О свойстве линейной реализуемости отображений

С. Б. Родин[1]

В данной работе изучается линейная реализуемость отображений на конечном множестве. Данное свойство важно с точки зрения линейной реализуемости автоматов, а именно, линейная реализуемость порождающих внутренней полугруппы автомата является одним из необходимых условий линейной реализуемости автомата. Ранее было показано, что любое отображение на конечном множестве является линейно реализуемой посредством кодирования с длиной кода равной мощности множества. В данной работе этот результат будет усилен и будет показано, что любое отображение является линейно реализуемым посредством кодирования, с длиной кода равной мощности множества минус один.

Ключевые слова: теория автоматов, переходные системы, подстановка, кодирование, сложность, булев оператор

1. Введение

На практике часто приходится решать задачу перехода от автоматного описания функционирования на язык схем. Например, при логическом синтезе чипов на первом этапе функционирование чипа описывается как конечный автомат. Переход к описанию на языке схем осуществляется с помощью кодирования алфавита состояний, входного алфавита и выходного алфавита в алфавите $E_2 = \{0, 1\}$. В результате кодирования возникает булев оператор. При этом автомат может обладать тем свойством, что каждое кодирование порождает оператор, отличный от оператора, порождаемого любым другим кодированием [8].

Возникаемый в результате кодирования булев оператор можно рассматривать как набор булевых функций. Сложность такого оператора можно определить как максимальную сложность получающихся булевых функций. Как известно [1], каждой булевой функции единственным образом соответствует полином Жегалкина. В статье [10] было предложено определить сложность как максимальную из сложностей полиномов Жегалкина функций, задающих этот оператор, т. е. как максимальную

[1] *Родин Сергей Борисович* — старший научный сотрудник каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: sergei_rodin@mail.ru.

Rodin Sergei Borisovich — Senior research scientist, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

степень полиномов. Тогда простейшими с точки зрения такой сложности являются такие операторы, что соответствующие полиномы Жегалкина имеют первую степень, или линейные булевы функции. Интересно заметить, что максимальность мощности множества возникаемых для автомата посредством кодирований операторов[8] не гарантирует существование «простой», в указанном выше смысле, реализации автомата [9].

В статье [10] был доказан критерий линейной реализуемости нумерованной переходной системы $V = (E_2, E_n, \varphi)$ [2] посредством неизбыточного кодирования F. Данный критерий был сформулирован в терминах порождающих внутренней полугруппы переходной системы [7]. Обозначим через p_0 отображение на n-элементном множестве [3], индуцированное входным символом 0, а через p_1 отображение на n-элементном множестве, индуцированное входным символом 1. Для линейной реализуемости переходной системы необходимыми и достаточными условиями являются, во-первых линейная реализуемость отображений p_0 и p_1, во-вторых выполнения свойства «аддитивного сдвига» на отображениях p_0 и p_1 [10]. Данная работа посвящена изучению первого свойства, а именно линейной реализуемости отображений.

В сформулированном критерии длина кода ограничена $]log_2 n[$. Однако переходные системы, не являвшиеся линейно реализуемыми посредством коротких кодов, могут оказаться линейно реализуемыми посредством более длинных. Соответственно интересно изучить вопрос линейной реализуемости без ограничения на длину кода. В работе [11] было показано, что любое отображение на n-элементном множестве является линейно реализуемым посредством позиционного кодирования, причем длина кода такого кодирования равна n. В данной работе будет показано, для любого отображения на n-элементном множестве, существует кодирование, посредством которого достигается линейная реализуемость отображения и длина кода при таком кодировании равна $n - 1$.

2. Основные понятия и определения

Основным объектом изучения являются отображения на множестве E_n, где $n = 2^k$. В частности, будет изучаться как с помощью кодирования можно перейти от отображения к булеву оператору [1].

2.1. Булев оператор и его сложность

Сначала введем понятия, связанные с булевым оператором, и определим его сложность.

Определение 1. *Пусть* $\phi : E_2^m \to E_2^k$ *— булев оператор. Его можно рассматривать как набор* k *булевых функций [1], зависящих от* m *переменных, а именно, если* $\phi(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = (\beta_0, \beta_1, \ldots, \beta_{k-1})$*, то* $f_j(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = \beta_j$*, где* $0 \le j \le k-1$*. Обозначим этот набор через* $\mathcal{F}_\phi = \{f_0, f_1, \ldots, f_{k-1}\}$.

Пример 1. *Рассмотрим оператор* ϕ*, заданный таблицей*

x_0	x_1	x_2	x_3	y_0	y_1	y_2
0	0	0	0	0	0	1
0	0	0	1	0	1	0
0	0	1	0	0	1	1
0	0	1	1	1	0	0
0	1	0	0	1	0	1
0	1	0	1	1	1	0
0	1	1	0	0	0	0
0	1	1	1	1	1	1
1	0	0	0	0	1	1
1	0	0	1	1	1	0
1	0	1	0	0	0	1
1	0	1	1	1	0	1
1	1	0	0	1	0	0
1	1	0	1	0	1	0
1	1	1	0	1	1	1
1	1	1	1	0	0	0

Тогда последние три столбца y_0, y_1, y_2 *можно рассматривать как булевы функции* f_0, f_1, f_2*. Эти функции имеют следующий вид*

$$
\begin{aligned}
f_0(x_0, x_1, x_2, x_3) =& x_1 + x_2 \cdot x_3 + x_0 \cdot x_3 + x_1 \cdot x_2 + x_0 \cdot x_2 \cdot x_3 + x_0 \cdot x_1 \cdot x_2 \\
f_1(x_0, x_1, x_2, x_3) =& x_0 + x_2 + x_3 + x_0 \cdot x_1 + x_0 \cdot x_3 + x_1 \cdot x_2 + \\
& + x_0 \cdot x_1 \cdot x_2 + x_0 \cdot x_1 \cdot x_3 \\
f_2(x_0, x_1, x_2, x_3) =& 1 + x_3 + x_1 \cdot x_2 + x_0 \cdot x_1 + x_0 \cdot x_1 \cdot x_3 \\
& + x_0 \cdot x_2 \cdot x_3 + x_0 \cdot x_1 \cdot x_2 + x_0 \cdot x_1 \cdot x_2 \cdot x_3
\end{aligned}
$$

Определение 2. *Пусть* $\mathcal{F} = \{f_0, f_1, \ldots, f_{k-1}\}$ *— набор булевых функций, зависящих от* m *переменных. Данный набор определяет булев оператор* $\phi_\mathcal{F} : E_2^m \to E_2^k$ *по правилу*

$$
\begin{aligned}
\phi_\mathcal{F}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) =& (f_0(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}), \\
& f_1(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}), \\
& \ldots \\
& f_{k-1}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})),
\end{aligned}
$$

где $\alpha_i \in E_2$.

Пример 2. *Пусть дана пара функций* $f_0(x_0, x_1, x_2, x_3) = x_0 + x_1$

x_0	x_1	x_2	x_3	f_0
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	1
0	1	0	1	1
0	1	1	0	1
0	1	1	1	1
1	0	0	0	1
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

и $f_1(x_0, x_1, x_2, x_3) = x_2 + x_3$

x_0	x_1	x_2	x_3	f_1
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	0
0	1	0	0	0
0	1	0	1	1
0	1	1	0	1
0	1	1	1	0
1	0	0	0	0
1	0	0	1	1
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	1
1	1	1	0	1
1	1	1	1	0

Данные функции определяют булев оператор оператор ϕ*, задаваемый таблицей*

x_0	x_1	x_2	x_3	y_0	y_1
0	*0*	*0*	*0*	*0*	*0*
0	*0*	*0*	*1*	*0*	*1*
0	*0*	*1*	*0*	*0*	*1*
0	*0*	*1*	*1*	*0*	*0*
0	*1*	*0*	*0*	*1*	*0*
0	*1*	*0*	*1*	*1*	*1*
0	*1*	*1*	*0*	*1*	*1*
0	*1*	*1*	*1*	*1*	*0*
1	*0*	*0*	*0*	*1*	*0*
1	*0*	*0*	*1*	*1*	*1*
1	*0*	*1*	*0*	*1*	*1*
1	*0*	*1*	*1*	*1*	*0*
1	*1*	*0*	*0*	*0*	*0*
1	*1*	*0*	*1*	*0*	*1*
1	*1*	*1*	*0*	*0*	*1*
1	*1*	*1*	*1*	*0*	*0*

Определение 3. *Пусть* $\phi : E_2^m \to E_2^k$ *— булев оператор. Сложностью оператора назовем максимальную степень полиномов Жегалкина функций* $\mathcal{F}_\phi$ *или* $L_{deg}(\phi) = max_{f_i \in \mathcal{F}_\phi}\{degf_i\}$

Заметим, что сложность оператора из примера 1 равна 4, а сложность оператора из примера 2 равна 1.

В предыдущих определениях предполагалось, что операторы определены на всех элементах множества E_2^m. Однако, в дальнейшем будут возникать частично-определенные операторы, т. е. операторы, определенные на подмножестве множества E_2^m. Определим понятие доопределения частично-определенного оператора.

Определение 4. *Оператор* $\widehat{\phi} : E_2^m \to E_2^k$, $m, k \in N$ *назовем доопределением оператора* $\phi : R \to {E_2}^k$, *где* $R \subseteq E_2^m$, *если для каждого* $(\alpha_1, \ldots, \alpha_m) \in R$ *верно*

$$\phi(\alpha_1, ..., \alpha_m) = \widehat{\phi}(\alpha_1, ..., \alpha_m).$$

Пример 3. *Рассмотрим частично-определенный оператор* ϕ

x_0	x_1	x_2	y_0	y_1
0	*0*	*0*	*0*	*0*
0	*0*	*1*	*0*	*1*
0	*1*	*0*	*1*	*0*
1	*0*	*0*	*1*	*0*

Примером доопределения является оператор $\widehat{\phi}$

x_0	x_1	x_2	y_0	y_1
0	*0*	*0*	*0*	*0*
0	*0*	*1*	*0*	*1*
0	*1*	*0*	*1*	*0*
0	*1*	*1*	*1*	*1*
1	*0*	*0*	*1*	*0*
1	*0*	*1*	*1*	*1*
1	*1*	*0*	*0*	*0*
1	*1*	*1*	*0*	*1*

2.2. Реализуемость отображения посредством кодирования

От отображения к булеву оператору можно перейти с помощью кодирования. Сначала определим кодирование, а затем как с помощью кодирование получается булев оператор.

Определение 5. *Кодированием множества* $E_n = \{0, \ldots, n-1\}$ *назовем взаимно-однозначное отображение (вложение)* $F : \{0, \ldots, n-1\} \to E_2^m$, *где* $m \geq] \log_2 n[$.

Пример 4. *В качестве примера кодирования можно рассмотреть следующее отображение* E_8 *в* E_2^3*:*

q	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
$F(q)$	*001*	*010*	*100*	*011*	*110*	*111*	*101*	*000*

Выделим из всех кодирований «стандартное» кодирование.

Определение 6. *Кодирование* $F_0 : \{0, \ldots, n-1\} \to E_2^k$ *назовем стандартным, если код элемента есть его двоичное представление.*

Пример 5. *В качестве примера стандартного кодирования можно рассмотреть следующее отображение* E_8 *в* E_2^3*:*

q	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
$F_0(q)$	*000*	*001*	*010*	*011*	*100*	*101*	*110*	*111*

Каждому кодированию F можно сопоставить подстановку s_F на множестве $Q = \{0, \ldots, n-1\}$ по правилу $s_F(i) = F_0^{-1}(F(i))$.

Кодированию F из примера 4 соответствует подстановка

$$s_F = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 3 & 6 & 7 & 5 & 0 \end{pmatrix}$$

Определение 7. *Пусть* $s : E_n \to E_n$ *— отображение множества* $E_n = \{0, \ldots, n-1\}$ *в себя. Кодирование* $F : E_n \to E_2^l$ *множества* E_n *сопоставляет отображению* s *булев оператор* $\phi_s^F : R \to R$, *где* $R \subseteq E_2^k$, *по правилу*

$$\phi_s^F(\alpha_1, ..., \alpha_{l-1}) = F(s(F^{-1}(\alpha_1, ..., \alpha_{l-1}))),$$

где $\alpha_1, ..., \alpha_{l-1} \in E_2$.

Пример 6. *Пусть задано отображение*

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \end{pmatrix}$$

Рассмотрим кодирование

q	0	1	2	3	4	5	6	7
$F(q)$	0000	0010	0100	0111	1000	1010	1100	1111

Построим булев оператор по отображению p *с использованием кодирования* F. *Запишем отображение* p *в табличном виде.*

i	$p(i)$
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	0

Заменим в таблице элементы множества E_8 *на их коды, определяемые кодированием* F. *В результате получится определяет следующий частично определенный булев оператор* ϕ

x_0	x_1	x_2	x_3	y_0	y_1	y_2	y_3
0	0	0	0	0	0	1	0
0	0	1	0	0	1	0	0
0	1	0	0	0	1	1	1
0	1	1	1	1	0	0	0
1	0	0	0	1	0	1	0
1	0	1	0	1	1	0	0
1	1	0	0	1	1	1	1
1	1	1	1	0	0	0	0

Определение 8. *Отображение $s : E_n \to E_n$ называется линейно реализуемым посредством кодирования F, если для оператора ϕ_s^F существует такое доопределение $\widehat{\phi}_s^F$, что набор $\mathcal{F}_{\widehat{\phi}_s^F}$ состоит из линейных булевых функций.*

Пример 7. *Заметим,что оператор ϕ из примера 6*

x_0	x_1	x_2	x_3	y_0	y_1	y_2	y_3
0	*0*	*0*	*0*	*0*	*0*	*1*	*0*
0	*0*	*1*	*0*	*0*	*1*	*0*	*0*
0	*1*	*0*	*0*	*0*	*1*	*1*	*1*
0	*1*	*1*	*1*	*1*	*0*	*0*	*0*
1	*0*	*0*	*0*	*1*	*0*	*1*	*0*
1	*0*	*1*	*0*	*1*	*1*	*0*	*0*
1	*1*	*0*	*0*	*1*	*1*	*1*	*1*
1	*1*	*1*	*1*	*0*	*0*	*0*	*0*

может быть доопределен до оператора $\widehat{\phi}$, таким образом что $\mathcal{F}_{\widehat{\phi}}^F$ состоит из линейных булевых функций. Жирным шрифтом выделены наборы, на которых оператор ϕ не определен и значения оператора $\widehat{\phi}$ на этих наборах.

x_0	x_1	x_2	x_3	y_0	y_1	y_2	y_3
0	*0*	*0*	*0*	*0*	*0*	*1*	*0*
0	**0**	**0**	**1**	**1**	**0**	**1**	**1**
0	*0*	*1*	*0*	*0*	*1*	*0*	*0*
0	**0**	**1**	**1**	**1**	**1**	**0**	**1**
0	*1*	*0*	*0*	*0*	*1*	*1*	*1*
0	**1**	**0**	**1**	**1**	**1**	**1**	**0**
0	**1**	**1**	*0*	**0**	**0**	**0**	**1**
0	*1*	*1*	*1*	*1*	*0*	*0*	*0*
1	*0*	*0*	*0*	*1*	*0*	*1*	*0*
1	**0**	**0**	**1**	**0**	**0**	**1**	**1**
1	*0*	*1*	*0*	*1*	*1*	*0*	*0*
1	**0**	**1**	**1**	**0**	**1**	**0**	**1**
1	*1*	*0*	*0*	*1*	*1*	*1*	*1*
1	**1**	**0**	**1**	**0**	**1**	**1**	**0**
1	**1**	**1**	**0**	**1**	**0**	**0**	**1**
1	*1*	*1*	*1*	*0*	*0*	*0*	*0*

Причем множество $\mathcal{F}_{\widehat{\phi}}^{F}$ *состоит из функций*

$$y_0 = x_0 + x_3$$
$$y_1 = x_1 + x_2$$
$$y_2 = x_2 + 1$$
$$y_3 = x_1 + x_3$$

Следовательно подстановка p *из примера 6 является линейной реализуемой посредством кодирования* F*.*

2.3. Понятие линеаризующего кодирования

Среди всех кодирований выделим специальное кодирование, которое назовем линеаризующим.

Определение 9. *Пусть задан вектор* $(q_0, \ldots, q_{k-1}) \in E_2^k$*. Множеством единиц* $\mathbb{I}_{q_0,\ldots,q_{k-1}}$ *назовем множество всех индексов* $\{i_1, \ldots, i_l\}$ *таких, что* $j \in \{i_1, \ldots, i_l\}$ *тогда и только тогда, когда* $q_j = 1$*.*

Пример 8. *Пусть задан вектор* $\underset{0\,1\,2\,3}{(0110)}$*. Тогда* $\mathbb{I}_{(0110)} = \{12\}$*.*

Определение 10. *Полиномиальным оператором назовем отображение* $\phi_{pol} : E_2^k \to E_2^{2^k-1}$*, где* i*-ая компонента результата* ϕ_{pol_i} *определяется соотношением*

$$\phi_{pol_i}(q_0, \ldots, q_{k-1}) = q_{j_1} \cdot q_{j_2} \cdot \ldots \cdot q_{j_l},$$

где $(j_1, j_2, \ldots, j_l) = \mathbb{I}_{F_0(i+1)}, F_0 : E_n \to E_2^k$ *- стандартное кодирование,* $i \in E_{2^k-1}$*.*

Пример 9. *Оператор* $\phi_{pol} : E_2^3 \to E_2^7$ *имеет вид*

x_0	x_1	x_2	y_0 {2}	y_1 {1}	y_2 {12}	y_3 {0}	y_4 {02}	y_5 {01}	y_6 {012}
0	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
0	*0*	*1*	*1*	*0*	*0*	*0*	*0*	*0*	*0*
0	*1*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*
0	*1*	*1*	*1*	*1*	*1*	*0*	*0*	*0*	*0*
1	*0*	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*
1	*0*	*1*	*1*	*0*	*0*	*1*	*1*	*0*	*0*
1	*1*	*0*	*0*	*1*	*0*	*1*	*0*	*1*	*0*
1	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*

Определение 11. *Пусть задано кодирование* $F : E_{2^k} \to E_2^k$. *Обозначим через* $L_F : E_{2^k} \to E_2^{2^k-1}$ *линеаризующее кодирование, задаваемое соотношение по формуле:*

$$L_F(q) = \phi_{pol}(F(q)), q \in E_{2^k}.$$

Заметим, что отображение $L_F : E_{2^k} \to S$ является взаимнооднозначным, т. е. из $q \neq q'$ следует $L_F(q) \neq L_F(q')$. Другими словами данное отображение может быть использовано в качестве кодирования. Это следует из определения, если $q \neq q'$, то $F(q) \neq F(q')$ в силу определения кодирования, а значит и $L_F(q)$ и $L_F(q')$ отличаются.

Пример 10. *Пусть задано стандартное кодирование* $F_0 : E_8 \to E_2^3$

q	0	1	2	3	4	5	6	7
$F_0(q)$	000	001	010	011	100	101	110	111

Тогда кодирование $L_F : E_8 \to E_2^7$ *задается как*

q	0	1	2	3	4	5	6	7
$L_F(q)$	0000000	0000001	0000010	0000111	0001000	0011001	0101010	111111

3. Линейная реализуемость отображений.

Теорема 1. *Пусть задано отображение* $p : E_n \to E_n$, *где* $n = 2^k$ *и кодирование* $F : E_n \to E_2^k$. *Отображение* p *является линейно реализуемым посредством линеаризующего кодирования* L_F

Доказательство. Построим по отображению p и кодированию L_F булев оператор $\phi_p^{L_F}$.

$$\begin{aligned}\phi_p^{L_F}(q_0, \ldots, q_{n-2}) &= L_F(p({L_F}^{-1}(q_0, \ldots, q_{n-2}))) \\ &= \phi_{pol}(F(p(F^{-1}(\phi_{pol}^{-1}(q_0, \ldots, q_{k-1}))))),\end{aligned}$$

где $(q_0, \ldots, q_{n-2}) \in R = Im(L_F)$. Схематически данное отображение можно представить следующим образом

$$E_2^{n-1} \supset R \overset{\phi_{pol}^{-1}}{\to} E_2^k \overset{F^{-1}}{\to} E_n \overset{p}{\to} E_n \overset{F}{\to} E_2^k \overset{\phi_{pol}}{\to} R \subset E_2^{n-1}.$$

Из определения отображения ϕ_{pol} следует, что $\forall (q_0, \ldots, q_{n-2}) \in Im(L_F)$, $\phi_{pol}^{-1}(q_0, \ldots, q_{n-2}) = (q'_0, \ldots, q'_{k-1})$, где $(q'_0, \ldots, q'_{k-1}) \in E_2^k$. Следовательно,

$$\phi_{pol}(F(p(F^{-1}(\phi_{pol}^{-1}(q_0, \ldots, q_{n-2}))))) = \phi_{pol}(F(p(F^{-1}(q'_0, \ldots, q'_{k-1})))).$$

Можно заметить, что булев оператор ϕ_p^F,построенный по отображению p с помощью кодирования F, задается соотношением $\phi_p^F(q'_0,\dots,q'_{k-1}) = F(p(F^{-1}(q'_0,\dots,q'_{k-1})))$. Следовательно,

$$\phi_{pol}(F(p(F^{-1}(q'_0,\dots,q'_{k-1})))) = \phi_{pol}(\phi_p^F(q'_0,\dots,q'_{k-1}))).$$

Согласно определению 7 оператор ϕ_p^F можно рассматривать как набор k булевых функций, зависящих от k переменных. Обозначим этот набор через $\mathcal{F}_p(F)$. Наше соотношение может быть переписано как

$$\phi_{pol}(\phi_p^F(q'_0,\dots,q'_{k-1}))) = \phi_{pol}(f_0(q'_0,\dots,q'_{k-1}),\dots,f_{k-1}(q'_0,\dots,q'_{k-1}))),$$

где $f_i \in \mathcal{F}_p(F)$. Согласно определению отображения ϕ_{pol} i-ая координата результата равна

$$\phi_{pol}{}_i(f_0(q'_0,\dots,q'_{k-1}),\dots,f_{k-1}(q'_0,\dots,q'_{k-1})))) = f_{j_1}(q'_0,\dots,q'_{k-1})\cdot f_{j_2}(q'_0,\dots,q'_{k-1})\cdot\ldots\cdot f_{j_l}(q'_0,\dots,q'_{k-1}),$$

где $\{j_1,j_2,\dots,j_l\} = \mathbb{I}_{F_0(i+1)}, F_0 : E_n \to E_k^2$. Произведение булевых функций $f_{j_1}(q'_0,\dots,q'_{k-1})\cdot f_{j_2}(q'_0,\dots,q'_{k-1})\cdot\ldots\cdot f_{j_l}(q'_0,\dots,q'_{k-1})$ есть булева функция. Обозначим ее $g(q'_0,\dots,q'_{k-1})$. Данная функция может быть представлена в виде полинома Жегалкина.

$$g(q'_0,\dots,q'_{k-1}) = \sum_{\{q'_{j_0}q'_{j_1}\dots q'_{j_l}\}\in 2^{E_n}} a_{\{q'_{j_0}q'_{j_1}\dots q'_{j_l}\}}\cdot q'_{j_0}\cdot q'_{j_1}\cdot\ldots\cdot q'_{j_l},$$

где $a_R \in E_2, R \subset E_n$. Заметим, что $q'_{j_0}\cdot q'_{j_1}\cdot\ldots\cdot q'_{j_l}$ есть t-ая компонента оператора ϕ_{pol} или в наших обозначениях q_t, где $\{q'_{j_0}q'_{j_1}\dots q'_{j_l}\} = \mathbb{I}_{F_0(t+1)}$. Обозначим коэффициент $a_{\{q'_{j_0}q'_{j_1}\dots q'_{j_l}\}}$ через a_t. Следовательно, i-ая координата оператора $\phi_p^{L_F}$ задается как

$$\phi_p^{L_F}{}_i(q_0,\dots,q_{n-2}) = \sum_t a_t\cdot q_t,$$

где $(q_0,\dots,q_{n-2}) \in R$. Доопределим данный оператор до оператора $\widehat{\phi}_p^{L_F}$, i-ая координата которого задается формулой

$$\widehat{\phi}_p^{L_F}{}_i(q_0,\dots,q_{n-2}) = \sum_t a_t\cdot q_t,$$

для любого вектора $(q_0,\dots,q_{n-2}) \in E_2^{n-2}$. Можно видеть, что $\mathcal{F}_{\widehat{\phi}_p^{L_F}}$ состоит из линейных функций. Следовательно, отображение p линейно реализуемо посредством кодирования L_F. □

В заключении автор выражает благодарность Алёшину Станиславу Владимировичу и Носову Михаилу Васильевичу за многочисленные обсуждения и советы, которые позволили получить результаты, изложенные в данной работе.

Список литературы

[1] Яблонский С.В., *Введение в дискретную математику*, Наука, Москва.

[2] Кудрявцев В.Б., Алёшин С.В., Подколзин А.С., *Введение в теорию автоматов*, «Наука», Москва, 1985, 320 с.

[3] А. Клиффорд, Г. Престон, *Алгебраическая теория полугрупп*, **1**, Мир, Москва.

[4] Р. Лидл, Г. Нидеррайтер, *Конечные поля*, Мир, Москва.

[5] М.И. Каргаполов, Ю.И. Мерзляков, *Основы теории групп*, 3, Наука, Москва.

[6] Алёшин С.В., *Алгебраические системы автоматов*, МАКС Пресс, Москва, 2016.

[7] М.А. Арбиб, *Алгебраическая теория автоматов, языков и полугрупп*, «Статистика», Москва.

[8] Родин С.Б., "Переходные системы с максимальной вариантностью относительно кодирования состояний", *Интеллектуальные системы*, **4**:3-4, 335–352.

[9] Родин С.Б., "О связи линейно реализуемых автоматов и автоматов с максимальной вариативностью относительно кодирования состояний", *Интеллектуальные системы*, **20**:2, 337–347.

[10] Родин С.Б., "Линейно реализуемые автоматы", *Дискретная математика*, **29**:1 (2016), 59–79.

[11] Родин С.Б., "О свойствах кодирований состояний автомата", *Интеллектуальные системы*, **21**:1, 97–111.

On the linear realizability property of the mappings

Sergey Rodin

This paper studies the property of linear realizability of mapping of the finite set into itself. This property is important from linear realizability of automata, namely linear realizability of the elements of the generating set of the automaton inner semigroup is the one of the necessary conditions for linear realizability of the automaton. Previously it was shown that every mapping of the finite set into itself is linear realizable via an encoding which code length is equal the finite

set cardinality. In this paper this result will be improved and it will be shown that every mapping of the finite set into itself is linear realizable via an encoding which code length is equal the finite set cardinality minus one.

Keywords: Automata theory, semiautomata, transition systems, assignment, state encoding, complexity, boolean operator

References

[1] Yablonskij S.V., *Introduction to the discrete math*, Nauka, Moscow.

[2] Kudryavtsev V.B., Alyoshin S.V., Podkolzin A.S., *Introduction to automata theory*, Nauka, Moscow, 1985, 320 c.

[3] Clifford A.H., Preston G.B., *The algebraic theory of semigroups*, **1**, Mir, Moscow.

[4] R. Lidl, H. Niederreiter, *Finite fields*, Mir, Moscow.

[5] Kargapolov M.I., Merzlyakov Yu. I., *Basics of group theory*, 3, Nauka, Moscow.

[6] Alyoshin S.V., *Algebraic automata systems*, MAKS Press, Moscow, 2016.

[7] M.A. Arbib, *Algebraic theory of machines, languages and semigroups*, «Statistika», Moscow.

[8] Rodin S.B., "The most variable semiautomata with respect to the states encoding", *Intelligent systems*, **4**:3-4, 335–352.

[9] Rodin S.B., "On relation between the linearly realizable automata and the most variable automata with respect to the states encoding", *Intelligent systems*, **20**:2, 337–347.

[10] Rodin S.B., "Linearly realizable automata", *Discrete Math*, **29**:1 (2016), 59–79.

[11] Rodin S.B., "On automata states encoding properties", *Intelligent systems*, **21**:1, 97–111.