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.*

Под *детерминированным автоматом* будем понимать пятёрку объектов $A = (S, X, Y, \delta, \lambda)$, где S — множество состояний; X — входной алфавит; Y — выходной алфавит; $\delta : S \times X \to S$ — функция переходов; $\lambda : S \times X \to Y$ — функция выходов. Для всех рассматриваемых в работе автоматов $|S|, |X|, |Y| \in \mathbb{N}$ и $X = Y = \{0, 1, \ldots, p-1\}$, p — простое.

Пусть X^* обозначает множество всех конечных слов над алфавитом X. Действие функций δ и λ можно расширить на множество слов X^* следующими рекуррентными правилами: $\delta(s, x \cdot w) = \delta(\delta(s, x), w)$, $\lambda(s, x \cdot w) = \lambda(s, x) \cdot \lambda(\delta(s, x), w)$, $x \in X$, $w \in X^*$.

Автомат с выделенным начальным состоянием называют *инициальным*. Инициальный автомат будем обозначать через A_s, где s — начальное состояние автомата. Каждый инициальный автомат A_s определяет отображение $f_{A_s} : X^* \to Y^*$, называемое *автоматным*, такое, что $f_{A_s}(w) = \lambda(s, w)$.

Автоматное отображение f называют *транзитивным на словах длины* k, если оно порождает одноцикловую перестановку на X^k. Отображение f *транзитивно*, если оно транзитивно на X^k для любого натурального k. Транзитивные отображения представляют значительный интерес в силу того, что применяются для решения как теоретических, так и практических задач. В частности, описаны семейства транзитивных автоматных отображений [1].

Будем называть *состоянием с потерей* [2] такое состояние s, что $\lambda(s, x_1) = \lambda(s, x_2)$ для некоторых $x_1, x_2 \in X$, $x_1 \neq x_2$.

Теорема 1 [3]. Автоматное отображение $f_{A_s} : X^* \to X^*$ биективно на X^k тогда и только тогда, когда автомат A_s не содержит состояний с потерей, достижимых из s за k шагов.

Далее будем рассматривать только инициальные автоматы, порождающие биективные отображения. Следовательно, отображение f_{A_s} осуществляет перестановку множества X, которую будем обозначать σ_s.

Действие инициального конечного автомата на входные последовательности можно описать с помощью бесконечного сбалансированного дерева [4]. Обозначим дерево, ассоциированное с действием автомата A_s, символом $T(A_s)$. Обозначим через $T(A_s, k)$ мультимножество состояний автомата A, где состояние s' входит в $T(A_s, k)$ ровно столько раз, со сколькими вершинами k-го яруса $T(A_s)$ ассоциировано состояние s'.

Рассмотрим итерацию слова $w \in X^k$ автоматным отображением f_{A_s}. Пусть $f_{A_s}(w) = w_1$, $f_{A_s}(f_{A_s}(w)) = w_2$, $\ldots$, $f^m_{A_s}(w) = w$ и m — наименьшее из возможных. Составим кортеж из перестановок $\sigma_{\delta(s,w)}, \ldots \sigma_{\delta(s,w_{m-1})}$ и обозначим через $Ar(T(A_s), w)$.

Лемма 1. Автоматное отображение f_{A_s} действует транзитивно на словах длины $(k+1)$, где $k \in \mathbb{N}$, тогда и только тогда, когда одновременно выполняются следующие условия:

1) f_{A_s} действует транзитивно на словах длины k;
2) для всех $w \in X^k$ композиция $\sigma_{\delta(s,w)} \circ \sigma_{\delta(s,w_1)} \circ \ldots \circ \sigma_{\delta(s,w_{p^k-1})}$ элементов $Ar(T(A_s), w)$ является одноцикловой перестановкой.

Заметим, что для каждого простого p существует циклическая группа перестановок $\langle \sigma_+(p) \rangle$, где $\sigma_+(p) = (0\ 1\ \ldots\ (p-1))$ — образующий элемент группы [5]. Инициальные автоматы, где с каждым состоянием связана перестановка из $\langle \sigma_+(p) \rangle$, образуют группу AS_p [6]. Важным является тот факт, что $\langle \sigma_+(p) \rangle$ — абелева группа.

Тут и далее под автоматом будем понимать автомат из группы AS_p.

Пусть автомат A_s действует транзитивно на словах длины k. Следовательно, $Ar(T(A_s), w)$ является некоторым упорядочиванием мультимножества перестановок, ассоциированных с состояниями из $T(A_s, k)$. Более того, в силу коммутативности перестановок из $\langle\sigma_+(p)\rangle$, композиции элементов из $Ar(T(A_s), w)$ совпадают для всех возможных w, т. е. композиция элементов $Ar(T(A_s), w)$ однозначно определяется мультимножеством $T(A_s, k)$ и не зависит от выбора w. Следовательно, достаточно проверить, что композиция перестановок (в произвольном порядке), ассоциированных с состояниями из $T(A_s, k)$, является одноцикловой.

Введём матрицы M и $\widehat{M}$, а также векторы V_σ и R. По таблице переходов конечного автомата A построим матрицу смежности M размера $n \times n$. Значения элементов матрицы M вычисляются как мощности множеств $\{x : x \in X, \delta(s_i, x) = s_j\}$, где i, j — номера строки и столбца матрицы. Таким образом, i-я строка матрицы M^k описывает $T(A_{s_i}, k)$.

Построим вектор V_σ следующим образом. Как отмечено выше, с состоянием s_i автомата связана некоторая перестановка τ_i из $\langle\sigma_+(p)\rangle$. Следовательно, в силу цикличности группы $\langle\sigma_+(p)\rangle$, $\tau_i = \sigma_+(p)^{h_i}$, $h_i = 0, \ldots, (p-1)$. Сопоставим i-му элементу вектора V_σ число h_i. Положим $R_k = M^k \cdot V_\sigma^{\mathrm{T}}$, где i-й элемент есть степень перестановки $\sigma_+(p)$, получаемой при композиции перестановок, ассоциированных с $T(A_{s_i}, k)$. Таким образом, задача проверки транзитивности сводится к последовательному сравнению с нулём значений i-х ячеек R_k, $k \geqslant 1$.

Основной проблемой использования матрицы M является то, что количество попарно различных матриц M^k, $k \in \mathbb{N}$, бесконечно. Построим матрицу $\widehat{M}$ из M следующим образом. Каждому элементу m_{ij} матрицы M сопоставим элемент $\widehat{m}_{ij} = m_{ij} \bmod p$ матрицы $\widehat{M}$.

Лемма 2. Пусть $\widehat{R}_k = \widehat{M}^k \cdot V_\sigma^{\mathrm{T}}$. Тогда $r_i^k = \widehat{r}_i^k \pmod p$.

Заметим, что количество различных матриц $\widehat{M}$ для фиксированных p и n конечно и равно p^{n^2}. Составим на основе представленных результатов алгоритм проверки транзитивности автомата A_{s_i} (алгоритм 1). Можно показать, что строки матрицы $\widehat{M}^k$ не могут быть произвольными, а лишь такими, где сумма элементов строки кратна p.

Алгоритм 1. Алгоритм проверки транзитивности автомата

Вход: Конечный автомат $A_{s_i} \in AS_p$
Выход: `true`, если A_{s_i} транзитивен, `false` иначе

1: Построить матрицу $\widehat{M}$ и вектор V_σ по автомату A_{s_i}.
2: **Если** i-й элемент V_σ равен нулю, **то**
3: вернуть `false`.
4: Положить $k := 1$, $L := \varnothing$.
5: **Пока** $\widehat{M}^k \notin L$
6: $\widehat{R}^k := \widehat{M}^k \cdot V_\sigma^{\mathrm{T}}$.
7: **Если** i-й элемент $\widehat{R}^k$ сравним с 0 по модулю p, **то**
8: вернуть `false`.
9: Добавить $\widehat{M}^k$ в L, увеличить k на 1.
10: Вернуть `true`.

Теорема 2. Максимальное число умножений матриц, требуемое для остановки алгоритма, ограничено сверху числом $(p^{(n-1)} - 1)$.

Полученная в теореме 2 оценка сложности является достижимой, что было подтверждено численными экспериментами.

ЛИТЕРАТУРА

1. *Тяпаев Л. Б.* Транзитивные семейства автоматных отображений // Дискретные модели в теории управляющих систем: IX Междунар. конф., Москва и Подмосковье, 20–22 мая 2015. Труды / отв. ред. В. Б. Алексеев, Д. С. Романов, Б. Р. Данилов. М.: МАКС Пресс, 2015. С. 244–247.
2. *Гилл А.* Введение в теорию конечных автоматов. М.: Наука, 1966. 272 с.
3. *Карандашов М. В.* Исследование биективных автоматных отображений на кольце вычетов по модулю 2^k // Компьютерные науки и информационные технологии: Материалы Междунар. науч. конф. Саратов: Издат. центр «Наука», 2014. С. 148–152.
4. *Яблонский С. В.* Введение в дискретную математику: учеб. пособие для вузов. 2-е изд., перераб. и доп. М.: Наука, 1986. 384 с.
5. *Калужнин Л. А., Сущанский В. И.* Преобразования и перестановки: пер. с укр. 2-е изд., перераб. и доп. М.: Наука, 1985. 160 с.
6. *Алешин С. В.* Конечные автоматы и проблема Бернсайда о периодических группах // Матем. заметки. 1972. Т. 11. № 3. С. 319–328.