Секция 9

ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ

УДК 519.7

ОЦЕНКА КРАТНОСТИ ВЫХОДНОГО СИМВОЛА
В ОБРАТИМОМ АВТОМАТЕ

Д. А. Катеринский

Доказано, что максимальное количество ρ повторений некоторого выходного символа в таблице выходов автомата с n состояниями и m входными символами, при котором автомат обратим, вычисляется по формуле $\rho = \lfloor (n+1)/2 \rfloor \lfloor (n+2)/2 \rfloor$, если $\lfloor (n+2)/2 \rfloor \leq m$, и $\rho = (n-m+1)m$ в противном случае.

Ключевые слова: конечные автоматы, обратимость, слабая обратимость, сильная обратимость, анализ обратимости, пороговое число обратимости.

Рассматриваются сильно и слабо обратимые конечные автоматы с конечной задержкой. В первых входная последовательность восстанавливается с задержкой по выходной последовательности, во вторых — по выходной последовательности и начальному состоянию [1, 2]. Автомат называется обратимым, если он слабо или сильно обратим. Множество всех обратимых автоматов обозначается Inv .

Пусть далее A есть произвольный конечный автомат с n состояниями, m входными символами и с множеством выходных символов Y . Пусть также $\rho^A(y)$ — количество вхождений выходного символа $y \in Y$ в таблице выходов автомата A , $\rho(A) = \max_{y \in Y} \{\rho^A(y)\}$ и $\rho = \max_{A \in Inv} \rho(A)$.

По определению, ρ есть максимально возможное количество повторений символа в таблице выходов автомата, при котором этот автомат обратим.

Теорема 1.

$$\rho = \begin{cases} \left\lfloor \frac{n+1}{2} \right\rfloor \left\lfloor \frac{n+2}{2} \right\rfloor, & \text{если } \left\lfloor \frac{n+2}{2} \right\rfloor \leq m; \\ (n-m+1)m, & \text{если } \left\lfloor \frac{n+2}{2} \right\rfloor > m. \end{cases}$$

ЛИТЕРАТУРА

1. Курмит А. А. Автоматы без потери информации конечного порядка. Рига: Зинатне, 1972.
2. Тао Р. J. Finite automata and application to cryptography. Tsinghua: Springer, 2008.