



## ИНФОРМАТИКА

УДК 519.713

### КРИТЕРИИ УНИВЕРСАЛЬНОСТИ КОНЕЧНОГО ДЕТЕРМИНИРОВАННОГО АВТОМАТА ДЛЯ КЛАССА КДА БЕЗ ПОТЕРИ ИНФОРМАЦИИ

**Н.С. Вагарина**

Саратовский государственный университет,  
кафедра теоретических основ информатики и информационных технологий  
E-mail: vagarinans@info.sgu.ru

Конечный детерминированный автомат является одной из наиболее используемых математических моделей при описании сложных систем дискретного типа.

Традиционно поведение моделируемых объектов рассматривается с преобразовательной точки зрения, то есть изучается механизм преобразования входных последовательностей (воздействий) в выходные (реакции). Однако для получения полного и всестороннего представления о функциональных возможностях системы полезно рассматривать и другой подход – если описанием автомата (как формальной модели системы) является множество выходных последовательностей, которые он генерирует, то говорят о перечислительной форме поведения автомата.

В данной статье исследуются возможности применения базисных множеств групп автоматных преобразований при решении задачи организации перехода от автомата-преобразователя к автомату-перечислителю и предлагается подход к решению задачи организации целенаправленного поведения в классе дискретных систем, описываемых взаимнооднозначными преобразованиями (системы без потери информации).

Основным результатом данной работы является нахождение вида автоматных подстановок и условий универсальности автомата для класса моделируемых систем без потери информации, что представляет теоретический интерес и может быть полезным с практической точки зрения при решении задач восстановления поведения сложных систем.

#### **Criteria of universality Finite determined machine for machines without loss of informing class**

**N.S. Vagarina**

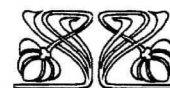
Finite determined machine is one of the most popular mathematical models of complex discrete systems. In this article possibilities of the application generable set of automate transformation groups are investigated. It is considered relatively to the decision of denumerability problem.

Approach to a organization goal-directed behavior problem decision in class of complex discrete systems described by one-to-one transformations (without loss of information) is offer in this scientific work.

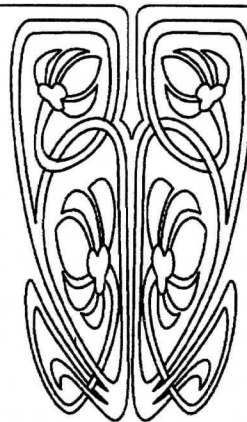
The main result of this work is definition the form of automate substitutions and conditions of automate universality for complex systems without loss of information.

#### **Введение**

В современных условиях развития и усложнения областей приложения технической диагностики необходим поиск новых способов восстановления поведения технических объектов. В широком смысле восстановление поведения означает возврат объекта к реализации заданного функционирования после возникновения, обнаружения и локализации неисправности без физического устранения



**НАУЧНЫЙ  
ОТДЕЛ**





дефекта. Традиционным подходом здесь является предположение о наличии структурной избыточности в рассматриваемых технических системах. Результаты, приведенные в данной статье, были получены в рамках альтернативного подхода, заключающегося в попытке восстановить правильное функционирование за счет использования только поведенческих свойств и особенностей объекта.

Содержательная постановка задачи восстановления поведения дискретных систем с памятью выглядит следующим образом. Реальное поведение системы отличается от заданного, определено текущее поведение, требуется:

- 1) определить возможность восстановления исходного поведения;
- 2) найти совокупность преобразований системы, позволяющих восстановить исходное поведение;
- 3) среди всех возможных преобразований, исходя из заданных ограничений, выбрать допустимое, желательно оптимальное.

Фундаментальной основой для решения задачи восстановления поведения служит теория универсальных автоматов. Универсальный автомат описывает поведение устройства, способного настраиваться на моделирование законов функционирования автоматов из некоторого семейства. В терминах универсальных автоматов основные задачи теории восстановления поведения конечных детерминированных автоматов (КДА) выглядят следующим образом.

Пусть задан конечный детерминированный автомат  $A$  и класс возможных неисправностей  $I$ . Каждой неисправности  $i \in I$  сопоставим конечный детерминированный автомат  $A_i$ . Таким образом, задано семейство  $\{A_i\}$ ,  $i \in I$  (класс возможных неисправностей). Можно выделить следующие задачи восстановления поведения.

**Задача 1** (*возможность восстановления поведения относительно заданного класса неисправностей*).

Для каждого конечного детерминированного автомата  $A_i$ ,  $i \in I$  проверить, является ли он универсальным для  $A$ , то есть проверить справедливость утверждения

$$A_i \in UnA, i \in I,$$

где  $UnA$  — множество всех универсальных автоматов для  $A$ .

**Задача 2** (*конструирование метода восстановления поведения относительно заданного класса неисправностей*).

Для каждого автомата  $A_i$ ,  $i \in I$ , построить множество отображений  $\{\varphi_j\}$ ,  $i \in I$ , таких, что  $\varphi_j(A) = A_i$ ,  $j \in I$ ,  $i \in I$ .

**Задача 3** (*выбор решения задачи восстановления поведения*).

Для каждого множества отображений  $\{\varphi_{ij}\}$ ,  $i \in I$  выбрать допустимое, желательно оптимальное  $\varphi$ .

Задача построения универсального автомата относительно произвольного семейства КДА алгоритмически неразрешима. Однако задача построения универсального конечного детерминированного автомата относительно конечного семейства конечных детерминированных автоматов алгоритмически разрешима. Таким образом, возможность восстановления поведения относительно заданного класса неисправностей предполагает нахождение критерия возможности синтеза универсального автомата для заданного класса. Решение задачи синтеза — универсальный автомат. С содержательной точки зрения он способен заменить любой автомат заданного класса при возникновении неисправностей.

Критерии, приведенные в статье, определяют вид пары автоматных подстановок, образующих функцию переходов автомата, универсального для класса конечных детерминированных автоматов без потери информации.



## 1. Основные понятия и определения

Пусть дан автомат  $M = (S, X, Y, \delta, \lambda)$ . Обозначим его внутренние состояния символами от 0 до  $n-1$ , то есть  $S = \{0, \dots, n-1\}$ . При фиксированном  $x \in X$  функцию переходов  $\delta$  данного автомата можно полагать как объединение подстановок вида

$$\delta_x = \begin{pmatrix} s_0 & \dots & s_{n-1} \\ s_{i_0} & \dots & s_{i_{n-1}} \end{pmatrix}, \text{ то есть } \delta = \{\delta_x\}, x \in X. \quad (1)$$

Всевозможные подстановки на множестве  $S$ , представимые в виде  $\delta_x(s) = \delta(s, x)$ , где  $x \in X^*$ , являются элементами полугруппы автомата  $M$ . В качестве умножения подстановок выступает их последовательное применение, нейтральным элементом является тождественная подстановка.

В этом случае множество  $\{\delta_x\}, x \in X$ , является порождающим множеством полугруппы преобразований  $G_M$  автомата  $M$ . Исследование поведения автомата  $M$  так или иначе связано с изучением элементов полугруппы  $G_M$ .

В теории автоматов рассмотрение различных отношений между последовательностями входных и выходных сигналов приводит к возможности выделения нескольких типов поведения КДА. Будем рассматривать конечный детерминированный автомат  $M$  как перечислитель.

Возможность восстановления поведения относительно заданного класса неисправностей предполагает нахождение критерия возможности синтеза универсального автомата для заданного класса. Решение задачи синтеза — универсальный автомат — с содержательной точки зрения способен заменить любой автомат заданного класса при возникновении неисправностей.

В данной работе рассматривается класс систем, описываемых взаимнооднозначными преобразованиями (системы без потери информации). В этом случае полугруппа автоматных преобразований становится группой.

Конечный детерминированный автомат  $M$  называется автоматом без потери информации, если для каждого состояния  $s \in S$  функция  $\lambda_s(x) = \lambda(s, x)$  определяет взаимно однозначное отображение множества  $X$  на множество  $Y$ . Автоматы без потери информации имеют следующее свойство: при заданном начальном состоянии по выходной последовательности можно всегда определить входную последовательность.

Введем несколько обозначений:

1. Пусть  $\mathfrak{T}_n$  — класс автоматов с  $n$  состояниями, моделирующих поведение систем без потери информации.

2. Пусть  $\mathfrak{T}'_n$  — подкласс автоматов из  $\mathfrak{T}_n$  таких, что их функция переходов реализуется только четными автоматными подстановками.

3. Пусть дана автоматная подстановка  $\delta_1 = \begin{pmatrix} 0 & 1 \dots & n-1 \\ 1 & 2 \dots & 1 \end{pmatrix}$ , являющаяся циклом,  $i_1$  и  $i_2$  — но-

мера двух различных состояний из этого цикла. Обозначим  $\overline{i_1 i_2}$  и назовем расстоянием между состояниями  $s_{i_1}$  и  $s_{i_2}$  в исходном цикле наименьшее целое число между 0 и  $n-2$ , такое, что  $i_1 + \overline{i_1 i_2} \equiv i_2 \pmod{(n)}$ .

Более общий случай: пусть  $k \geq 1, m_1, m_2, \dots, m_k$  — последовательность из  $k$  целых чисел, таких, что  $1 \leq m_1 \leq m_2 \leq \dots \leq m_k$  и по крайней мере одно из чисел  $m_{i+1} - m_i$  ( $i = 0, \dots, k-1, m_0 = 0$ )

больше 1. Пусть  $\delta_1 = \begin{pmatrix} 0 & 1 \dots & m_1 \\ 1 & 2 \dots & 0 \end{pmatrix} \begin{pmatrix} m_1 + 1 \dots & m_2 \\ m_1 + 2 \dots & m_1 + 1 \end{pmatrix} \begin{pmatrix} m_{k-1} + 1 \dots & m_k \\ m_{k-1} + 2 \dots & m_{k-1} + 1 \end{pmatrix}$  — автоматная подстановка



и пусть  $C = \left( \begin{matrix} m_i + 1 \dots m_{i+1} \\ m_i + 2 \dots m_i + 1 \end{matrix} \right)$ ,  $0 \leq i \leq k-1$  — какой-либо цикл порядка больше 1 в ней. Пусть  $i_1$  и

$i_2$  — номера двух различных состояний из цикла  $C$ . Назовем расстоянием и обозначим  $\overline{i_1 i_2}$  наименьшее положительное целое число, такое, что  $i_1 + \overline{i_1 i_2} \equiv i_2 \pmod{(m_{i+1} - m_i)}$ .

Иными словами, считаем «расстоянием между состояниями» в автоматной подстановке, являющейся циклом, число шагов в этом цикле, необходимое для перехода КДА из одного рассматриваемого состояния в другое под воздействием входного символа, индуцирующего эту подстановку.

*Пример 1.* Дан конечный детерминированный автомат  $M = (S, X, \delta)$  с множеством входных символов  $X = (x_1, \dots, x_{n-1})$  и множеством состояний  $S = (0, \dots, n-1)$ . Пусть  $n = 5$  и  $\exists i, i \in \{1, \dots,$

$n-1\}$  такое, что  $\delta_{x_i} = \left( \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 0 \end{matrix} \right)$ . Тогда

а) если  $s_1 = 3, s_2 = 5$ , то  $\overline{s_1 s_2} = 2$ ;

б) если  $s_1 = 5, s_2 = 3$ , то  $\overline{s_1 s_2} = 4$ , так как  $5 + 4 = 3 \pmod{6}$ ;

с) если  $s_1 = 5, s_2 = 4$ , то  $\overline{s_1 s_2} = 5$ , так как  $5 + 5 = 4 \pmod{6}$ .

4. Наибольший общий делитель целых чисел  $a_1, a_1, \dots, a_k$  ( $k \geq 2$ ) обозначим через  $D(a_1, a_1, \dots, a_k)$ .

5. Обозначим  $M\mathfrak{S}_n$  симметрическую группу автоматных преобразований автомата  $M$  с  $n$  состояниями.

6. Обозначим  $M\mathfrak{S}'_n$  знакопеременную группу автоматных преобразований автомата  $M$  с  $n$  состояниями.

В дальнейшем примем следующие положения:

1. Так как наблюдаемая выходная реакция является по существу информацией о внутренних изменениях системы и ее состояниях, а неисправности в автоматах — это ошибки в переходах состояний, то без ограничений на общность рассуждений будем рассматривать конечные детерминированные автоматы с  $n$  – состояниями без потери информации с выходным множеством, равным множеству состояний, и функцией выхода, равной функции переходов, т. е.  $M = (S, X, \delta)$ .

2. Для удобства изложения наряду с фразой «функция переходов, реализуемая автоматными подстановками  $\delta_i$  (где  $i$  принадлежит некоторому множеству индексов)» будем применять выражение «функция переходов вида  $\delta_i$ ».

3. Состояния автомата будем отождествлять с их порядковыми номерами.

Итак, пусть дан автомат  $M = (S, X, \delta)$  с множеством состояний  $S = \{0, \dots, n-1\}$ . При фиксированном  $x \in X$  функцию переходов  $\delta$  данного автомата можно считать обобщенной подстановкой вида

$$\delta_x = \left( \begin{matrix} s_0 & \dots & s_{n-1} \\ s_{i_0} & \dots & s_{i_{n-1}} \end{matrix} \right), \text{ то есть } \delta = \{\delta_x\}, x \in X.$$

В этом случае всевозможные подстановки на множестве  $S$ , которые можно представить в виде  $\delta_x(s) = \delta(x, s)$ , где  $x \in X^*$ , являются элементами группы преобразований автомата  $M$ . Множество подстановок  $\{\delta_x\}$ , реализующих функцию переходов автомата  $M$ , является порождающим множеством группы преобразований автомата  $M$ .



Итак, пусть  $M$  – автомат с  $n \geq 3$  состояниями, и подстановки, реализующие его функцию переходов, порождают симметрическую группу преобразований  $MJ_n$  этого автомата степени  $n$  и порядка  $n!$ . Тогда очевидно  $M$  является универсальным для автоматов из класса  $\mathfrak{T}_n$ .

Замечания:

1) поскольку группы автоматных преобразований автоматов из класса  $\mathfrak{T}_n$  транзитивны, то необходимым условием того, чтобы две автоматные подстановки порождали универсальный для автоматов из класса  $\mathfrak{T}_n$  автомат, является их связанность;

2) поскольку группы автоматных преобразований автоматов из класса  $\mathfrak{T}_n$  примитивны, то необходимым условием того, чтобы две автоматные подстановки порождали универсальный для автоматов из класса  $\mathfrak{T}_n$  автомат, является их примитивность.

Приведем без доказательства следующие вспомогательные факты.

**Теорема 1.1.** Пусть дан КДА  $M = (S, X, \delta)$  с множеством состояний  $S = (0, \dots, n-1)$ , где  $n \geq 3$ , и множеством входных символов  $X = (x_0, \dots, x_p)$ ,  $p \geq 1$ . Тогда если  $\exists x_1, x_2$  такие, что

$$\delta_{x_1} = \begin{pmatrix} 0 & 1 \dots n-1 \\ 1 & 2 \dots 0 \end{pmatrix}, \delta_{x_2} = \begin{pmatrix} m & \dots m+k-1 \\ m+1 \dots & m \end{pmatrix},$$

где  $0 < k < n-1$ ,  $0 \leq m \leq n-1$ , и числа большие  $n-1$  берутся по модулю  $n-1$ , то  $M$  является универсальным перечислителем для автоматов из класса  $\mathfrak{T}_n(\mathfrak{T}'_n)$ , если хотя бы одно из чисел  $n, k$  четно (оба нечетны).

**Лемма 1.1.** Пусть дан КДА  $M = (S, X, \delta)$  с множеством состояний  $S = (0, \dots, n-1)$  и множе-

ством входных символов  $X = (x_0, \dots, x_p)$ . Пусть  $\forall x \in X \delta_x = \begin{pmatrix} s_0 \dots s_i \dots s_i' \dots s_i'' \dots s_{n-1} \\ s_0 \dots s_i' \dots s_i'' \dots s_i \dots s_{n-1} \end{pmatrix}$ ,

$i = 1, \dots, k \geq 1$ . Тогда, если множества  $\{s_1, s_1', s_1'', s_2, s_2', s_2'', \dots, s_i, s_i', s_i''\}$  и  $\{s_{i+1}, s_{i+1}', s_{i+1}''\}$  имеют по крайней мере один общий элемент, то  $M$  является универсальным перечислителем для

всех автоматов, множества состояний которых есть  $\{s_i\}_{i=1}^k \cup \{s_i'\}_{i=1}^k \cup \{s_i''\}_{i=1}^k$ .

## 2. Критерии универсальности конечного детерминированного автомата для автоматов без потери информации

**Теорема 2.1.** Пусть дан КДА  $M = (S, X, \delta)$  с множеством состояний  $S = (0, \dots, n-1)$ , где  $n \geq 4$ , множеством входных символов  $X = (x_0, \dots, x_p)$  и три его различных состояния  $s_{i_1}, s_{i_2}, s_{i_3}$ . Необходимым и достаточным условием того, чтобы автомат  $M$  с функцией переходов, реализуемой

подстановками вида  $\delta_1 = \begin{pmatrix} 0 & 1 \dots n-1 \\ 1 & 2 \dots 0 \end{pmatrix}$  и  $\delta_2 = \begin{pmatrix} s_0 \dots s_{i_1} \dots s_{i_2} \dots s_{i_3} \dots s_{n-1} \\ s_0 \dots s_{i_2} \dots s_{i_3} \dots s_{i_1} \dots s_{n-1} \end{pmatrix}$ , был универсальным для

автоматов из класса  $\mathfrak{T}_n$  (если  $n$  – четное) или  $\mathfrak{T}'_n$  (если  $n$  – нечетное), является равенство

$$D(\overline{i_1 i_2}, \overline{i_2 i_3}, n-1) = 1.$$

**Доказательство.** Ограничимся случаем  $i_1 < i_2 < i_3$ . Это всегда можно сделать за счет выбора обозначений. Тогда  $\overline{i_1 i_2} = i_2 - i_1$ ,  $\overline{i_2 i_3} = i_3 - i_2$ .

**Необходимость.** Пусть  $\delta_1$  и  $\delta_2$  реализуют функцию переходов автомата  $M$ , универсального для автоматов из класса  $\mathfrak{T}_n$  (если  $n$  – четное) или  $\mathfrak{T}'_n$  (если  $n$  – нечетное). В этом случае данные автоматные подстановки примитивны, то есть невозможно множество состояний  $\{0, \dots, n-1\}$  представить в виде суммы попарно не пересекающихся множеств  $\{E_i\}$  одинакового порядка



таким образом, чтобы  $\delta_1$  и  $\delta_2$  преобразовывали каждое из этих множеств  $E_i$  в некоторое множество  $E_j$ .

Пусть  $D(i_2 - i_1, i_3 - i_2, n-1) = r > 1$ ,  $i_2 - i_1 = kr$ ,  $i_3 - i_2 = r$ ,  $n \equiv n'r$  и пусть  $M_j = \{j, j+r, j+2r, \dots, j+(n'-1)r\}$ ,  $j = 0, \dots, r$ .

Автоматная подстановка  $\delta_1$  преобразует все множества  $M_j$  в  $M_{j+1}$  (где  $j+1$  надо заменить на 0, если  $j=r$ ).

Функция переходов, выраженная подстановкой  $\delta_2$ , преобразует все множества  $M_j$  в себя. Таким образом, получили, что  $\delta_1$  и  $\delta_2$  примитивны, то есть пришли к противоречию.

**Достаточность.** Пусть выполнено условие теоремы. Предположим сначала, что  $i_2 - i_1 = i_3 - i_2 = k$ . Если  $k=1$ , то теорема верна в силу теоремы 1.1. Пусть  $k > 1$ . Тогда  $k$  взаимно просто с  $n-1$ . Следовательно, существует целое число  $m$  такое, что  $mk \equiv 1 \pmod{(n-1)}$ . В этом случае

$$\delta_2 = \begin{pmatrix} s_i & s_i + k & s_i + 2k \\ s_i + k & s_i + 2k & s_i \end{pmatrix}.$$

Рассмотрим автоматные подстановки следующего вида:  $t_j = \delta_1^{jk} \delta_2 \delta_1^{-jk}$ ,  $j = 1, 2, \dots, 2m-2$ .

Получим:

$$t_{m-2} = \begin{pmatrix} s_i + (m-2)k & s_i + (m-1)k & s_i + mk \\ s_i + (m-1)k & s_i + mk & s_i + (m-2)k \end{pmatrix},$$

$$t_{2m-2} = \begin{pmatrix} s_i + (2m-2)k & s_i + (2m-1)k & s_i + 2mk \\ s_i + (2m-1)k & s_i + 2mk & s_i + (2m-2)k \end{pmatrix}.$$

Здесь числа большие  $n-1$  берутся по  $\text{mod}(n-1)$ . В силу сказанного выше  $s_i + mk \equiv s_i + 1 \pmod{(n-1)}$ ,  $s_i + 2mk \equiv s_i + 2 \pmod{(n-1)}$  и в силу леммы 1.1 автоматные подстановки  $\delta_2, t_1, \dots, t_{2m-2}$  — функция переходов универсального перечислителя для тех автоматов из  $\mathfrak{T}'_n$ , у которых множества состояний содержат только те состояния, которые данные автоматные подстановки пере-

ставляют. А следовательно, они порождают и подстановку  $\begin{pmatrix} s_i & s_i + 1 & s_i + 2 \\ s_i + 1 & s_i + 2 & s_i \end{pmatrix}$ , которая вместе

с  $\delta_1$  в силу теоремы 1.1 дает функцию переходов универсального перечислителя для автоматов из класса  $\mathfrak{T}_n$  (если  $n$  — четное) или  $\mathfrak{T}'_n$  (если  $n$  — нечетное). Это же относится и к  $\delta_1$  и  $\delta_2$ .

Предположим теперь, что  $i_2 - i_1 \neq i_3 - i_2$ . Пусть  $D(i_2 - i_1, i_3 - i_2) = r \geq 1$ . Так как  $D(i_2 - i_1, i_3 - i_2, n-1) = 1$ , то  $D(r, n-1) = 1$ . Имеем, что  $D(i_2 - i_1, i_3 - i_2) = D(i_2 - i_1, i_3 - i_1) = r$ , и в

силу леммы 7  $\begin{pmatrix} s_i & s_i + r & s_i + 2r \\ s_i + r & s_i + 2r & s_i \end{pmatrix}$  может быть получена из  $\delta_1$  и  $\delta_2$ . Так как  $r$  взаимно просто

с  $n$ , то  $\begin{pmatrix} s_i & s_i + r & s_i + 2r \\ s_i + r & s_i + 2r & s_i \end{pmatrix}$  вместе с  $\delta_1$  дают функцию переходов универсального перечис-

лителя для автоматов из  $\mathfrak{T}_n$  (если  $n$  — четное) или  $\mathfrak{T}'_n$  (если  $n$  — нечетное). Следовательно, условие достаточно.  $\square$



**Теорема 2.2.** Пусть дан КДА  $M = (S, X, \delta)$  с множеством состояний  $S = (0, \dots, n-1)$ , где  $n \geq 3$  и множеством входных символов  $X = (x_0, \dots, x_p)$ . Пусть  $S_m$  — некоторое состояние автомата  $M$  и  $i_1, i_2$  и  $i_3$  — номера состояний автомата  $M$  такие, что по крайней мере одно из них меньше или равно  $m$  и одно больше  $m$ .

Необходимым и достаточным условием того, чтобы автомат  $M$  с функцией переходов, реализуемой подстановками вида  $\delta_1 = \begin{pmatrix} 0 & 1 \dots S_m \\ 1 & 2 \dots 0 \end{pmatrix} \begin{pmatrix} S_m + 1 \dots n-1 \\ S_m + 2 \dots S_m + 1 \end{pmatrix}$  и  $\delta_2 = \begin{pmatrix} S_0 \dots S_{i_1} \dots S_{i_2} \dots S_{i_3} \dots S_{n-1} \\ S_0 \dots S_{i_2} \dots S_{i_3} \dots S_{i_1} \dots S_{n-1} \end{pmatrix}$ , был универсальным перечислителем для автоматов из класса  $\mathfrak{T}_n$  (если  $n$  четно) или  $\mathfrak{T}'_n$  (если  $n$  нечетно), является равенство

$$D(m, n-1-m, d) = 1,$$

где  $d$  — абсолютное значение разности номеров тех состояний из  $S_{i_1}, S_{i_2}$  и  $S_{i_3}$ , которые содержатся в одном и том же цикле автоматной подстановки  $\delta_1$ .

**Доказательство.** Ограничимся рассмотрением случая, когда два из трех номеров состояний  $i_1, i_2$  и  $i_3$ , например,  $i_1$  и  $i_2$  не превосходят  $m$ . Кроме того, ограничимся случаем, когда  $i_1 < i_2$ . Тогда имеем  $d = i_2 - i_1$ .

**Необходимость.** Пусть условие не выполняется, то есть  $D(m, n-1-m, d) = k > 1$ . Пусть  $m = m'k, n-1-m = n'k, d = d'k$ . Рассмотрим  $k$  множеств:

$$M_j = \{i_1 + j, i_1 + j + k, \dots, i_1 + j + (m' - 1)k, i_3 + j, i_3 + j + k, \dots, i_3 + j + (n' - 1)k\}, j = 0, \dots, k-1,$$

где числа, предшествующие  $i_3 + j$  должны быть взяты по  $\text{mod } (m)$ , а остальные по  $\text{mod } (n-1-m)$ . Из вида  $\delta_1$  и  $\delta_2$  следует, что  $\delta_1$  преобразует каждое  $M_j$  в  $M_{j+1}$  ( $i = 0, \dots, k-2$ ) и множество  $M_{k-1}$  в  $M_0$ , а  $\delta_2$  преобразует каждое  $M_j$  в себя. То есть  $\delta_1$  и  $\delta_2$  являются по определению непримитивными подстановками. Таким образом, пришли к противоречию.

**Достаточность.** Пусть  $D(m, n-1-m, d) = 1$ .

Допустим сначала, что  $n-1 = m+1$  и, следовательно,  $\delta_1 = \begin{pmatrix} 0 & 1 \dots S_m \\ 1 & 2 \dots 0 \end{pmatrix}$  и  $\delta_2 = \begin{pmatrix} S_{i_1} & S_{i_2} & S_{m+1} \\ S_{i_2} & S_{m+1} & S_{i_1} \end{pmatrix}$ .

Рассмотрим автоматные подстановки вида  $\delta'_i = \delta_1^i \delta_2 \delta_1^{-i} = \begin{pmatrix} S_{i+i} & S_{i_2+i} & S_{m+1} \\ S_{i_2+i} & S_{m+1} & S_{i+i} \end{pmatrix}, i = 0, \dots, m-1$ .

Здесь числа берутся по  $\text{mod } (m)$ . Эти подстановки вместе с  $\delta_2$  переставляют все состояния  $0, \dots, m+1$ , они удовлетворяют условию леммы 1.1 и, следовательно, дают функцию переходов универсального перечислителя для тех автоматов из  $\mathfrak{T}'_n$ , у которых множества состояний содержат состояния  $0, \dots, m+1$ .

Пусть теперь  $n > m+1$ . Пусть  $D(m, d) = k$ . Автоматная подстановка  $\delta' = \begin{pmatrix} S_{i_1} & S_{i_1+k} & S_{i_3} \\ S_{i_1+k} & S_{i_3} & S_{i_1} \end{pmatrix}$

может быть получена суперпозицией  $\delta_1$  и  $\delta_2$ .

Так как  $D(m, n-1-m, d) = 1$ , то  $D(k, n-1-m) = 1$ . Рассмотрим последовательность автоматных подстановок

$$\delta_j = \delta_1^{jk} \delta_2 \delta_1^{-jk} = \begin{pmatrix} S_{i_1+jk} & S_{i_1+(j+1)k} & S_{i_3+jk} \\ S_{i_1+(j+1)k} & S_{i_3+jk} & S_{i_1+jk} \end{pmatrix}, j = 1, \dots, n-m-2.$$



Так как  $k$  и  $n - 1 - m$  взаимно просты, то последовательность  $i_3, i_3 + k, \dots, i_3 + (n - m - 2)k$  содержит все числа из последовательности  $m + 1, \dots, n - 1$ .

Автоматные подстановки  $\delta'$  и  $\delta_j$  в силу леммы 1.1 дают функцию переходов универсального перечислителя для тех автоматов из  $\mathfrak{T}'$ , у которых множества состояний содержат только те состояния, которые данные автоматные подстановки переставляют.

Рассмотрим отдельно два случая.

1.  $n - 1 - m$  – нечетное число ( $\geq 3$ ). Поскольку подстановки  $\delta'$  и  $\delta_j$  удовлетворяют условию леммы 1.1, то мы можем получить автоматные подстановки  $\begin{pmatrix} n-1 & n-2 \dots s_{m+1} \\ n-2 & n-3 \dots n-1 \end{pmatrix}$ , а также

$$\begin{pmatrix} s_i & s_{m+1} & s_{m+2} \\ s_{m+1} & s_{m+2} & s_i \end{pmatrix}, \begin{pmatrix} s_{m+1} & s_{m+2} & s_{m+3} \\ s_{m+2} & s_{m+3} & s_{m+1} \end{pmatrix}, \dots, \begin{pmatrix} s_{n-3} & s_{n-2} & s_{n-1} \\ s_{n-2} & s_{n-1} & s_{n-3} \end{pmatrix}. \quad (*)$$

Но  $\delta_1 \begin{pmatrix} n-1 & n-2 \dots s_{m+1} \\ n-2 & n-3 \dots n-1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \dots s_m \\ 1 & 2 \dots 0 \end{pmatrix}$  и из теоремы 1.1 и рассмотренного случая  $n - 1 = m + 1$

следует, что  $\begin{pmatrix} 0 & 1 \dots s_m \\ 1 & 2 \dots 0 \end{pmatrix}$  вместе с (\*) порождают группу  $M\mathfrak{T}_n$  ( $M\mathfrak{T}'_n$ ), если  $m$  четно (нечетно).

Следовательно, автомат  $M$  с функцией переходов, реализуемой автоматными подстановками  $\delta_1$  и  $\delta_2$ , будет универсальным перечислителем для автоматов из класса  $\mathfrak{T}_n$  ( $\mathfrak{T}'_n$ ), если  $n$  четно (нечетно).

2.  $n - 1 - m$  – четное число ( $\geq 2$ ). В этом случае, поскольку подстановки  $\delta'$  и  $\delta_j$  удовлетворяют условию леммы 1.1, мы можем получить автоматные подстановки  $\begin{pmatrix} s_i & n-1 \dots s_{m+1} \\ n-1 & n-2 \dots s_i \end{pmatrix}$ , а также

$$\begin{pmatrix} s_i & s_{m+1} & s_{m+2} \\ s_{m+1} & s_{m+2} & s_i \end{pmatrix}, \begin{pmatrix} s_{m+1} & s_{m+2} & s_{m+3} \\ s_{m+2} & s_{m+3} & s_{m+1} \end{pmatrix}, \dots, \begin{pmatrix} s_{n-3} & s_{n-2} & s_{n-1} \\ s_{n-2} & s_{n-1} & s_{n-3} \end{pmatrix}. \quad (**)$$

Но автоматная подстановка  $\delta_1 \begin{pmatrix} s_i & n-1 & n-2 \dots s_{m+1} \\ n-1 & n-2 & s_{m+1} \dots s_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \dots s_i & s_{m+1} & s_{i+1} & s_{i+2} \dots s_m \\ 1 & 2 \dots s_{m+1} & s_{i+1} & s_{i+2} & s_{i+3} \dots 0 \end{pmatrix}$

вместе с (\*\*), учитывая случай  $n - 1 = m + 1$ , образуют функцию переходов универсального перечислителя для автоматов из класса  $\mathfrak{T}_n$  ( $\mathfrak{T}'_n$ ), если  $n$  четно (нечетно). Следовательно, то же относится и к  $\delta_1$  и  $\delta_2$ . Достаточность доказана.  $\square$

### Заключение

Основным результатом данной работы является нахождение вида автоматных подстановок и условий универсальности автомата для класса моделируемых систем без потери информации, что представляет теоретический интерес и может быть полезным с практической точки зрения при решении задач восстановления поведения сложных систем. Результаты проведенных исследований позволяют решать важные в практическом плане задачи:





— восстановление правильного функционирования сложных систем, когда невозможно или нецелесообразно немедленное проведение ремонтно-восстановительных мероприятий, а также исключается подключение резервной или дублирующей составляющей или она вышла из строя;

— организация модификации поведения сложных систем без их физического перепроектирования, только за счет использования текущих функциональных возможностей;

— разработка отказоустойчивых систем, использующих весь спектр потенциальных средств для восстановления своего поведения — от традиционного резервирования-дублирования до особенностей с существующего в данный момент времени закона функционирования.

### Библиографический список

1. Алгебраическая теория автоматов, языков и полугрупп / Под ред. М.А. Арбиба; пер. с англ. М., 1975.
2. Богомолов А.М., Сытник А.А., Твердохлебов В.А. Автоматные модели и рекурсивный конструктивизм. Саратов, 1992.
3. Кострикин А.И. Введение в алгебру. М., 1977.
4. Пикар С. О базисах симметрической группы // Кибернетический сборник. 1965. № 1.
5. Сытник А.А. Методы и модели восстановления поведения автоматов // Автоматика и телемеханика. 1992. № 11.
6. Sytnik A.A., Posohina N.I. On some methods of discrete systems behaviour simulation // CASYS'97: The 1st Intern. Conf. on computing anticipatory systems. Liege, 1997.

УДК 519.17

## T-НЕПРИВОДИМЫЕ РАСШИРЕНИЯ ОБЪЕДИНЕНИЙ ПОЛНЫХ ГРАФОВ

С.Г. Курносова

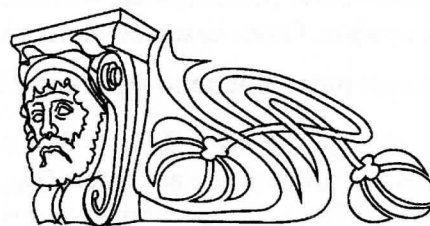
Саратовский государственный университет,  
кафедра теоретических основ компьютерной безопасности  
и криптографии

E-mail: csc@info.sgu.ru

T-неприводимое расширение является одним из видов оптимальных расширений для графов. Конструкции оптимальных расширений применяются в диагностике дискретных систем и криптографии.

Расширением  $n$ -вершинного графа  $G$  называется граф  $H$  с  $n+1$  вершинами такой, что граф  $G$  вкладывается в каждый максимальный подграф графа  $H$ . У любого графа есть тривиальное расширение — соединение  $G+v$  графа  $G$  с одной вершиной. T-неприводимые расширения получаются из тривиального удалением максимального числа ребер, не нарушающим свойство расширения.

Задача нахождения графа по его T-неприводимому расширению имеет линейную сложность, а для задачи отыскания всех T-неприводимых расширений произвольного графа в настоящее время эффективного алгоритма нет. В данной работе предлагается алгоритм построения всех T-неприводимых расширений и оценка их количества для объединений полных графов, каждый из которых имеет не менее одной вершины.



### T-irreducible extensions for unions of complete graphs

S.G. Kurmosova

T-irreducible extension is one of kinds of optimal extensions of graphs. Constructions of optimal extensions are used in diagnosis of discrete systems and in cryptography.

A graph  $H$  with  $n+1$  vertices is called an extension of a graph  $G$  with  $n$  vertices if  $G$  can be embedded in every maximal subgraph of  $H$ . Any graph  $G$  has the trivial extension that is the join  $G+v$  of  $G$  with some outer vertex  $v$ . T-irreducible extensions are obtained from the trivial extension by removal of maximal number of edges in such a way that the extension property is preserved.

The problem of finding of the initial graph from any of its T-irreducible extensions has a linear complexity, but until now there is no efficient algorithm for finding of all T-irreducible extensions of a given graph. Graphs studied in this paper are unions of complete graphs each of which has more than one vertex. An algorithm of construction of all T-irreducible extensions for such graphs is presented. Also an estimate of a total amount of the resulting extensions is made.