# О мощности порождающих множеств в классе автоматов с линейной функцией выходов

Ф. Р. Юсупов[1]

Аннотация: Класс конечных автоматов конечно порожден по операциям композиции [1]. Важными его подклассами являются классы автоматов с линейными функциями выходов. Набор операций над автоматами, состоящий из подстановки переменных, подстановки автоматов и обратной связи, мы называем ограниченной композицией. По операциям ограниченной композиции класс одноместных автоматов замкнут. В настоящей работе показано, что в классе одноместных конечных автоматов с линейными функциями выходов и операциями ограниченной композиции отсутствуют конечные полные множества, но автоматы из этого класса, реализуемые схемами с не более чем одной задержкой, порождают этот класс.

**Ключевые слова:** конечные автоматы, операции композиции для автоматов, конечные автоматы с линейными выходами

## 1. Определения и преамбула

Мы используем определение инициального конечного автомата из работы [1].

**Определение 1.** *Конечный автомат* $\mathfrak{A}$ *– это шестерка* $(A, B, Q, \Phi, \Psi, \overline{q}_0)$, *где:*
$A = E_2^n$ *- входной алфавит*
$B = E_2^m$ *- выходной алфавит*
$Q = E_2^s$ *- алфавит состояний*
$\Phi : A \times Q \to Q$ *- функция переходов*
$\Psi : A \times Q \to B$ *- функция выходов*
$\overline{q}_0 \in \{0, 1\}^s$ *- начальное состояние.*

Конечный автомат $\mathfrak{A}$, заданный шестеркой из определения 1, имеет $n$ входов, $m$ выходов и функционирует в дискретном времени $t$, $t = 0, 1, \ldots$. Полагаем: $\overline{q}(0) = \overline{q}_0$. Если в момент времени $t$ заданы значения вектора состояния $\overline{q}(t)$ и входов автомата $\overline{x}(t) = (x_1(t), x_2(t), ..., x_n(t))$,

[1] *Юсупов Феликс Ренатович* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: fel.99@list.ru

Yusupov Feliks Renatovich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

то значения вектора состояний $\overline{q}(t+1)$ в момент $t+1$ и выходов $\overline{y}(t)=(y_1(t), y_2(t), ..., y_m(t))$ в момент $t$ определяются, соответственно, равенствами:

$$\overline{q}(t+1)=\Phi(\overline{x}(t), \overline{q}(t)), \tag{1}$$

$$\overline{y}(t)=\Psi(\overline{x}(t), \overline{q}(t)). \tag{2}$$

Конечный автомат может быть задан схемой из элементов $\vee, \wedge, \neg, q^0$(задержка с начальным состоянием 0), $q^1$ (задержка с начальным состоянием 1), множество которых обозначим $M^0$.

**Определение 2.** *Схемой из элементов множества $M^0$ называется ориентированный граф, полустепени захода вершин которого не превосходят двух, каждой вершине которого приписан:*
*- элемент множества $X=\{x_i | i=1,2,\dots\}$ (входная переменная), если полустепень захода вершины 0,*
*- один из элементов множества $\{\neg, q^0, q^1\}$, если полустепень захода вершины 1,*
*- конъюнкция $\wedge$ либо дизъюнкция $\vee$, если полустепень захода вершины 2, некоторым вершинам приписана переменная из множества выходных переменных $Y=\{y_i | i=1,2,\dots\}$, причем, разным вершинам – разные выходные переменные, а любой контур графа проходит через задержку. Вершины графа, которым приписаны входные (выходные) переменные, мы называем входами (выходами) схемы, а каждый выход схемы выделяем еще исходящим из него полуребром.*

Заметим, что мы не нумеруем входы элементов, так как перестановка входов не изменяет функции $\wedge$ и $\vee$.

Функционирование схемы определяется во времени. Начальные состояния задержек составляют вектор $\overline{q}(0)$. Если в момент времени $t$ определены состояния задержек $\overline{q}(t)$ и заданы значения входных переменных $\overline{x}(t)$, то значения на выходах элементов $\vee, \wedge, \neg$ и на входах задержек определяются также, как и в [2] для схемы из функциональных элементов с входами $\overline{x}(t), \overline{q}(t)$ и с выходами схемы, к которым добавлены выходы элементов, соединенных с входами задержек. Набор значений, получаемых на выходах схемы в момент $t$, составляет вектор $\overline{y}(t)$, а состоянием схемы в момент $t+1$ является набор значений входов задержек $\overline{q}(t+1)$.

Таким образом, для некоторых отображений $\Phi$ и $\Psi$, $\Phi: E_2^n \times E_2^s \to E_2^s$, $\Psi: E_2^n \times E_2^s \to E_2^m$, имеют место равенства (1), (2), и схема из элементов множества $M^0$ задает некоторый конечный автомат $\mathfrak{A}=(E_2^n, E_2^s, E_2^m, \Phi, \Psi, \overline{q}(0))$.

С другой стороны, каждый автомат $\mathfrak{A}=(E_2^n, E_2^m, E_2^s, \Phi, \Psi, \overline{q}(0))$ можно реализовать схемой, как показано на рисунке 1.

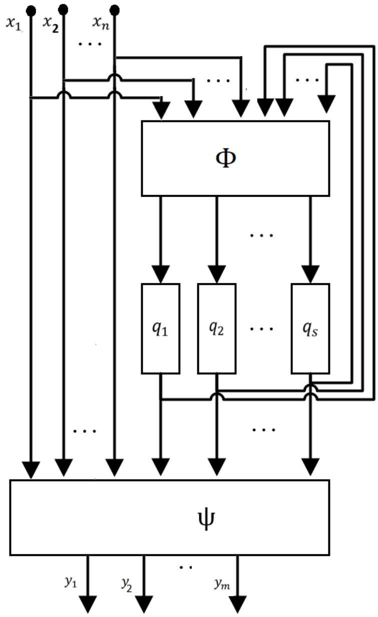



Рис. 1. Схема автомата $\mathfrak{A} = (E_2^n, E_2^s, E_2^m, \Phi, \Psi, \overline{q}(0))$.

Определим два набора операций над автоматами, используя схемы автоматов: операции ограниченной композиции и операции пополненной композиции. Пусть автоматы $\mathfrak{A}_1$, $\mathfrak{A}_2$ заданные шестерками $(A_i, B_i, Q_i, \Phi_i, \Psi_i, \overline{q}_{i,0})$, где $A_i = E_2^{n_i}$, $B_i = E_2^{m_i}$, $Q_i = E_2^{s_i}$, $i = 1, 2$, реализуются, соответственно, схемами $S_1$ и $S_2$, изображенными на рисунке 2.

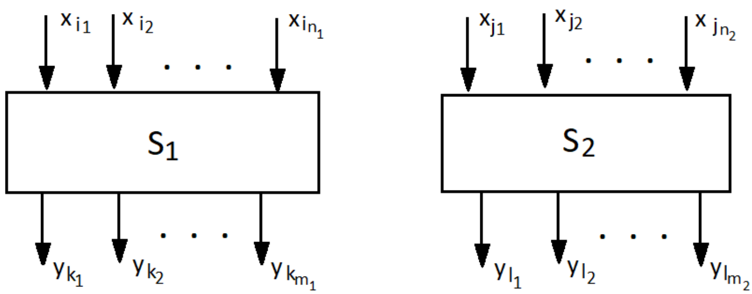



Рис. 2. Схемы автоматов $\mathfrak{A}_1$, $\mathfrak{A}_2$.

**Определение 3.** *Предположим, что* $\{i_1, \ldots, i_{n_1}\} \cap \{j_1, \ldots, j_{n_2}\} = \emptyset$ *и* $\{k_1, \ldots, k_{m_1}\} \cap \{l_1, \ldots, l_{m_2}\} = \emptyset$.

*Операции ограниченной композиции* ($K_c$).

*1)* Подстановка переменных.*[3] Пусть $\sigma$ – взаимнооднозначное отображение индексов переменных $i_1, i_2, \ldots, i_{n_1}$ на множество индексов $i'_1, i'_2, \ldots, i'_{n_1}$. Заменяя в схеме $S_1$ переменные $x_{i_1}, x_{i_2}, \ldots, x_{i_{n_1}}$ на переменные $x_{i'_1}, x_{i'_2}, \ldots, x_{i'_{n_1}}$, получим схему автомата $\mathfrak{A}_3$, изображенную на рисунке 3.*

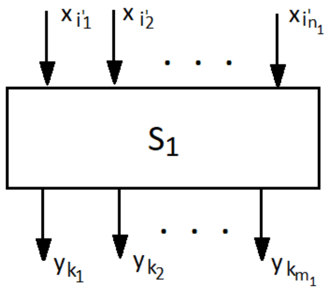



Рис. 3. Схема автомата $\mathfrak{A}_3$, полученного из $\mathfrak{A}_1$ подстановкой переменных.

*Нетрудно видеть, что операция подстановки переменных включает операции переименования переменных, перестановки переменных и отождествления переменных.*

*2)* Подстановка автоматов. *Пусть количество входов $n_1$ автомата $\mathfrak{A}_1$ не меньше количества выходов $m_2$ автомата $\mathfrak{A}_2$. Тогда, соединяя дугами выход $y_{l_r}$ схемы $S_2$ с каждым элементом схемы $S_1$, который соединен дугой с входом $x_{i_r}$, $r = 1, \ldots, m_2$, и удаляя все вершины $x_{i_r}$, $r = 1, \ldots, m_2$, вместе с дугами, выходящими из этих вершин, получим схему $S_4$ автомата $\mathfrak{A}_4$. Входами схемы $S_4$ являются все входы $S_2$ и входы $x_{m_2+1}$, $x_{m_2+2}, \ldots$, $x_{n_1}$ схемы $S_1$, а ее выходами – выходы схемы $S_1$. Автомат $\mathfrak{A}_4$ получен подстановкой автомата $\mathfrak{A}_2$ на автомат $\mathfrak{A}_1$. Схема $S_4$ представлена на рисунке 4. Жирные линии на рисунке указывают на возможность наличия нескольких дуг.*

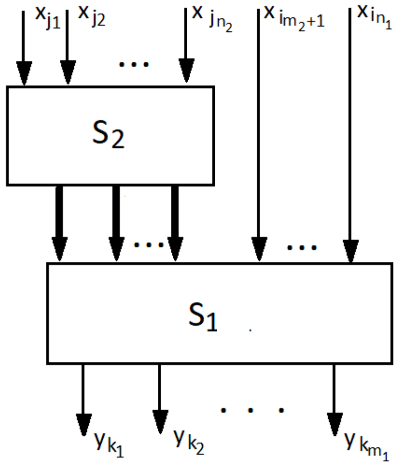



Рис. 4. Схема автомата $\mathfrak{A}_4$, полученного подстановкой автомата $\mathfrak{A}_2$ на автомат $\mathfrak{A}_1$.

*Отметим, что использование операции подстановки переменных снимает ограничение на выбор входов схемы $S_1$ для операции подстановки автоматов.*

*3)* Обратная связь. *Если каждый ориентированный путь от входа $x_{n_1}$ схемы $S_1$ к ее выходу $y_{k_i}$ проходит через задержку, то к $S_1$ добавим дуги из вершины $y_{k_i}$, в вершины, соединенные дугами с $x_{n_1}$. При этом удалим вершину $x_{n_1}$ и ведущие из нее дуги. Получим схему $S_5$ нового автомата $\mathfrak{A}_5$, изображенную на рисунке 5, на котором жирной линией обозначена возможность наличия нескольких дуг. Будем говорить, что автомат $\mathfrak{A}_5$ получен применением операции обратной связи к автомату $\mathfrak{A}_1$.*

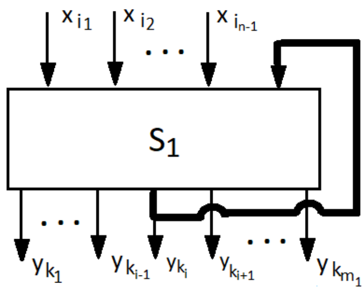



Рис. 5. Схема автомата $\mathfrak{A}_5$, полученного применением операции обратной связи к автомату $\mathfrak{A}_1$.

*Использование операции подстановки переменных снимает ограничение на выбор входа схемы $S_1$ для операции обратной связи.*

Добавляя к операциям ограниченной композиции, операцию объединения двух автоматов, получаем операции *пополненной композиции*:
4) *Объединение автоматов.* Автоматы $\mathfrak{A}_1$ и $\mathfrak{A}_2$ могут быть объединены в один автомат $\mathfrak{A}_6$. При этом входами схемы $S_6$, реализующей $\mathfrak{A}_6$, является объединение входов $S_1$ и $S_2$, а выходами $S_6$ – объединение выходов $S_1$ и $S_2$ (рисунок 6).

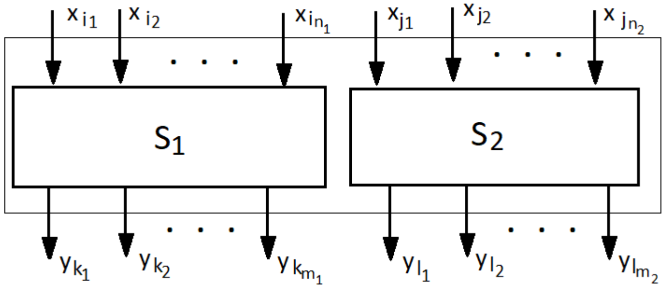



Рис. 6. Схема автомата $\mathfrak{A}_6$, полученного объединением автоматов $\mathfrak{A}_1$ и $\mathfrak{A}_2$.

Для автомата с линейной функцией выходов найдутся такие матрицы из $GF(2)$ $T$ и $R$, где $T = (t_{ij})_{m\times n}, R = (r_{ij})_{m\times s}$, что для его функции выходов выполнено:

$$\Psi(\overline{x}, \overline{q}) = T\overline{x}^* + R\overline{q}^*.$$

Через $P_{F.D.L.}$ обозначим множество всех конечных автоматов с линейной функцией выходов.

Обозначим через $K_c(M)$ множество всех автоматов, полученных из множества $M, M \subseteq P_{F.D.L.}$, с использованием операций ограниченной композиции, через $K_s(M)$ обозначим множество автоматов, полученных из множества M при помощи операций пополненной композиции.

Далее, с использованием введенных определений, будут сформулированы и доказаны результаты этой работы.

## 2. Результаты и их доказательства

Из последних двух определений вытекает утверждение:

**Утверждение 1.** $K_c(M) \subset K_s(M)$.

Нетрудно видеть, что для класса $P_{F.D.L}$ имеет место следующая лемма.

**Лемма 1.** *Автоматы с одним выходом образуют замкнутый класс по операциям ограниченной композиции.*

Имеет место:

**Утверждение 2.** *В классе конечных автоматов с операциями пополненной композиции автоматы из $P_{F.D.L}$ выражаются через элементы конечного множества $M^0$.*

*Доказательство.* Для заданного автомата с функциями переходов $\Phi$ и выходов $\Psi$ с использованием операций пополненной композиции из элементов множества $M^0$ можно построить автомат $(A, B, Q, \Phi, \Psi, \overline{q}_0)$ со схемой, представленной на рисунке 1 [1]. □

Конечный автомат $(A, B, Q, \Phi, \Psi, \overline{q}_0)$ реализует ограниченно-детерминированную функцию [1], преобразующую последовательности из $A^{\infty}$ в последовательности из $B^{\infty}$. Мы не будем различать автоматы, реализующие одну и ту же ограниченно-детерминированную функцию. При этом, автомат будем отождествлять с этой функцией.

Далее рассмотрим класс автоматов $P^1_{F.D.L.}$ с одним линейным выходом. Покажем, что в классе $P^1_{F.D.L}$ отсутствует конечный базис по операциям ограниченной композиции. Имеет место:

**Теорема 1.** $\forall M, M \subset P^1_{F.D.L}, |M| < \infty$, *выполнено:* $K_c(M) \neq P^1_{F.D.L}$.

*Доказательство.* Возьмем произвольное $M \subseteq P^1_{F.D.L}, |M| < \infty$.

$$M = \{f_1, ..., f_s\}, f_i = f_i(x_{i,1}, ..., x_{i,n_i}),$$

$$n = \max\{n_i | i = \overline{1, s}\}.$$

Рассмотрим автомат $f\left(x_1, \ldots, x_{n+1}\right)$, получаемый подстановкой конъюнкции переменных $x_1, \ldots, x_{n+1}$ на задержку с начальным состоянием 0,

$$f\left(x_1, \ldots, x_{n+1}\right) = q^0\left(x_1 \wedge \cdots \wedge x_{n+1}\right).$$

Имеем: $f\left(x_1, \ldots, x_{n+1}\right) \in P^1_{F.D.L}$.

Для выхода этого автомата в момент времени 1 имеет место равенство: $y(1) = x_1(0) \wedge x_2(0) \wedge ... \wedge x_{n+1}(0)$. Далее покажем, что $f \notin K_c(M)$. Рассмотрим выход y автомата из $M$. Пусть этот автомат имеет $n'$ входов, $n' \leq n$. Он задается системой канонических уравнений [1]:

$$\begin{cases} \overline{q}(0) = \overline{q}_0, \\ \overline{q}(t+1) = \Phi(\overline{x}(t), \overline{q}(t)), \\ y(t) = \psi(\overline{x}(t), \overline{q}(t)). \end{cases}$$

В момент времени $t = 0$: $y(0) = \psi(\overline{x}(0), \overline{q}(0)) = \psi(\overline{x}(0), \overline{q}_0)$
В момент времени $t = 1$: $y(1) = \psi(\overline{x}(1), \overline{q}(1)) = \psi(\overline{x}(1), \Phi(\overline{x}(0), \overline{q}(0)))$
$\overline{q}(0)$ - это вектор из констант. $\overline{x}(0) = (x_1(0), \ldots, x_{n'}(0))$. В то время как $\Phi$ может быть любым булевским оператором. Распишем подробнее: пусть рассматриваемый автомат реализуется схемой с l задержками. Тогда: $\overline{q}(t) = (q_1(t), ..., q_l(t))$, $\Phi = (\varphi_1, ..., \varphi_l)$. Возвращаясь к $y(1)$:
$y(1) = \psi(x_1(1), \ldots, x_{n'}(1), \varphi_1(x_1(0), \ldots, x_{n'}(0), q_1(0), \ldots, q_l(0)),$
$\varphi_2(x_1(0), \ldots, x_{n'}(0), q_1(0), \ldots, q_l(0)), \ldots, \varphi_l(x_1(0), \ldots, x_{n'}(0), q_1(0), \ldots, q_l(0)))$.

Далее
$y(1) = \psi(x_1(1), \ldots, x'_n(1), \Pi_1, \Pi_2, \ldots, \Pi_l)$, где $\Pi_i$ - полином Жегалкина для $\varphi_i(x_1(0), \ldots, x'_n(0), q_1(0), \ldots, q_l(0))$

Функция $\psi$ линейна относительно всех своих переменных, поэтому:
$y(1) = c_1\Pi_1 + c_2\Pi_2 + \cdots + c_l\Pi_l + d_1x_1(1) + d_2x_2(1) + \cdots + d_{n'}x_{n'}(1)$.

Для степени $\Pi_i$ по компонентам вектора $\overline{x}(0)$ имеем: $\deg_{\overline{x}(0)}\Pi_i \leq n'$. Так как степени у каждого полинома Жегалкина $\Pi_i$ не превосходят $n'$, следовательно: $\deg_{\overline{x}(0)}y(1) \leq n'$.

То есть, мы показали, что для выхода в момент $t = 1$ автомата из $M$ выполнено: $deg_{\overline{x}_0}y(1) \leq n$.
Далее несложно показать, что если взять две функции $f_1$ и $f_2$ из $P_{F.D.L}$, степени выходов которых по $\overline{x}(0)$ в момент времени $t = 1$ не более $n$, то, применяя однократно операции 1-3 из определения операций $K_c(M)$, получаем функции с таким же свойством. Следовательно, $f(x_1, \ldots, x_{n+1}) \notin K_c(M)$. □

Мы показали, что класс $P^1_{F.D.L}$ не является конечнопорожденным по операциям ограниченной композиции.

Далее, введем множество $M_0$, состоящее из сумматора по модулю 2, константы 1 и всех автоматов, получаемыми подстановкой булевской функции на задержку (рисунок 7, где $\varphi$ - булевская функция)

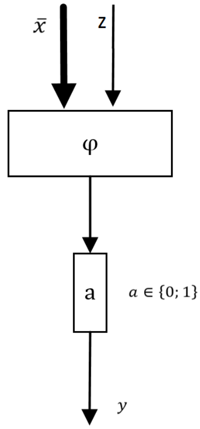



Рис. 7. Автоматы, содержащиеся в $M_0$.

**Теорема 2.** $P^1_{F.D.L.} = K_c(M_0)$.

*Доказательство.* Докажем теорему индукцией по числу задержек в схеме автомата. Пусть $f \in P^1_{F.D.L}$.
1) Если задержек 0, то $f$ - линейная функция алгебры логики, которую нетрудно получить, используя операции $K_c$ из сумматора и константы 1.
2) Если задержка одна, то рассмотрим каноническую схему этого автомата (см. рисунок 8).

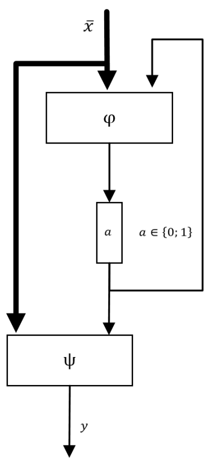
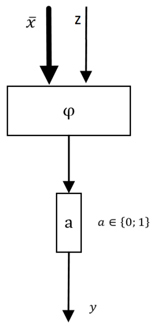


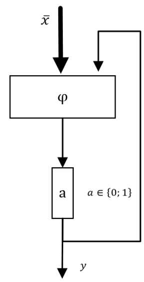

Рис. 8. Каноническая схема автомата с одной задержкой.

Автомат, схема которого представлена на рисунке 8, строится с использованием операций ограниченной композиции из элементов множества

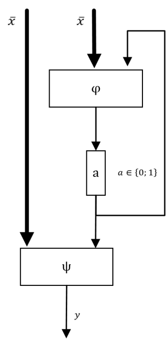
$M_0$. На рисунке 9 представлена последовательность построения этого автомата из автоматов множества $M_0$. Жирные линии для соединений схемы, возникающие при использовании операций подстановки и обратной связи, в дальнейшем не прорисовываем.



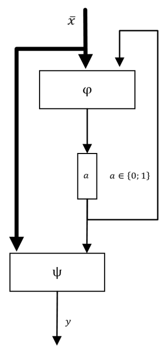

Шаг 1: строим схему для функции $\varphi$ и подстановляем ее на задержку.




Шаг 2: используем операцию обратной связи.




Шаг 3: строим функцию $\psi$ и используем подстановку.




Шаг 4: отождествляем соответствующие переменные.

Рис. 9. Построение автомата с одной задержкой.

Мы построили канонический автомат с одной задержкой, используя операции сокращенной композиции. Получили базу индукции. Далее рассмотрим **индукционное предположение:** Если автомат $f$ из $P^1_{F.D.L.}$ можно реализовать схемой, содержащей не более $s, s \geq 1$, задержек, то $f \in K_c(M_0)$.

**Индукционный переход:** Пусть схема $S$ содержит $s + 1$ задержку. Тогда автомат $f$, реализуемый схемой S, можно задать системой канонических уравнений:

$$\begin{cases} q_0 - \text{вектор начальных состояний задержек}, \\ q_i(t+1) = \varphi_i(\overline{x}(t), q_1(t), q_2(t), ..., q_{s+1}(t)), i = 1, ..., s+1 \\ y(t) = \psi(\overline{x}(t), q_1(t), q_2(t), ..., q_{s+1}(t)). \end{cases}$$

Для заданного $k$, $k \in \{1, 2..., s+1\}$, по предположению индукции, в $K_c(M_0)$ содержатся автоматы $h_j\,(\overline{x}, z)$, заданные следующими системами канонических уравнений:

$$\begin{cases} q_i(t+1) = \varphi_i(\overline{x}(t), q_1(t), q_2(t), ..., q_{k-1}(t), z, q_{k+1}(t), ..., q_{s+1}(t)), \\ i = 1, ..., k-1, k+1, ..., s+1, \\ y(t) = q_j(t). \end{cases}$$

$j = 1, ..., k-1, k+1, ..., s+1.$

Операциями ограниченной композиции из автоматов $h_j\,(\overline{x}, z)$, $j = 1, ..., k-1, k+1, ..., s+1$, и автомата $q^a\,(\varphi_k\,(\overline{x}, x_{n+1}, \ldots, x_{n+s}, z))$, содержащегося в $M_0$, построим автомат, изображенный на рисунке 10.

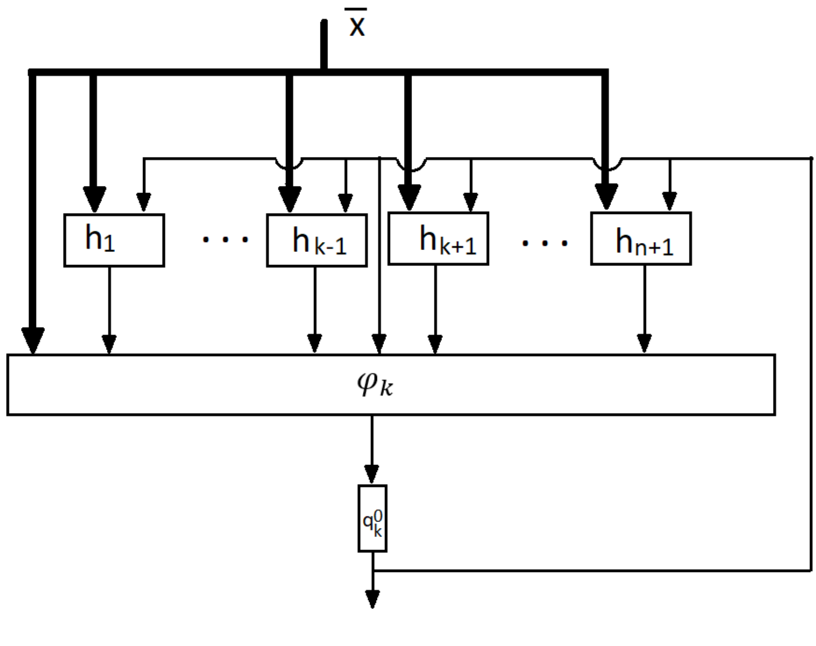



Рис. 10. Схема автомата с выходом $q_k(t)$ в момент времени $t$.

Здесь $a = q_k^0$ – начальное состояние задержки $q_k$.

Нетрудно видеть, что на выходе схемы, изображенной на рисунке 10, в момент времени $t$ получаем $q_k(t)$. Обозначим функцию, реализуемую этой схемой $f_k(\overline{x})$. Схема, изображенная на рисунке 11, реализует автомат $f$, который содержится в $K_c(M_0)$.

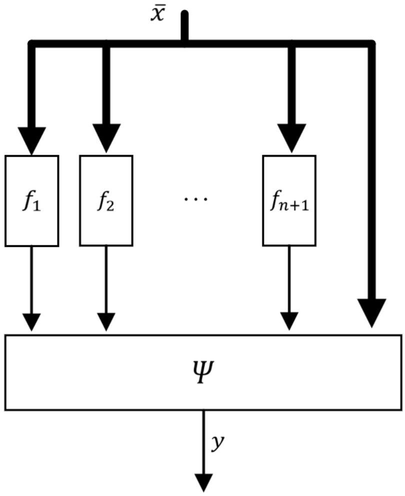



Рис. 11. Схема автомата $f$.

$\square$

# 3. Заключение

В работе рассматривается класс автоматов с линейными выходами и два набора операций композиции над автоматами: операции ограниченной композиции и операции пополненной композиции. Доказана теорема об отсутствии конечной полной системы по операциям ограниченной композиции для класса конечных автоматов с одним линейным выходом, найдено содержательное бесконечное множество автоматов, порождающее этот класс по операциям ограниченной композиции.

Автор выражает благодарность профессору кафедры МаТИС механико-математического факультета МГУ имени М.В. Ломоносова Часовских А.А. за научное руководство.

# Список литературы


[1] Кудрявцев В.Б., Алешин С.В., Подколзин А.С., *Введение в теорию автоматов*, «Наука», Москва, 1985, 320 pp.

[2] Лупанов О.Б., *Курс лекций по дискретной математике*, Механико-математический факультет МГУ им. М.В. Ломоносова, Москва, 2006, 38 pp.

[3] Яблонский С.В., Лупанов О.Б., *Дискретная математика и математические вопросы кибернетики*, **1**, Наука, Москва, 1974, 313 pp.


**On the cardinality of generating sets in the class of finite automata with a linear output function**

**Yusupov F.R.**

Abstract: The class of finite automata is finitely generated by composition operations [1]. An important subclass of this class are classes of automata with linear output functions. A set of operations on automata consisting of variable substitution, automata substitution, and feedback is called bounded composition. The class of unary automata is closed under bounded composition operations. In this paper, we show that the class of unary finite automata with linear output functions and bounded composition operations lacks finite complete sets. However, automata from this class, implemented by circuits with at most one delay, generate this class.

**Keywords:** finite automata, composition operations for automata, finite automata with linear outputs.

# References


[1] Кудрявцев В.Б., Алешин С.В., Подколзин А.С., *Введение в теорию автоматов*, «Наука», Москва, 1985, 320 pp.

[2] Лупанов О.Б., *Курс лекций по дискретной математике*, Механико-математический факультет МГУ им. М.В. Ломоносова, Москва, 2006, 38 pp.

[3] Яблонский С.В., Лупанов О.Б., *Дискретная математика и математические вопросы кибернетики*, **1**, Наука, Москва, 1974, 313 pp.