Доклады Академии наук СССР
1970. Том 194, № 6

УДК 519.95 *МАТЕМАТИКА*

А. Н. МАСЛОВ

ОЦЕНКИ ЧИСЛА СОСТОЯНИЙ КОНЕЧНЫХ АВТОМАТОВ

(Представлено академиком А. Н. Колмогоровым 27 III 1970)

В настоящей работе рассматриваются операции над множествами слов, представимыми в конечных автоматах. Важной характеристикой сложности этих множеств является число состояний минимального представляющего автомата.

Клини доказал ([1], [2]), что множество слов представимо в конечном автомате тогда и только тогда, когда оно получается из $\{\Lambda\}$ и $\{\sigma_i\}$ (где Λ — пустое слово, а σ_i — буквы входного алфавита Σ) применением операций объединения $(\bigcup)$ произведения $(\cdot)$ и итерации $(^*)$.

Далее $S_ix = S_k$ обозначает, что при поступлении на вход слова x автомат, находящийся в состоянии S_i, переходит в состояния S_k; индекс 0 соответствует начальному состоянию, если не оговорено противное; $[x^\partial$ обозначает длину слова x; $T(A)$ обозначает множество слов, представимых в автомате A. В дальнейшем под представимостью событий мы везде будем подразумевать представимость в конечном автомате.

Известно, что если $T(A)$ и $T(B)$ представимы в автоматах A и B с m и n состояниями соответственно ($m \geqslant 1$, $n \geqslant 1$), то

1) $T(A) \bigcup T(B)$ представимо в автомате с $m \cdot n$ состояниями,

2) $T(A) \cdot T(B)$ представимо в автомате с $(m-1) \cdot 2^n + 2^{n-1}$ состояниями ($n \geqslant 3$),

3) $T(A)^*$ представимо в автомате $\frac{3}{4} \cdot 2^m - 1$ состояниями ($m \geqslant 2$).

Нами построены примеры автоматов над алфавитом $\Sigma = \{0, 1\}$, на которых эти оценки достигаются.

1. Объединение: A имеет состояния $\{S_0, \ldots, S_{m-1}\}$ и переходы $S_{m-1}1 = S_0$, $S_i1 = S_{i+1}$ при $i \neq m-1$, $S_i0 = S_i$, S_{m-1} — заключительное состояние; B имеет состояния $\{P_0, \ldots, P_{n-1}\}$ и переходы $P_i1 = P_i$, $P_{n-1}0 = P_0$, $P_i0 = P_{i+1}$ при $i \neq n-1$, P_{n-1} — заключительное состояние.

2. Произведение: B имеет состояния $\{P_0, \ldots, P_{n-1}\}$ и переходы $P_{n-1}1 = P_{n-2}$, $P_{n-2}1 = P_{n-1}$, $P_i1 = P_i$ при $i < n-2$, $P_{n-1}0 = P_{n-1}$, $P_i0 = P_{i+1}$ при $i \neq n-1$, P_{n-1} — заключительное состояние; автомат A такой же, как для объединения.

3. Итерация: A имеет состояния $\{S_0, \ldots, S_{m-1}\}$ и переходы $S_{m-1}1 = S_0$, $S_i1 = S_{i+1}$ при $i \neq m-1$, $S_00 = S_0$, $S_i0 = S_{i-1}$ при $i > 0$, S_{m-1} — заключительное состояние.

По A и B строим соответствующие автоматы, как в ([2], [4]), и находим необходимое число достижимых и различных состояний, что и доказывает минимальность ([3]).

Общая постановка задач такого рода: имеются события $T(A_i)$ ($1 \leqslant i \leqslant k$), представимые в автоматах A_i с n_i состояниями соответственно, и k — местная операция f над событиями, сохраняющая представимость в конечных автоматах. Каким может быть максимальное число состояний минимального автомата, представляющего $f(T(A_1), \ldots, T(A_k))$, при данных n_i?

Рассмотренные выше задачи принадлежат этому классу. Ранее был получен результат ([2], [6]), что обращения слов из множества, представимого в автомате с m состояниями, представимо в автомате с 2^m состояниями и эта оценка достижима над алфавитом $\Sigma = \{a, b, c\}$.

Из результатов [8] следует, что для множества T (представимого в автомате A с n состояниями) $\{xz \mid \exists y (xy \cdot z \in T \& [x^\partial = [y^\partial = [z^\partial)\}$ может быть непредставимо. Мы докажем, что множества $\frac{p}{q} T = \left\{x \mid \exists y \left(x \cdot y \in T \& \frac{[x^\partial}{[y^\partial} = \frac{p}{q}\right)\right\}$ и $\sqrt{T} = \{x \mid xx \in T\}$ всегда представимы. Нас будут интересовать оценки сложности этих множеств.

4. Для представления $\frac{p}{q} T$ построим сначала недетерминированный автомат A_1, состояниями которого будут состояния A, а матрица переходов для всех входных букв строится так: $a_{ij} = 1 \leftrightarrow \exists x ([x^\partial = p \& S_j x = S_i)$. Множество начальных состояний P_0 состоит из заключительных состояний A. Из [5] известно, что при детерминизации получается автомат A_2, имеющий не более $2^{c\sqrt{n \ln n}}$ достижимых состояний. Искомый автомат имеет состояния $(S_i | l | P_j)$, где S_i — состояние A, P_j — состояние A_2, $0 \leqslant l < q$ — целое число. Переходы определяются формулой: $(S_i | l | P_j) \sigma = (S_i \sigma | l + 1 \pmod q) | P_j \sigma^{1 - \operatorname{sign} l})$ $(S_0 | 0 | P_0)$ — начальное состояние. Состояние является заключительным, если $l = 0$ и $S_i \in P_j$. Число состояний этого автомата $N(p, q, n) \leqslant qn 2^{c\sqrt{n . \ln n}}$. Нижнюю оценку для $\log_2 N(p, q, n)$ можно получить, используя пример в работе [5], но она будет отличаться мультипликативной константой.

Далее нам понадобятся оценки числа классов конгруэнтности представимого события [2].

5. Каждому слову Z соответствует отображение состояний Z: $S_i \to S_i Z$. Очевидно, что если словам x и y соответствуют одинаковые отображения, то они конгруэнтны, т. е. классов конгруэнтности не более n^n. Рассмотрим автомат из [7]. Это автомат B^n над алфавитом $\Sigma = \{a, b, c\}$ с состояниями $\{Q_0, \ldots, Q_{n-1}\}$ и переходами $Q_{n-1} a = Q_0$, $Q_i a = Q_{i+1}$ при $i \neq n - 1$, $Q_0 b = Q_1$, $Q_1 b = Q_0$, $Q_i b = Q_i$ при $i > 1$, $Q_0 c = Q_0$, $Q_1 c = Q_0$, $Q_i c = Q_i$ при $i > 1$; Q_0 — заключительное. B^n имеет ровно n^n классов конгруэнтности.

6. Над алфавитом $\Sigma = \{0, 1\}$ не может быть автомата с n состояниями и n^n классами конгруэнтности. Точное значение максимума числа классов конгруэнтности в этом случае неизвестно, однако можно построить автомат $B_1{}^n$, имеющий их не меньше, чем $(n - 1)^{n-1}$. Состояния его $\{P_0, \ldots, P_{n-1}\}$, а переходы $P_{n-1} 1 = P_1$, $P_0 1 = P_2$, $P_i 1 = P_{i+1}$, при $i \neq 0$, $n - 1$, $P_1 0 = P_0$, $P_0 0 = P_2$, $P_2 0 = P_1$, $P_i 0 = P_i$ при $i > 2$; P_1 — начальное и заключительное состояние одновременно.

Заметим, что состояния $P_1, \ldots, P_{n-1}$ словами $a' = 1$, $b' = 001^{n-1}$ и $c' = 01^{n-1}$ отображаются так же, как состояния автомата B^{n-1} словами a, b и c. Следовательно, в множестве $(a' \cup b' \cup c')^*$ имеется $(n - 1)^{n-1}$ неконгруэнтных слов.

7. Множество $\sqrt{T}$ представимо в автомате, состояниями которого являются отображения или упорядоченные наборы длины n состояний A, переходы задаются формулой

$$(S_{i_1}, \ldots, S_{i_n}) \sigma = (S_{i_1} \sigma, \ldots, S_{i_n} \sigma),$$

$(S_0, S_1, \ldots, S_{n-1})$ — начальное состояние. Состояние является заключительным, если набор имеет координату $S_{i_{i_1}}$ заключительным состоянием A. Нижние оценки n^n и $(n - 1)^{n-1}$ дают автоматы B^n и $B_1{}^n$.

8. В [4] показано, что перестановки букв в словах из представимого множества могут образовывать непредставимое множество. Если допускать только циклические перестановки, т. е.

$$T' = \{x \mid x = \sigma_{i_1} \ldots \sigma_{i_k} \& \exists l (\sigma_{i_l} \ldots \sigma_{i_k} \sigma_{i_1} \ldots \sigma_{i_{l-1}} \in T\}$$

(где T представимо в автомате A с n состояниями), то можно доказать, что и T' представимо в автомате B с $(n2^n - 2^{n-1})^n$ состояниями. Действительно, пусть B_i имеет те же состояния и переходы, что и A, S_i — его начальное состояние, заключительные состояния те же, что в автомате A. C_i имеет те же состояния и переходы, что и A, S_0 — его начальное, а S_i — единственное заключительное состояние. $T' = \bigcup_{i=0}^{n-1} (T(B_i) \cdot T(C_i))$ и, следовательно (см. 1) и 2)), представимо в автомате с $(n \cdot 2^n - 2^{n-1})^n$ состояниями. Ниже указан пример, дающий нижнюю оценку $((n-2) \cdot 2^{n-2})^{n-2}$ при $n > 3$. При этом, правда, входной алфавит растет вместе с ростом n. $\Sigma = \{a_0, \ldots, a_{n-2}, b_0, \ldots, b_{n-2}\}$. Состояния автомата $\{S_0, \ldots, S_{n-1}\}$, переходы $S_i a_i = S_{n-1}$, $S_{n-1} a_i = S_i$, $S_j a_i = S_j$ при $i \neq j$, $S_0 b_i = S_i$, $S_j b_i = S_j$ при $i \neq j$; S_{n-1} — заключительное состояние.

Автор выражает благодарность А. А. Мучнику за руководство.

Московский государственный университет
им. М. В. Ломоносова

Поступило
18 III 1970

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] С. К. Клини, Сборн. Автоматы, М., 1956. [2] М. О. Рабин, Д. Скотт, Кибернетический сборник, в. 4, 58 (1962). [3] Э. Ф. Мур, Сборн. Автоматы, М., 1956. [4] В. М. Глушков, УМН, 16, в. 5 (101), 3 (1961). [5] Ю. И. Любич, Сибирский математический журнал, 5, № 2, 337 (1964). [6] Б. Г. Миркин, Кибернетика, № 1, 7 (1966). [7] A. Paz, Bull. Res. Council Israel, 10F, № 3, 93 (1962). [8] R. E. Stearns, J. Hartmanis, Information and Control, 6, № 1, 55 (1963).