

Math-Net.Ru

Общероссийский математический портал

В. И. Малыгин, Операция обратной связи и класс группо-  
вых автоматов,  
*Дискрет. матем.*, 1990, том 2, выпуск 3, 81–89

<https://www.mathnet.ru/dm870>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением  
<https://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.97.14.88

23 апреля 2025 г., 14:56:48



УДК 519.7

## ОПЕРАЦИЯ ОБРАТНОЙ СВЯЗИ И КЛАСС ГРУППОВЫХ АВТОМАТОВ

В. И. Малыгин

В работе изучается вопрос о том, что будет с внутренней группой автомата при применении операции обратной связи при условии, что каждое применение этой операции не выводит автомат из класса групповых автоматов. Основной результат работы состоит в том, что если внутренняя группа автомата отлична от циклической группы простого порядка, то существует автомат для этой группы такой, что примененная достаточное число раз операция обратной связи дает автомат с любой подгруппой полной симметрической группы для этого данного числа состояний. Наряду с этим исследуется вопрос об изменении группы автомата при однократном применении операции обратной связи.

Операция обратной связи наряду с операцией суперпозиции играет фундаментальную роль в задачах декомпозиции автоматов. В настоящее время наиболее изученной является операция суперпозиции и тесно связанный с ней класс групповых автоматов, замкнутый относительно этой операции [1, 2].

Операция обратной связи, будучи примененной к автомату, может вывести его из класса групповых автоматов. В настоящей работе исследуется вопрос о том, что будет с внутренней группой автомата при применении операции обратной связи при условии, что каждое применение этой операции не выводит автомат из класса групповых автоматов. Основной результат состоит в том, что если внутренняя группа автомата отлична от циклической группы простого порядка, то существует такой автомат для этой группы, что примененная достаточное число раз операция обратной связи дает автомат с любой подгруппой полной симметрической группы для этого данного числа состояний (теорема 2). Здесь же изучается вопрос о «локальном» изменении внутренней группы, т. е. вопрос об изменении группы автомата при однократном применении операции обратной связи (теорема 1).

Дадим необходимые определения. Пусть имеется конечный автомат

$$A = (A, Q, B, \varphi, \psi),$$

где  $A = E_2^m$ ,  $Q = E_2^n$ ,  $B = E_2^k$  — декартовы степени множества  $E_2 = \{0, 1\}$ .

Функция переходов  $\varphi$  и функция выходов  $\psi$  определены следующим образом:

$$\begin{aligned}\varphi: E_2^m \times E_2^n &\rightarrow E_2^n, \\ \psi: E_2^m \times E_2^n &\rightarrow E_2^k.\end{aligned}$$

Отображения  $\varphi$  и  $\psi$  рассматриваются как булевские вектор-функции

$$\begin{aligned}\varphi &= (\varphi_1(x_1, \dots, x_m, z_1, \dots, z_n), \dots, \varphi_n(x_1, \dots, x_m, z_1, \dots, z_n)), \\ \psi &= (\psi_1(x_1, \dots, x_m, z_1, \dots, z_n), \dots, \psi_k(x_1, \dots, x_m, z_1, \dots, z_n)).\end{aligned}$$

Пусть  $k$ -я компонента вектор-функции  $\psi$  есть

$$\psi_k(x_1, \dots, x_m, z_1, \dots, z_n)$$

и не зависит существенно от переменной  $x_m$ . Тогда, сопоставив с конечным автоматом  $A$  конечный автомат  $A'$ , получаемый из  $A$  применением операции обратной связи (см. [2, с. 160]), имеем

$$\begin{aligned}A' &= (E_2^{m-1}, E_2^n, E_2^k, (\varphi'_1, \dots, \varphi'_n), (\psi'_1, \dots, \psi'_k)), \\ \varphi'_s &= \varphi(x_1, \dots, x_{m-1}, \psi_k(x_1, \dots, x_{m-1}, z_1, \dots, z_n), z_1, \dots, z_n), s = 1, \dots, n; \\ \psi'_t &= \psi_t(x_1, \dots, x_{m-1}, \psi_k(x_1, \dots, x_{m-1}, z_1, \dots, z_n), z_1, \dots, z_n), t = 1, \dots, k.\end{aligned}\quad (1)$$

В таком случае будем использовать запись  $A \vdash A'$ .

Пусть  $G_A$  — внутренняя группа автомата  $A$ . Будем считать, что операция обратной связи  $A \vdash A'$  допустима, если  $G_A$  является группой перестановок состояний автомата  $A$ .

Определение 1. Скажем, что группа  $G'$  непосредственно трансформируется из группы  $G$  ( $G \vdash G'$ ), если существует автомат  $A$ , который имеет допустимую операцию обратной связи  $A \vdash A'$ , причем для групп  $G_A$ ,  $G$  и  $G_{A'}$ ,  $G$  справедливо следующее:

$$G_A = G, \quad G_{A'} = G'.$$

Скажем, что группа  $G'$  получается трансформацией группы  $G$   $G \vdash G'$ , если автомат  $A$  допускает применение конечного числа раз допустимой операции обратной связи  $A \vdash A'$  так, что  $G_A = G$  и  $G_{A'} = G'$ .

Знак равенства двух групп понимается как совпадение двух групп перестановок в соответствующей симметрической группе.

Определим элемент  $\tilde{x}$  следующим образом:

$$\tilde{x} = (x_1, \dots, x_{m-1}, x_m) \in E_2^m,$$

$S_{\tilde{x}}$  — подстановка  $S_{|Q|}$ , соответствующая  $\tilde{x}$ . Тогда подстановка, соответствующая элементу

$$\tilde{x}' = (x_1, \dots, x_{m-1}) \in E_2^m,$$

получается из двух  $S_{(x', 0)}$  и  $S_{(x', 1)}$ , так как для любого элемента  $\tilde{z} \in Q$ :

$$\varphi'(\tilde{x}', \tilde{z}) = \varphi(\tilde{x}', \psi_k(\tilde{x}', \tilde{z}), \tilde{z}) = \begin{cases} \varphi(\tilde{x}', 0, \tilde{z}) & \text{при } \psi_k(\tilde{x}', \tilde{z}) = 0, \\ \varphi(\tilde{x}', 1, \tilde{z}) & \text{при } \psi_k(\tilde{x}', \tilde{z}) = 1. \end{cases}$$

Определение 2. Операция склеивания  $\otimes$ . Пусть  $x, y$  — элементы симметрической группы  $S_t$ . Определим подмножество  $x \otimes y \subset S_t$  следующим образом:

$$x \otimes y = \{z \in S_t \mid \forall i = 1, \dots, t \quad iz = ix \vee iy\}.$$

Лемма 1. Свойства операции склеивания  $\otimes$ :

- 1)  $\{x, y\} \subset x \otimes y$ ;
- 2)  $x \otimes y = y \otimes x$ .

Утверждение леммы 1 непосредственно следует из определения 2.

Лемма 2. Пусть  $A \vdash A'$ , тогда обратная связь будет допустимой тогда и только тогда, когда для всех элементов  $\tilde{x}' \in E_2^{m-1}$

$$S_{\tilde{x}'} \in S_{\tilde{x}', 0} \otimes S_{\tilde{x}', 1}.$$

Доказательство леммы показано выше.

Пусть теперь выбраны элементы  $x$  и  $y$  из симметрической группы  $S_t$ , причем

$$x = \left( \begin{matrix} 1, \dots, t \\ i_{x,1}, \dots, i_{x,t} \end{matrix} \right), \quad y = \left( \begin{matrix} 1, \dots, t \\ i_{y,1}, \dots, i_{y,t} \end{matrix} \right).$$

Для элементов склейки  $x \otimes y$  запишем возможность выбора:

$$\begin{matrix} 1 & \rightarrow & i_{x,1} \\ & & \rightarrow & i_{y,1} \\ 2 & \rightarrow & i_{x,2} \\ & & \rightarrow & i_{y,2} \\ \cdot & \dots & \cdot \\ t & \rightarrow & i_{x,t} \\ & & \rightarrow & i_{y,t} \end{matrix} \quad (2)$$

Введем отношение эквивалентности  $R$  на множестве пар:  $(i_{x,s}; i_{y,1}) \times \times R (i_{x,q}; i_{y,q})$ , если либо

$$\{i_{x,s}; i_{y,s}\} \cap \{i_{x,q}; i_{y,q}\} \neq \emptyset, \quad (3)$$

либо существует цепочка пар с условием (3), идущая из пары  $(i_{x,s}; i_{y,s})$  к паре  $(i_{x,q}; i_{y,q})$ .

Определение 3. Разбиением склейки  $x \otimes y$  на блоки назовем классы смежности по отношению к эквивалентности  $R$ .

Выберем такую подстановку  $z$ , что  $z \in x \otimes y$ , и стрелку  $pz = i_{q,p}$ , где  $p = \overline{1, t}$ . Скажем, что для числа  $p$  в подстановке  $z$  взята стрелка типа  $g$ , т. е. либо  $g = x$ , либо  $g = y$ .

Лемма 3. Пусть подстановка  $z$  такова, что  $z \in x \otimes y$ , а для чисел  $p$  и  $q$  имеем  $p, q = \overline{1, t}$ . Тогда утверждается, что если стрелки  $pz = i_{g,p}$  и  $qz = i_{g',q}$  принадлежат одному блоку, то для стрелок  $g, g'$  справедливо равенство  $g = g'$ . Выбор типа стрелок для различных блоков независим.

Доказательство. Предположим, что стрелки  $pz = i_{g,p}$  и  $qz = i_{g',q}$  лежат в одном блоке. Пусть для определенности  $pz = i_{x,p}$ . Докажем тогда, что  $g' = x$ . Доказательство ведется по длине цепочки, соединяющей пары  $(i_{x,p}; i_{y,p})$  и  $(i_{x,q}; i_{y,q})$ . Пусть пары  $(i_{x,p}; i_{y,p})$  и  $(i_{x,s}; i_{y,s})$ , где  $s \neq p$ , таковы, что

$$\{i_{x,p}; i_{y,p}\} \cap \{i_{x,s}; i_{y,s}\} = \emptyset.$$

Так как стрелки  $i_{x,p} \neq i_{x,s}$  при  $s = p$ , то либо совпадают стрелки  $i_{x,p}$ ,  $i_{y,s}$ , т. е.  $i_{x,p} = i_{y,s}$ , либо совпадают стрелки  $i_{y,p}$ ,  $i_{x,s}$ , т. е.  $i_{y,p} = i_{x,s}$ . Если  $i_{x,p} = i_{y,s}$ , то  $sz = i_{y,s}$ , поэтому  $sz = i_{x,s}$ . Если  $i_{y,p} = i_{x,s}$ , то, так как элемент  $i_{y,p}$  не выбран в подстановке  $z$  при отображении  $p \rightarrow pz$ , он должен быть выбран при  $sz$ , иначе в подстановке  $z$  он никогда не встретится. Итак, для очередной пары в блоке тип стрелки сохраняется. Ясно, что подмножества состояний  $i = \overline{1, t}$ , отвечающие различным блокам, не пересекаются, поэтому выбор типа стрелок для различных блоков независим. Лемма доказана.

Назовем длиной блока  $B$  количество входящих в него пар, для него будем использовать обозначение  $|B|$ .

Следствие 3.1. Пусть  $B_1, \dots, B_l, B_{l+1}, \dots, B_k$  — разбиение подмножества  $x \otimes y$  на блоки, где длина блоков выражается соотношениями

$$|B_j| > 1 \text{ при } j \leq l, \quad |B_j| = 1 \text{ при } j \geq l+1.$$

Тогда  $|x \otimes y| = 2^l$ .

Доказательство. Каждому блоку длины больше 1 отвечают две возможности различным образом выбрать тип стрелки. При этом будут получаться различные элементы склейки  $x \otimes y$ .

Лемма 4. Склейка  $1 \otimes x$ . Пусть  $1$  — единичный элемент группы  $S_t$ ,  $x = \prod_j c_j$  — разложение элемента  $x$  на циклы, причем длина любого цикла больше единицы, т. е.  $|c_j| > 1$ . Тогда

$$z \in 1 \otimes x \Leftrightarrow z = \prod_j c_j^{\sigma_j},$$

где  $\sigma_j \in \{0, 1\}$  и  $c_j^0 = 1$ ;  $c_j^1 = c_j$ .

Доказательство. Достаточно доказать лемму в случае, когда  $x$  — один цикл. Не ограничивая общности, будем считать, что  $x = \{1, \dots, t\}$ . Имеем следующую склейку:

$$\begin{array}{l} 1 \rightarrow 1 \\ 1 \rightarrow 2 \\ 2 \rightarrow 2 \\ 2 \rightarrow 3 \\ \dots \\ t \rightarrow t \\ t \rightarrow 1 \end{array}$$

Но тогда, очевидно, имеется один блок

$$B_1 = \{(1, 2); (2, 3); (3, 4); \dots; (t, 1)\},$$

и склейка  $1 \otimes x = \{1, x\}$ , что и требовалось доказать.

Лемма 5. Дистрибутивные законы склейки. Для любых элементов  $x, y, z \in S_t$  справедливы следующие равенства:

$$\begin{aligned} (x \otimes y) z &= xz \otimes yz, \\ z(x \otimes y) &= zx \otimes zy. \end{aligned}$$

Доказательство. Докажем сначала предварительную формулу (4) для любых элементов  $x, y \in S_t$

$$(1 \otimes x) y = y \otimes xy. \quad (4)$$

Для элемента  $g \in S_t$  положим

$$g = \left( \begin{array}{c} 1, \dots, t \\ i_{g,1}, \dots, i_{g,t} \end{array} \right).$$

Без ограничения общности можно считать, что  $x$  является циклом, причем

$$x = (1, 2, \dots, q)(q+1) \dots (t).$$

Тогда

$$1 \otimes x = \{1, x\}, \quad (1 \otimes x) y = \{y, xy\},$$

поэтому для доказательства равенства (4) достаточно показать, что в склейке  $y \otimes xy$  имеется не более одного блока с длиной, большей 1. Склейка  $y \otimes xy$  выглядит так:

$$\left. \begin{array}{l} 1 \rightarrow i_{y,1} \\ 1 \rightarrow i_y, i_{x,1} = i_{y,2} \\ \dots \\ q \rightarrow i_{y,q} \\ q \rightarrow i_y, i_{x,q} = i_{y,1} \end{array} \right\} B_1 \text{ один блок}$$

$$\left. \begin{array}{l} q+1 \rightarrow i_{y,q+1} \\ q+1 \rightarrow i_y, q+1 \\ \dots \\ t \rightarrow i_{y,t} \\ t \rightarrow i_y, t \end{array} \right\} \text{блоки длины 1.}$$

Докажем равенства леммы. Из соотношения (4) имеем

$$(1 \otimes yx^{-1})x = x \otimes yxx^{-1} = x \otimes y.$$

Умножим это равенство на элемент  $z$ :

$$(x \otimes y)z = (1 \otimes yx^{-1})xz = xz \otimes yx^{-1}x^{-1}z = xz \otimes yz.$$

Доказательство второй формулы леммы проводится аналогично.

**Теорема 1.** Для любых элементов  $x, y \in S_t$  справедливо представление

$$x \otimes y = x(1 \otimes x^{-1}y) = \left\{ x \prod_j c_j^{\sigma_j}, \sigma_j = 0 \vee 1 \right\},$$

где  $x^{-1}y = \prod_j c_j$  — разложение на циклы элемента  $x^{-1}y$ .

**Доказательство.** Теорема является непосредственным следствием лемм 4 и 5.

Дадим теперь описание множества групп, в которые может трансформироваться внутренняя группа конечного автомата при допустимых операциях обратной связи.

**Теорема 2.** Пусть дана конечная группа перестановок  $R$ .

1. Если  $R \models G$ , то для любой группы  $G'$  такой, что  $G' \subseteq G$ , следует, что  $R \models G'$ .

2. Если  $R$  является транзитивной подгруппой симметрической группы  $S_{|Q|}$  и

- А)  $R = \mathbf{Z}_p$ , где  $p$  — простое число, то либо  $R \models \mathbf{Z}_p$ , либо  $R \models \mathbf{1}$ , где  $\mathbf{1}$  — единичная подгруппа симметрической группы  $S_{|Q|}$ ;
- Б)  $R \neq \mathbf{Z}_p$ , то  $R \models S_{|Q|}$ .

3. Если  $R$  не является транзитивной подгруппой, то любая трансформация группы есть подгруппа прямого произведения трансформаций из транзитивных компонент  $R$ .

В доказательстве теоремы 2 разберем теоретико-групповую часть, а затем автоматную. Теорема 1 позволяет описать локальное изменение образующих в группе автомата при однократном применении обратной связи. Новыми образующими являются циклы элементов трансформируемой группы.

**Определение 4.** Скажем, что группа  $G'$  непосредственно выводится из группы перестановок  $G: G \rightarrow G'$ , если

$$G' = \langle Z \mid \exists x, y \in G: z \in x \otimes y \rangle.$$

Скажем, что группа  $G'$  выводится из группы  $G (G \Rightarrow G')$ , если существует цепочка непосредственных выводимостей из группы  $G$  в группу  $G'$ .

**Лемма 6.** Если группа  $G'$  выводится из группы  $G$ , а группа  $G''$  такова, что  $G'' \subseteq G'$ , то группа  $G''$  выводится из группы  $G$ , т. е.  $G \Rightarrow G''$ .

**Доказательство.** Покажем, что группа  $G''$  непосредственно выводится из группы  $G'$ , т. е.  $G' \rightarrow G''$ . В самом деле, рассмотрим все склейки вида  $1 \otimes g$ , где  $g' \in G'$ . Положим

$$\theta_{G''}(1 \otimes g') = \begin{cases} 1, & \text{если } g' \in G', \\ g', & \text{если } g' \in G''. \end{cases}$$

Тогда  $G'' = \langle \theta_{G''}(1 \otimes g'), g' \in G' \rangle$ .

**Лемма 7.** Пусть имеются группы  $G, G'$  такие, что  $G \rightarrow G'$ , причем  $G = \langle g \rangle$ ,  $G' = \langle c \rangle$  и  $\tau = \prod_{j=1}^m c_j \in G'$ . Тогда элемент  $\tau$  может быть получен из не более чем  $m$  склеек элементов группы  $G$ .

Доказательство. Для любого элемента  $c_j$  существует такой элемент  $g_j$ , что  $c_j \in 1 \otimes g_j$ . Тогда

$$\tau \in \prod_{j=1}^m (1 \otimes g_j).$$

Теперь каковы бы ни были элементы  $g_1, \dots, g_4$  из группы  $G$ , утверждение леммы вытекает из следующей цепочки формул и леммы 5:

$$(g_1 \otimes g_2) (g_3 \otimes g_4) = (g_1 (g_3 \otimes g_4)) \otimes (g_2 (g_3 \otimes g_4)) = (g_1 g_3 \otimes g_1 g_4) \otimes (g_2 g_3 \otimes g_2 g_4).$$

Лемма 8. Выводимость из циклических групп. Пусть дана циклическая группа  $Z_n$  порядка  $n$ ,  $x = (1, \dots, n)$  — ее стандартная образующая. Тогда утверждается:

- а) если  $n = p$ , где  $p$  — простое число, тогда либо  $Z_p \Rightarrow Z_p$ , либо  $Z_p \Rightarrow 1$ ;  
 б) если  $n$  является составным числом, тогда  $Z_n \Rightarrow S_n$ .

Доказательство.

а) Если  $n = p$ , тогда  $Z_p = \{1, x, \dots, x^{p-1}\}$ , причем все  $x^k$  являются циклами. Следовательно, для любого элемента  $g \in Z_p$  склейка  $1 \otimes g = \{1, g\}$ , откуда следует утверждение пункта а).

б) Пусть  $n = p_1 p_2$ ;  $p_1 > 1$ ,  $p_2 > 1$ . Покажем, что выводимы следующие элементы из группы  $S_n$ :

$$T_i = (i, i+1, i+2, \dots, i+p_1-1), \quad \text{где } i = 1, 2, \dots, n-p+1.$$

Получим сначала подстановку  $T_1 = (1, 2, \dots, p_1)$ ,

$$x^{p_1} = (1, 1+p_1, \dots, 1+(p_2-1)p_1) \dots (p_1, 2p_1, \dots, p_1 p_2) = z_1 z_2 \dots z_{p_1}.$$

Это есть разложение на циклы. Но тогда

$$xz_1^{-1} = (1, \dots, p_1) \omega_2 \dots \omega_{p_2}$$

— разложение на циклы, т. е.

$$T_1 \in 1 \otimes xz_1^{-1} \subset 1 \otimes [x(1 \otimes x^{-p_1})].$$

Таким образом, элемент  $T_1$  выводим. Выводимость подстановок  $T_i$ , где  $i > 1$ , получается аналогично. Нужно только записать цикл

$$x = (i, i+1, \dots, i-1)$$

и провести перенумерацию

$$1' \leftrightarrow i, 2' \leftrightarrow i+1, \dots, n' \leftrightarrow i-1,$$

вывести подстановку  $T_1$  и провести обратную перенумерацию.

Воспользуемся теперь одной леммой С. Пикар (см. [4], лемма 3). Каковы бы ни были числа  $n, k$ , причем  $n \geq 3$ ,  $2 \leq k \leq n$ , подстановки  $T_i = (i, i+1, \dots, i+k-1)$ , где  $i = 1, \dots, n-k+1$ , порождают группу  $S_n(A_n)$ , если  $k$  — четно (нечетно). Итак, в силу леммы можно вывести, по крайней мере, группу  $A_n$  и, следовательно, подстановку  $(i, j)(k, l)$  из  $A_n$  для любых  $i, j, k, l$  таких, что  $1 \leq i, j, k, l \leq n$ . Поэтому можно вывести любую транспозицию  $(i, j)$  из группы  $S_n$  и, следовательно, всю группу  $S_n$ .

Лемма 9. Пусть даны группы

$$Q' = \{i_1, \dots, i_t\}, \quad Q'' = \{i_1, \dots, i_t\}$$

такие, что  $Q' \not\subseteq Q''$  и  $Q' \cap Q'' \neq \emptyset$ . Пусть  $c = (i_1, \dots, i_t)$  — цикл, а  $S_t$  — множество подстановок группы  $Q'$ , и  $S_t \subseteq S_{1 \cup Q' \cup Q''}$ . Тогда

$$S_{1 \cup Q' \cup Q''} = \langle S_t, c \rangle.$$

Доказательство. Из условия леммы следует, что  $|Q'| \geq 2$ , причем существуют такие элементы  $j_{k_1}, j_{k_2}$ , что

$$j_{k_1} \in Q' \setminus Q'', \quad j_{k_2} \in Q'' \cap Q'.$$

Без ограничения общности можно считать, что цикл  $c$  есть  $c = (2, \dots, l+1)$ , где  $j_{k_1} = 1, j_{k_2} = 2$ . Транспозиция  $x = (1, 2)$  принадлежит множеству подстановок  $S_t$ , тогда

$$c^{-k-2}xc^{k-2} = (1, k), \quad k = \overline{2, l+1},$$

поэтому для любого элемента  $q_1 \in Q' \cup Q''$  транспозиция

$$(1, q) \in \langle S_t, c \rangle,$$

откуда следует утверждение леммы.

*Лемма 10.* Пусть дана транзитивная группа  $G$  из множества  $S_t$ , причем  $G \not\Rightarrow S_t$ . Тогда  $G = Z_t$  и  $t$  является простым числом.

*Доказательство.* Пусть  $x$  есть цикл максимальной длины, выводимый из группы  $G$ . Покажем, что  $|x| = t$ . Отсюда будет следовать, что  $t$  является простым числом (иначе бы была выводимость группы  $S_t$ ). Допустим, что  $|x| < t$ . Тогда, в силу транзитивности группы  $G$ , существует выводимый из  $G$  цикл  $y$ :

$$\{x\} \cap \{y\} = \emptyset, \quad \{y\} \subseteq \{x\}.$$

С точностью до перенумерации возможны следующие два случая:

$$1^\circ. |\{x\} \cap \{y\}| = 1, \quad x = (1, \dots, p), \quad y = (p, p+1, \dots, q), \quad \text{но тогда}$$

$$xy = (1, \dots, p-1, p+1, \dots, q, p)$$

— цикл длины, большей, чем  $x$ , что невозможно.

$$2^\circ. |\{x\} \cap \{y\}| > 1, \quad x = (1, \dots, p). \quad \text{Цикл } y \text{ имеет вид}$$

$$y = (\dots, i_1, s_1, \dots, s_\tau, i_2, \dots),$$

где  $i_1, i_2 \in \{1, \dots, p\}$ , а  $s_j > p$  для всех  $j = \overline{1, \tau}$ . Тогда существует такое число  $k$ , что

$$x^k = (i_1, i_2, \dots),$$

где, возможно,  $x^k$  содержит несколько циклов. Но тогда элемент  $y^{-1}x^k$  содержит цикл  $(i_2, s_\tau, s_{\tau-1}, \dots, s_1)$ , и для этого цикла выполнены условия пункта 1°.

Полученное противоречие доказывает равенство  $|x| = t = p$ , где  $p$  — простое число. С точностью до перенумерации можно считать, что  $x = (1, 2, \dots, p)$ . Допустим, возможен вывод цикла  $y$  меньшей длины:

$$y = (1, s_1, \dots, s_\tau, \dots, l),$$

где  $s_j < l$  при  $j = \overline{1, \tau}$ . Но тогда

$$xy^{-1} = (l, l+1, \dots, t) \prod_s c'_s,$$

т. е. выводим цикл  $(l, l+1, \dots, p)$ . Сравнивая циклы

$$x = (p, p-1, \dots, l, l-1, \dots, 1), \quad z = (p, \dots, l+1, l),$$

аналогично выводу цикла  $z$ , можно получить элемент  $w = (1, \dots, l)$ . Но тогда

$$z^{-1}wz = (1, 2, \dots, l, p),$$

и по той же лемме С. Пикар выводима группа четных подстановок  $A_{l+1}$  множества  $(1, 2, \dots, l, p)$ . Если  $l > 2$ , то  $l+1 > 3$ , и, следовательно, в группе  $A_{l+1}$  есть произведение двух транспозиций. Значит, выводима одна транспозиция. Если  $l = 2$ , то в качестве транспозиции можно взять элемент  $w$ . Без ограничения общности можно считать, что выводима транспозиция  $\varepsilon = (1, 2)$ . Но

$$\langle (1, 2), (1, 2, \dots, p) \rangle = S_p,$$



так как можно получить все транспозиции вида

$$(s + 1, s + 2) = x^{-s} \varepsilon x^s,$$

где  $s = \overline{0, p-1}$ ;  $s + 1, s + 2$  — сумма по модулю числа  $p$ . Итак, из группы  $G$  выводимы только циклы простой длины  $p$ . Пусть  $y$  — любой элемент группы  $G'$ . Покажем, что элемент  $y$  есть степень  $x$ . Существует такое число  $k$ , что

$$y^k = (1, 2, i_1, \dots, i_{p-2}).$$

Но тогда элемент  $xy^{-k}$  переводит 1 в 1. Следовательно, в разложении элемента  $xy^{-k}$  на циклы присутствуют только циклы единичной длины. Поэтому

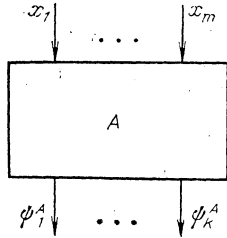


Рис. 1

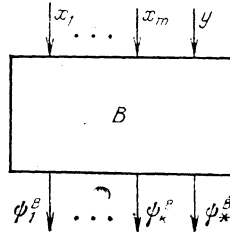


Рис. 2

$xy^{-k} = 1$  и  $x = y^k$ , так как  $y$  является циклом простой длины, следовательно,  $y = x^{k^{-1}}$ , поэтому  $G = \mathbb{Z}_p$ . Лемма доказана.

Пусть теперь задан автомат  $A$  с  $m$  входами и  $k$  выходами, внутренней группой  $G_A$ , и пусть из группы  $G$  непосредственно выводится группа  $G_A$ , т. е.  $G \rightarrow G_A$ . Построим автомат  $B$  с внутренней группой  $G_B$  ( $G_B = G$ ) такой, что однократное применение операции обратной связи дает автомат  $A$ .

Изобразим автомат  $A$  схемой на рис. 1. Построим автомат  $B$  (рис. 2).

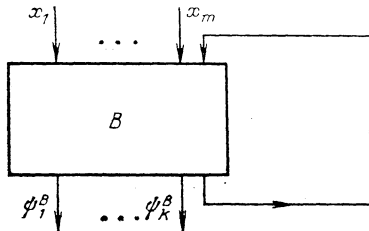
Из выводимости группы  $G_A$  из группы  $G$  следует, что перестановка состояний автомата  $A$ , индуцируемая  $x_0$ , получается из двух элементов  $g_0, g_1 \in G$ , т. е.  $\tilde{x}_0 \in g_0 \otimes g_1$ . Положим тогда

$$\varphi^B(\tilde{x}_0, 0, \tilde{z}) = \tilde{z}g_0, \quad \varphi^B(\tilde{x}_0, 1, \tilde{z}) = \tilde{z}g_1,$$

где  $\varphi^B$  — вектор-функция. Так сделаем для всех элементов  $\tilde{x}_0 \in E_2$ . Положим

$$\begin{aligned} \psi^B(\tilde{x}, y, \tilde{z}) &= \psi^A(x, z), \\ \psi_*^B(\tilde{x}_0, \tilde{z}) &= \begin{cases} 0, & \varphi^A(\tilde{x}_0, \tilde{z}) = \tilde{z}g_0, \\ 1, & \varphi^A(\tilde{x}_0, \tilde{z}) = \tilde{z}g_1 \end{cases} \end{aligned}$$

(при одинаковых значениях  $\tilde{z}g_0 = \tilde{z}g_1$  считаем  $\psi_*^B(\tilde{x}_0, \tilde{z}) = 0$ ), и так для всех элементов  $\tilde{x}_0$ . Ясно, что следующая схема 1



есть в точности автомат  $A$ , что следует из равенства

$$\psi^B(\tilde{x}_0, \psi_*^B(\tilde{x}_0, \tilde{z}), \tilde{z}) = \varphi^A(\tilde{x}_0, \tilde{z})$$

для всех  $\tilde{x}_0$  и  $\tilde{z}$ .

Таким образом, поднимаясь по цепочке вывода  $G \Rightarrow G_A$ , можно построить автомат, существование которого утверждалось в теореме 2, что и требовалось доказать.

В заключение автор хотел бы выразить признательность С. В. Алешину, который обратил его внимание на данную задачу.

#### СПИСОК ЛИТЕРАТУРЫ

1. Алгебраическая теория автоматов, языков и полугрупп /Под ред. М. А. Арбиба.— М.: Статистика, 1975.
2. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов.— М.: Наука, 1985.
3. Малыгин В. И. Трансформации группы автомата под действием операции обратной связи // Тезисы VI Всесоюзной конференции по теоретическим проблемам кибернетики, 1983.— Саратов: Изд-во Саратов. ун-та, 1986.— С. 93—94.
4. Пикар С. О базисах симметрической группы // Кибернетический сб. Вып. 1.— М.: Мир, 1965.— С. 7—34.

Статья поступила 03.11.89