paz, *Bull. Res. Council Israel*, 10F, No. 3, 93 (1962).
8. R. E. Stearns, J. Hartmanis, *Information and Control*, 6, No. 1, 55 (1963).