ИНФОРМАТИКА

УДК 519.7

АЛГОРИТМ ПРОВЕРКИ ТРАНЗИТИВНОСТИ ОТОБРАЖЕНИЙ, АССОЦИИРОВАННЫХ С КОНЕЧНЫМИ АВТОМАТАМИ ИЗ ГРУПП AS_p

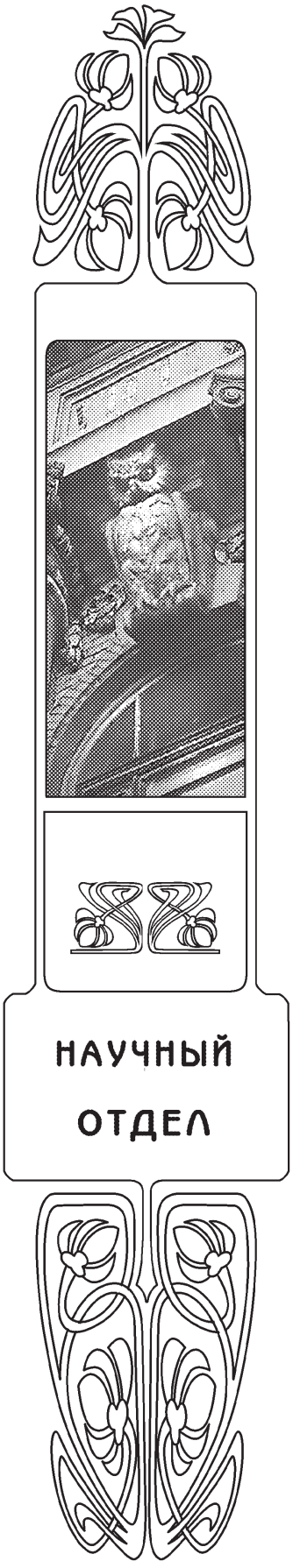
М. В. Карандашов

Карандашов Максим Валерьевич, ассистент кафедры дискретной математики и информационных технологий, Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, Россия, 410012, Саратов, Астраханская, 83, norg113@gmail.com

В статье затрагивается вопрос определения свойства транзитивности автоматных отображений, определяемых конечными детерминированными автоматами. Приведен критерий транзитивности автоматных отображений на словах конечной длины в терминах конечных детерминированных автоматов и деревьев детерминированных функций. Показано, что для конечных автоматов из групп AS_p можно построить алгоритм проверки транзитивности. Для доказательства данного факта использованы свойства абелевых групп перестановок. На основе представленных результатов построен матричный алгоритм проверки транзитивности автоматных отображений на словах конечной длины для инициальных автоматов из групп AS_p. Особенностью данного алгоритма является его независимость от длин рассматриваемых слов. Даны результаты численных экспериментов и точная верхняя граница сложности представленного алгоритма.

Ключевые слова: конечные автоматы, транзитивность, автоматные отображения, группы AS_p.

DOI: 10.18500/1816-9791-2017-17-1-85-95



ВВЕДЕНИЕ

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 рассматриваемых в работе автоматов входной и выходной алфавиты совпадают и равны $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, где p — простое.

Автомат с выделенным начальным состоянием называют *инициальным*. Инициальный автомат будем обозначать через A_s, где s — начальное состояние автомата.

Пусть X^* обозначает множество всех конечных слов над алфавитом X. Действие функций δ и λ можно расширить на множество слов X^* следующими реккурентными правилами:

$$\delta(s, x \cdot w) = \delta(\delta(s, x), w), \quad \lambda(s, x \cdot w) = \lambda(s, x) \cdot \lambda(\delta(s, x), w),$$
$$x \in X, \quad w \in X^*, \quad e \text{ — пустой символ.}$$

Преобразование $f : X^* \to X^*$ называется (синхронно) автоматным, если существует задающий его инициальный автомат A_s [1]. В дальнейшем если автомат ясен из контекста, будем обозначать автоматное отображение f_{A_s} через f_s или же просто как f (если и начальное состояние автомата следует из контекста).

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 [2, 3].

1. ОБЩИЕ СВОЙСТВА АВТОМАТНЫХ ОТОБРАЖЕНИЙ

Покажем основные свойства автоматных отображений, представляющие интерес в контексте данной работы.

Перед тем как перейти к дальнейшим рассуждениям, следует указать критерий биективности автоматного отображения (в силу очевидной связи между свойствами биективности и транзитивности отображений).

Будем называть s *состоянием с потерей* [4], если существуют такие $x_1, x_2 \in X$, что $x_1 \neq x_2$ и $\lambda(s, x_1) = \lambda(s, x_2)$.

Теорема 1 (см. [5]). *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.*

Таким образом, из теоремы 1 становится понятно, что искать автоматы, порождающие транзитивные отображения, следует лишь среди автоматов, с каждым состоянием которых связана перестановка элементов входного алфавита. Далее будем рассматривать только инициальные автоматы, порождающие биективные отображения.

Под *перестановкой* множества X будем понимать биекцию $X \to X$. Для перестановок определена операция композиции $\circ$ такая, что для $\psi = \pi \circ \sigma$ справедливо, что $\psi(x) = \pi(\sigma(x))$.

В силу того что мы рассматриваем только такие инициальные автоматы, которые порождают биективные автоматные отображения, имеет место следующий факт: для автомата A_s с каждым достижимым из s состоянием s' (включая само s) связано такое автоматное отображение $f_{s'}$, что $f_{s'}$ действует биективно на словах длины 1, т. е. $f_{s'}$ осуществляет перестановку множества X. Будем обозначать данную перестановку через $\sigma_{s'}$.

Действие инициального конечного автомата на входные последовательности можно описать с помощью бесконечного сбалансированного дерева [6]. 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 (нумерация ярусов начинается с нуля) $T(A_s)$ 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 (m существует в силу биективности f_{A_s}). Слова $w, w_1, w_2, \ldots, w_{m-1}$ описывают последовательность вершин k-го яруса дерева $T(A_s)$, возникающую при итерации слова w. С данными вершинами $T(A_s)$ связаны состояния $s_{\delta(s,w)}, s_{\delta(s,w_1)}, \ldots s_{\delta(s,w_{m-1})}$ автомата A.

Составим кортеж из перестановок $\sigma_{\delta(s,w)}, \sigma_{\delta(s,w_1)}, \ldots \sigma_{\delta(s,w_{m-1})}$, ассоциированных с состояниями $s_{\delta(s,w)}, s_{\delta(s,w_1)}, \ldots s_{\delta(s,w_{m-1})}$. Обозначим данный кортеж через $Ar(T(A_s), w)$, т. е. $Ar(T(A_s), w)$ описывает то, как автомат A_s будет преобразовывать $(k+1)$-й символ последовательности $w \cdot a$ при её итерировании отображением f_{A_s}. Отметим, что если f_{A_s} транзитивно на словах из $X^{|w|}$, то в кортеже $Ar(T(A_s), w)$ будет ровно $p^{|w|}$ элементов.

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 любого слова $w \in X^k$ композиция $\sigma_{\delta(s,w_1)} \circ \sigma_{\delta(s,w_2)} \circ \ldots \circ \sigma_{\delta(s,w_{p^k})}$ элементов $Ar(T(A_s), w)$ является одноцикловой перестановкой.

Доказательство. Обозначим $\sigma_{\delta(s,w_1)} \circ \sigma_{\delta(s,w_2)} \circ \ldots \circ \sigma_{\delta(s,w_{p^k})}$ символом ψ. Тогда

$$\forall\ a \in X:\ f^{p^k}_{A_s}(w \cdot a) = w \cdot \psi(a).$$

Покажем *достаточность*. Пусть условие леммы выполняется, т. е. для слов длины $k \in \mathbb{N}$ отображение f_{A_s} действует транзитивно и ψ есть одноцикловая перестановка множества X. Следовательно, если ψ есть одноцикловая перестановка X, то $f^{p^k \cdot p}_{A_s}(w \cdot a) = w \cdot \psi^p(a) = w \cdot a$, т. е. f_{A_s} действует транзитивно на словах длины $k+1$.

Покажем *необходимость*. Пусть не выполняется первое условие леммы, тогда отображение f_{A_s} не действует транзитивно на словах длины $k \in \mathbb{N}$, т. е. существует такое число $m \in \mathbb{N}$, что $m \bmod p^k \neq 0$ и $f^m_{A_s}(w) = w$.

Возьмём символ $a \in X$ и рассмотрим слово $w \cdot a \in X^{k+1}$. Тогда $f^m_{A_s}(w \cdot a) = w \cdot \psi(a)$. В силу того что $m \bmod p^k \neq 0$, найдётся такое слово $w' \in X^k$, для которого не существует $c \in \mathbb{N}$ такого, что $f^c_{A_s}(w) = w'$. Следовательно, не существует $d \in \mathbb{N}$ такого, что $f^d_{A_s}(w \cdot a) = w' \cdot a'$, где a' есть произвольный элемент X. Что противоречит определению транзитивности на словах фиксированной длины.

Теперь пусть не выполняется второе условие леммы, т. е. ψ не является одноцикловой перестановкой (не выполняется второе условие леммы) для некоторого k. Рассмотрим символы $a, b \in X$ такие, что $a \neq b$, и пусть не существует такого числа $c \in \mathbb{N}$, что $\psi^c(a) = b$. Тогда для слова $w \cdot a \in X^{k+1}$ не существует такого числа $d \in \mathbb{N}$, что $f^d_{A_s}(w \cdot a) = w \cdot b$. Следовательно, f_{A_s} не транзитивно на словах длины $k+1$. □

Из леммы 1 следует, что для проверки транзитивности автоматного отображения требуется построение композиции элементов из $Ar(T(A_s), w)$ для любого натурального k и для всех возможных слов $w \in X^k$. Это требование возникает в силу того, что операция $\circ$ (композиции перестановок) в общем случае не коммутативна, т. е. $\sigma \circ \pi \neq \pi \circ \sigma$.

2. ПОСТРОЕНИЕ АЛГОРИТМА

Покажем, что существуют автоматы, для которых можно обойти описанные выше ограничения на явное вычисление $Ar(T(A_s), w)$.

Заметим, что для каждого простого p существует циклическая группа перестановок $\langle\sigma_+(p)\rangle$, где $\sigma_+(p)$ — образующий элемент группы и $\sigma_+(p) = (0, \ldots, (p-1))$ [7]. Инициальные автоматы, где с каждым состоянием связана перестановка из $\langle\sigma_+(p)\rangle$, образуют группу AS_p [8]. В качестве групповой операции используется последовательное соединение автоматов. Стоит отметить, что AS_2 совпадает с классом инициальных автоматов, определяющих биективные отображения на алфавите $\{0, 1\}$.

Важным является тот факт, что $\langle\sigma_+(p)\rangle$ — абелева группа, т. е. операция $\circ$ для перестановок из данной группы является коммутативной. Далее, используя свойство коммутативности операции $\circ$ для перестановок из $\langle\sigma_+(p)\rangle$, будет построен алгоритм определения транзитивности для инициальных автоматов из групп AS_p.

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

Пусть автомат A_s действует транзитивно на словах длины k. Следовательно, во-первых, количество элементов в кортеже $Ar(T(A_s), w)$ будет ровно p^k. Во-вторых, $Ar(T(A_s), w)$ будет являться 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 $Ar(T(A_s), w)$ будут совпадать для всех возможных w, т. е. композиция элементов $Ar(T(A_s), w)$ будет однозначно определяться мультимножеством $T(A_s, k)$ и не будет зависеть от выбора w. Данный факт имеет важное значение для построения алгоритма.

Чтобы показать, что некоторый автомат A_s действует транзитивно на словах длины $k+1$, по лемме 1 нам необходимо знать, что A_s действует транзитивно на словах длины k и проверить одноцикловость перестановок, порождаемых всеми возможными $Ar(T(A_s), w), w \in X^k$.

Достаточно проверить, что композиция перестановок (в произвольном порядке), ассоциированных с состояниями из $T(A_s, k)$, является одноцикловой. Построим алгоритм, который будет последовательно проверять одноцикловость перестановок, ассоциированных с $T(A_s, k)$.

Для построения данного алгоритма введём матрицы M и $\widehat{M}$, а также векторы V_σ и R. Использование данных объектов преследует две основные цели. Во-первых, это получение критерия останова алгоритма. Во-вторых, представление автоматов в матричном виде, являющемся более удобным для обработки вычислительными устройствами.

2.1. Матрица M и векторы V_σ, R

Первой задачей, которую требуется решить, будет построение $T(A_s, k)$.

По таблице переходов конечного автомата A построим матрицу смежности M размерности $n \times n$, где n — количество состояний в автомате A. С целью сопоставления строк и столбцов матрицы M с состояниями автомата A, пронумеруем состояния автомата A числами от 1 до n и будем отождествлять i-е состояние автомата с i-й строкой и i-м столбцом матрицы. Значения ячеек матрицы M вычисляются как мощности множеств $\{x \mid x \in X, \delta(s_i, x) = s_j\}$, где i — номер строки матрицы, j — номер столбца матрицы.

Из построения M следует, что в ячейках матрицы M^k будет располагаться количество слов длины k, переводящих i-е состояние в j-е. i-я строка матрицы M^k будет

полностью описывать набор состояний, достижимых из i-го за k шагов. M^0 обозначает единичную матрицу размерности $n \times n$. Таким образом, i-я строка матрицы M^k описывает $T(A_{s_i}, k)$.

Матрица M^k описывает лишь количество различных состояний, достижимых на k-м шаге. Для проверки транзитивности необходимо определить перестановку, описываемую композицией перестановок, ассоциированных с состояниями из $T(A_s, k)$.

Для решения данной задачи построим вектор V_σ следующим образом. Как уже было 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. $R_k = M^k \times V_\sigma^T$, где i-й элемент есть степень перестановки $\sigma_+(p)$, получаемой при композиции перестановок, ассоциированных с $T(A_{s_i}, k)$.

Например, $V_{\sigma_B} = (1\ 0\ 1\ 0\ 1\ 0), (M_B \times V_{\sigma_B}^T)^T = (1\ 0\ 1\ 0\ 1\ 2)$.

Таким образом, задача проверки транзитивности сводится к последовательному сравнению с нулём значений i-х ячеек $R_k, k \geqslant 1$ для заданной вершины автомата. Если i-я ячейка вектора R_k равняется нулю, то композиция соответствующих перестановок есть тождественная подстановка, что ведёт к неудовлетворению автоматом с начальным состоянием s_i условию леммы 1 и, как следствие, отсутствию транзитивности на словах длины k. Основной проблемой использования матрицы M является тот факт, что количество попарно различных матриц M^k, где $k \in \mathbb{N}$, — бесконечно.

2.2. Матрица $\widehat{M}$

Построим матрицу $\widehat{M}$ из M следующим образом. Каждой ячейке m_{ij} матрицы M сопоставим ячейку $\widehat{m}_{ij} = m_{ij} \bmod p$. Обозначим это как $\widehat{M} = M \bmod p$. Также определим возведение $\widehat{M}$ в k-ю степень как $\widehat{M}^k = \left(\underbrace{\widehat{M} \times \ldots \times \widehat{M}}_{k} \right) \bmod p$.

Для степенных последовательностей вида $A, A^2, A^3, \ldots$ будем использовать обозначение $Seq(A) = a_1 a_2 \ldots$, где a_i из $Seq(A)$ равняется A^i.

Лемма 2. *Пусть* $\widehat{R}_k = \widehat{M}^k \times V_\sigma^T$. *Тогда* $r_i^k \bmod p = \widehat{r}_i^k$.

Доказательство. По построению $r_i^k = \sum\limits_{j=1}^{n} m_{ij}^k \cdot V_{\sigma_j}^T$. Тогда

$$r_i^k \bmod p = (\sum_{j=1}^{n} m_{ij}^k \cdot V_{\sigma_j}^T) \bmod p = \sum_{j=1}^{n} (m_{ij}^k \cdot V_{\sigma_j}^T \bmod p) \bmod p = \widehat{r}_i^k.$$

Что и требовалось показать. □

Следствие. *Для любого* $k \in \mathbb{N}$ *справедливо, что* $\widehat{M}^k = M^k \bmod p$.

Из построения матрицы $\widehat{M}$ следует оценка сверху общего числа попарно различных матриц, которые могут входить в $Seq(\widehat{M})$.

Для получения следующей оценки достаточно вспомнить формулу размещений с повторениями.

Лемма 3. *Количество попарно различных матриц* $\widehat{M}$ *для фиксированных* p *и* n *конечно и равняется* p^{n^2}, *где* n — *количество состояний автомата.*

Но тогда справедливо, что существуют числа $d, c \in \mathbb{N}$ такие, что $\widehat{M}^d = \widehat{M}^{c \cdot d}$. Другими словами, начиная с некоторого шага d, последовательность $Seq(\widehat{M})$ является периодической. Следовательно, для проверки транзитивности достаточно найти период последовательности $Seq(\widehat{M})$ и проверить неравенство нулю i-го элемента каждого вектора из $Seq(\widehat{R})$, соответствующих периоду и предпериоду $Seq(\widehat{M})$.

2.3. Общий ход алгоритма

Составим на основе представленных ранее результатов алгоритм проверки транзитивности автомата A_{s_i}.

Вход: Конечный автомат $A_{s_i} \in AS_p$.

Выход: **True**, если отображение, связанное с A_{s_i}, транзитивно. **False** в ином случае.

1. Построить матрицу $\widehat{M}$ и вектор V_σ;
2. Если i-й элемент V_σ равен 0 — завершить работу и вернуть **False**;
3. Положим $k = 1$, $L = \varnothing$;
4. Если $\widehat{M}^k \in L$, то завершить работу и вернуть **True**;
5. $\widehat{R}^k = \widehat{M}^k \times V_\sigma^T$;
6. Если i-й элемент $\widehat{R}^k$ сравним с нулём по модулю p, то завершить работу и вернуть **False**;
7. Добавить $\widehat{M}^k$ в L, увеличить k на 1;
8. Перейти к шагу 4.

Рассмотрим принцип работы представленного алгоритма.

На шаге 2 производится проверка того, что автомат A_{s_i} действует транзитивно на словах длины 1. Если это не так, то выводится **False**.

Шаги с 4-го по 8-й производят последовательную проверку того, что автомат A_{s_i} действует транзитивно на словах длины $2, 3, \ldots$. Для этого используется критерий из леммы 1 с уточнениями из параграфа 2. Действительно, на каждой итерации по 4–8 шагам, производится построение вектора $\widehat{R}^k$ и проверка того, что i-й элемент $\widehat{R}^k$ не равен 0. Если же i-й элемент $\widehat{R}^k$ равен нулю, что соответствует случаю, когда композиция перестановок, порождаемая $T(A_s, k)$, есть тождественная подстановка на X, то алгоритм возвращает **False**.

Если же алгоритм возвращает **True**, то это означает, что найдено такое k, что матрица $\widehat{M}^k$ уже была встречена ранее, т. е. найден период и предпериод последовательности $Seq(\widehat{M})$. Следовательно, для каждого элемента из $Seq(\widehat{R})$ мы проверили, что i-й элемент не равен нулю.

В описанном алгоритме происходит определение свойства транзитивности сразу для всех инициальных автоматов, определяемых автоматом A. Если же интерес представляет какое-либо конкретное состояние автомата, тогда имеет смысл использовать вместо всей матрицы $\widehat{M}$ только i-ю строку $\widehat{M}$. Это значительно сокращает количество арифметических операций, требуемых для выполнения одного прохода по 4–8 шагам алгоритма.

3. ОЦЕНКА СЛОЖНОСТИ

После формализации общего хода алгоритма перейдём к уточнению оценки сложности. Как следует из описания, каждый проход алгоритма по 4–8 шагам имеет полиномиальную сложность, так как выполняется умножение матриц фиксированной размерности (относительно количества состояния автомата), а умножение матриц, как известно, имеет полиномиальную сложность.

Следовательно, основным вопросом, на котором стоит остановиться подробнее, является количество проходов алгоритма по шагам 4–8. Оно не превышает числа p^{n^2}. Данная оценка является достаточно грубой и может быть улучшена.

3.1. Экспериментальная оценка

В целях оценки числа требуемых умножений матриц были проведены численные эксперименты. При проведении каждого эксперимента использовался фиксированный класс автоматов, определяемый числом состояний автомата — n и числом входных и выходных символов автомата — p. В ходе экспериментов для каждой из матриц $\widehat{M}$ производилось вычисление количества умножений матриц до останова алгоритма. Результаты экспериментов представлены в таблице. Оказалось, что оценка числа умножений, представленная в лемме 3, не достигается на практике.

Количество матриц $\widehat{M}$ и среднее число умножений до останова алгоритма

p	n	Число матриц $\widehat{M}$	Среднее число умножений до останова алгоритма
2	2	4	1
2	3	64	1.9375
2	4	4096	3.17041
2	5	1048567	4.88959
3	2	9	1.44444
3	3	729	3.631
3	4	531441	7.72993
5	2	25	2.52
5	3	15625	8.61779

3.2. Теоретическая оценка

Обозначим через m_i^k i-ю строку матрицы M^k. На шестом шаге алгоритма производится проверка значения r_i^k. Притом, что

$$r_i^k = (\widehat{m}_{i1}^{k-1} \dots \widehat{m}_{im}^{k-1}) \times \widehat{M} \times V_\sigma^T,$$

т. е. для вычисления r_i^k достаточно знать i-ю строку матрицы $\widehat{M}^{k-1}$. Тогда проверку совпадения $\widehat{M}^k$ с одной из матриц $\widehat{M}, \dots, \widehat{M}^{k-1}$ можно проводить независимо для каждой из строк. Другими словами, достаточно проверять не совпадение матрицы $\widehat{M}^k$ с одной из предыдущих матриц, а совпадение $\widehat{m}_i^k$ со строками $\widehat{m}_i, \widehat{m}_i^2, \dots, \widehat{m}_i^{k-1}$.

Лемма 4. *Максимальное число умножений, требуемое для останова алгоритма, ограниченно сверху числом* p^n.

В таком случае интерес представляют возможные значения i-й строки матриц из $Seq(\widehat{M}^k)$. Пусть $e_i^k(\widehat{M}) = \sum\limits_{j=1}^{n} \widehat{m}_{ij}^k$.

Лемма 5. *Для любой матрицы* $\widehat{M}$ *справедливо, что*

$$e_i^k(\widehat{M}) \bmod p = 0, \quad i \in \overline{1,n}, \quad k > 0. \tag{1}$$

Доказательство. Проведём доказательство по индукции. Для $k = 1$ утверждение леммы справедливо по построению $\widehat{M}$.

Пусть для $\widehat{m}_i^k$ условие леммы выполняется, где $k > 1$.

Рассмотрим $\widehat{m}_i^{k+1} = \widehat{m}_i^k \cdot \widehat{M} \bmod p$. Из определения $\widehat{M}^{k+1}$ и свойств операции умножения матриц получаем, что

$$\widehat{m}_{ij}^{k+1} = (\widehat{m}_{i1}^k \cdot \widehat{m}_{1j} + \widehat{m}_{i2}^k \cdot \widehat{m}_{2j} + \ldots + \widehat{m}_{in}^k \cdot \widehat{m}_{nj}) \bmod p.$$

Выразим $e_i^{k+1}(\widehat{M}) \bmod p$ через $\widehat{m}_i^k$ и $e_1^1(\widehat{M}), \ldots e_n^1(\widehat{M})$:

$$e_i^{k+1}(\widehat{M}) = \sum_{j=1}^{n} \widehat{m}_{ij}^{k+1} =$$

$$= \widehat{m}_{i1}^k \underbrace{(\widehat{m}_{11} + \ldots + \widehat{m}_{1n})}_{e_1^1(\widehat{M})} \bmod p + \ldots + \widehat{m}_{in}^k \underbrace{(\widehat{m}_{n1} + \ldots + \widehat{m}_{nn})}_{e_n^1(\widehat{M})} \bmod p =$$

$$= \sum_{j=1}^{n} \left(\widehat{m}_{ij}^k \cdot e_1^j(\widehat{M}) \bmod p \right).$$

В силу того что для любого $j \in \overline{1,n}$ $e_j^1(\widehat{M}) \bmod p = 0$, имеем $e_i^{k+1}(\widehat{M}) \bmod p = 0$. □

Теорема 2. *Максимальное число умножений матриц, требуемое для останова алгоритма, ограниченно сверху числом* $p^{n-1} - 1$.

Доказательство. Покажем справедливость теоремы по индукции числа состояний автомата.

Следует отметить тот факт, что в силу построения матриц $\widehat{M}$ элементами $Seq(\widehat{M})$ могут быть только матрицы, удовлетворяющие условию (1).

Равенству (1) удовлетворяет только нулевая матрица $\widehat{M}$ для $n = 1$, что соответствует утверждению теоремы. Действительно, нулевой вектор $\widehat{m}_i^k$ даст (в результате умножения $\widehat{M}^k \times V_\sigma^T$) нулевое значение $\widehat{r}_i^k$, что приведёт к останову алгоритма без проверки повтора матрицы.

Пусть для некоторого $n > 1$ условие теоремы справедливо. Покажем, что утверждение теоремы справедливо и для автомата с $n + 1$ состояниями.

Возьмём произвольный вектор $v = (x_1\ x_2\ \ldots\ x_n)$, удовлетворяющий условию (1) и составим вектор $v' = (x_1\ x_2\ \ldots\ ((x_n + p - x_{n+1}) \bmod p)\ x_{n+1}), x_{n+1} \in \{0, 1, \ldots, p-1\}$ путём добавления $(n+1)$-го элемента. Тогда справедливо, что $x_i \in \{0, \ldots, p-1\}$, где $i \in \overline{1, n+1}$.

Заметим, что имеет смысл рассмотрение только одного варианта добавления элемента (с точки зрения позиции добавления), так как в силу произвола выбора v данным способом можно получить все возможные вектора длины $n+1$, удовлетворяющие условию (1).

Покажем, что сумма элементов v' кратна p.

Пусть $x_n + (p - x_{n+1}) < p$, тогда $\sum\limits_{i=1}^{n+1} x'_i = p + \sum\limits_{i=1}^{n} x_i$. Следовательно, сумма элементов v' кратна p.

Пусть $x_n + (p - x_{n+1}) \geqslant p$. Тогда

$$\begin{gathered}((x_n + p - x_{n+1}) \bmod p + x_{n+1} (\bmod p)) \bmod p = \\ = (x_n + (p - x_{n+1}) + x_{n+1}) \bmod p = x_n.\end{gathered}$$

Следовательно, сумма элементов вектора v' равна сумме элементов вектора v.

Таким образом, перебирая все p^{n-1} (включая нулевой) векторов v, получаем, что для каждого вектора имеется ровно p вариантов расширения длины. Тогда количество различных векторов v' равняется p^n, что при вычитании нулевого вектора удовлетворяет условию теоремы. □

Полученная в теореме 2 оценка числа умножений была достигнута на практике и является точной верхней границей количества умножений.

ЗАКЛЮЧЕНИЕ

Представленный в статье алгоритм, несмотря на его экспоненциальную сложность, может представлять практический интерес с той точки зрения, что его трудоёмкость не зависит от длины входных слов. Следовательно, представленный алгоритм можно с успехом применять для проверки транзитивности автоматного отображения в случаях, когда входные слова могут иметь значительные длины или когда заранее не известны требуемые длины входных слов.

Библиографический список

1. *Григорчук Р. И., Некрашевич В. В., Сущанский В. И.* Автоматы, динамические системы и группы // Динамические системы, автоматы и бесконечные группы : сб. ст. Тр. МИАН. Т. 231. М. : Наука, 2000. С. 134–214.
2. *Тяпаев Л. Б.* Транзитивные семейства автоматных отображений // Дискретные модели в теории управляющих систем : тр. IX Междунар. конф. (Москва и Подмосковье, 20–22 мая 2015 г.); отв. ред. В. Б. Алексеев, Д. С. Романов, Б. Р. Данилов. М. : МАКС Пресс, 2015. С. 244–247.
3. *Туараев L. B.* Transitive families and measure-preservind an N-unit delay mappings // Компьютерные науки и информационные технологии : материалы Междунар. науч. конф. Саратов : Издат. центр «Наука», 2016. С. 425–429.
4. *Гилл А.* Введение в теорию конечных автоматов. М. : Наука, 1966. 272 с.
5. *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.
6. *Яблонский С. В.* Введение в дискретную математику : учеб. пособие для вузов. М. : Наука ; Гл. ред. физ.-мат. лит., 1986. 384 с.
7. *Калужин Л. А., Сущанский В. И.* Преобразования и перестановки : пер. с укр. М. : Наука ; Гл. ред. физ.-мат. лит., 1985. 160 с.

8. *Алешин С. В.* Конечные автоматы и проблема Бернсайда о периодических группах // Матем. заметки. 1972. Т. 11, № 3. С. 319–328.

Образец для цитирования:
Карандашов М. В. Алгоритм проверки транзитивности отображений, ассоциированных с конечными автоматами из групп AS_p // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2017. Т. 17, вып. 1. С. 85–95. DOI: 10.18500/1816-9791-2017-17-1-85-95.

The Algorithm for Checking Transitivity of Mappings Associated with the Finite State Machines from the Groups AS_p

M. V. Karandashov

Maksim V. Karandashov, Saratov State University, 83, Astrakhanskaya str., 410012, Saratov, Russia, norg113@gmail.com

The paper deals with a question of determining the property of transitivity for mappings defined by finite automata. A criterion of transitivity for mappings defined by finite automata on the words of finite length in terms of finite automata and trees of deterministic functions is presented. It is shown that for finite automata from groups AS_p an algorithm can be constructed for checking transitivity. To prove this fact some properties of Abelian groups of permutations are used. Based on these results a matrix algorithm is constructed for checking transitivity of mappings associated with initial automata from groups AS_p. The special feature of this algorithm is its independence from lengths of the considered words. Results of numerical experiments and the upper bound of complexity of the algorithm are presented.

Key words: finite state machine, transitivity, automata mapping, AS_p groups.

References

1. Grigorchuk R. I., Nekrashevych V. V., Sushchanskii V. I. Automata, Dynamical Systems and Groups. *Proc. Steklov Inst. Math.*, 2000, vol. 231, pp. 128–203 (in Russian).
2. Tyapaev L. B. Tranzitivnye semejstva avtomatnykh otobrazhenij [Transitive family automaton mappings]. *Komp'iuternye nauki i informatsionnye tekhnologii : materialy Mezhdunar. nauch. konf.* [Computer Science and Information Technologies : Proc. Intern. Sci. Conf.]. Saratov, Publ. center "Nauka", 2014, pp. 244–247 (in Russian).
3. Tyapaev L. B. Transitive families and measure-preservind an N-unit delay mappings. *Komp'iuternye nauki i informatsionnye tekhnologii : materialy Mezhdunar. nauch. konf.* [Computer Science and Information Technologies : Proc. Intern. Sci. Conf.]. Saratov, Publ. Center "Nauka", 2016, pp. 425–429. (in Russian).
4. Gill A. *Introduction to the theory of finite-state machines*. New York, Toronto, Ontario, London, McGraw-Hill Book Co., Inc., 1962. 207 p. (Russ. ed. : Gill A. *Vvedenie v teoriiu konechnykh avtomatov*. Moscow, Nauka, 1966. 272 p.)
5. Karandashov M. V. Issledovanie biektivnykh avtomatnykh otobrazhenii na kol'tse vychetov po moduliu 2^k [Research bijective automaton mappings on the ring of residues modulo 2^k]. *Komp'iuternye nauki i informatsionnye tekhnologii : materialy Mezhdunar. nauch. konf.* [Computer Science and Information Technologies : Proc. Intern. Sci. Conf.]. Saratov, Publ. Center "Nauka", 2014, pp. 148–152 (in Russian).

6. Yablonsky S. V. *Vvedenie v diskretnuiu matematiku : Ucheb. posobie dlia vuzov* [Introduction to Discrete Mathematics : Textbook. manual for schools]. Moscow, Nauka, 1986. 384 p. (in Russian).
7. Kaluzhin L. A., Sushchanskii V. I. *Preobrazovaniia i perestanovki: Per. s ukr.* [Transformations and permutations : Trans. RBM]. Moscow, Nauka, 1985. 160 p. (in Russian).
8. Aleshin S. V. Finite automata and Burnside's problem for periodic groups. *Math. Notes*, 1972, vol. 11, iss. 3, pp. 199–203. DOI: 10.1007/BF01098526.

Cite this article as:
Karandashov M. V. The Algorithm for Checking Transitivity of Mappings Associated with the Finite State Machines from the Groups AS_p. *Izv. Saratov Univ. (N. S.), Ser. Math. Mech. Inform.*, 2017, vol. 17, iss. 1, pp. 85–95 (in Russian). DOI: 10.18500/1816-9791-2017-17-1-85-95.