УДК 519.713.4 DOI 10.17223/2226308X/9/45

О ПРОСТЫХ УСЛОВНЫХ ЭКСПЕРИМЕНТАХ ИДЕНТИФИКАЦИИ ОБРАТИМЫХ АВТОМАТОВ НЕКОТОРОГО КЛАССА

А. О. Жуковская, В. Н. Тренькаев

Рассматривается класс сильносвязных автоматов, получаемых из некоторого инициального обратимого автомата с m состояниями, n входными и n выходными символами путём изменения его функции переходов в зависимости от ключа. Показывается существование простого условного эксперимента, идентифицирующего автоматы в этом классе и имеющего длину не более $mn(m+3)/2$.

Ключевые слова: *инициальный автомат, перестраиваемый автомат, обратимый автомат, сильносвязный автомат, идентификация автоматов, простые условные эксперименты.*

Следуя [1], назовём *перестраиваемым автоматом* набор из восьми объектов $R = (X, S, Y, K, \psi, \varphi, \delta_0, \delta_1)$, где $X = \{x_1, x_2, \ldots, x_n\}$, $Y = \{y_1, y_2, \ldots, y_n\}$, $S = \{s_1, s_2, \ldots, s_m\}$ — множества входных символов, выходных символов и состояний соответственно; $K = \{k : k = ||k_{ij}||, k_{ij} \in \{0,1\}, i = 1, \ldots, n, j = 1, \ldots, m\}$ — множество ключей; $\varphi : X \times S \to Y$ — функция выходов; $\psi : X \times S \times K \to S$ — функция переходов, такая, что $\psi(x_i, s_j, k) = \psi_k(x_i, s_j) = \delta_{k_{ij}}(x_i, s_j)$ для некоторых функций $\delta_p : X \times S \to S$, $p \in \{0,1\}$.

Автомат R называется *обратимым*, если функция $\varphi_s(x) = \varphi(x, s)$ является биекцией для любого $s \in S$.

Обозначим через $A_{n,m}$ множество всех инициальных обратимых перестраиваемых автоматов R с фиксированными множествами X, S, Y, K и следующими свойствами:

1) среди $\varphi_s(x)$, $s \in S$, нет одинаковых биекций; 2) при любом $k \in K$ автомат $R_k = (X, S, Y, \psi_k, \varphi)$ сильносвязен.

Теорема 1. Для любого автомата $R \in A_{n,m}$ существует простой условный эксперимент длины не более $nm(m+3)/2$, идентифицирующий автоматы в классе $\{R_k : k \in K\}$.

ЛИТЕРАТУРА

1. *Тренькаев В. Н.* Реализация шифра Закревского на основе перестраиваемого автомата // Прикладная дискретная математика. 2010. № 3. С. 69–77.

УДК 519.7 DOI 10.17223/2226308X/9/46

О ТРАНЗИТИВНОСТИ ОТОБРАЖЕНИЙ, АССОЦИИРОВАННЫХ С КОНЕЧНЫМИ АВТОМАТАМИ ИЗ ГРУПП AS_p

М. В. Карандашов

Рассматривается вопрос определения свойства транзитивности автоматных отображений. Приводится общий критерий транзитивности автоматного отображения на словах длины $k \in \mathbb{N}$. Для автоматов из групп AS_p предложен алгоритм проверки транзитивности. Сложность представленного алгоритма зависит от числа состояний автомата и не зависит от длины входного слова; приведена верхняя граница сложности алгоритма.

Ключевые слова: *конечные автоматны, автоматные отображения группы AS_p, транзитивность.*