О свойстве аддитивного сдвига для линейной реализуемости автоматов

С. Б. Родин[1]

Одним из необходимых условий для линейной реализуемости автомата является выполнения условия «аддитивного сдвига» на порождающих внутренней полугруппы автомата. «Аддитивный сдвиг» задается отображением на множестве состояний автомата. В данной работе изучаются такие отображения. Приведены свойства, которыми должно обладать отображение, чтобы задавать «аддитивный сдвиг». Так же показано, что такие отображения линейно реализуемы посредством неизбыточных кодирований и приведен явный вид получаемого оператора.

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 [1].

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 [2], каждой булевой функции единственным образом соответствует полином Жегалкина. В статье [3] было предложено определить сложность как максимальную из сложностей полиномов Жегалкина функций, задающих этот оператор, т. е. как максимальную степень полиномов. Тогда простейшими с точки зрения такой сложности являются такие операторы, что соответствующие полиномы Жегалкина имеют первую степень, или линейные булевы функции. Интересно

[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.

заметить, что максимальность мощности множества возникаемых для автомата посредством кодирований операторов [1] не гарантирует существование «простой», в указанном выше смысле, реализации автомата [4].

В статье [3] был доказан критерий линейной реализуемости нумерованной переходной системы $V = (E_2, E_n, \varphi)$ [5] посредством неизбыточного кодирования F. Данный критерий был сформулирован в терминах порождающих внутренней полугруппы переходной системы [6]. Обозначим через p_0 отображение на n-элементном множестве [7], 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 [3]. В работах [8] и [9] изучался вопрос линейной реализуемости отображений. Данная работа посвящена изучению отображений, задающих «аддитивный сдвиг». В частности, будут сформулированы свойства, которыми должны обладать отображения, задающие «аддитивный сдвиг», а также доказана линейная реализуемость таких отображений с указанием кодирования.

2. Основные понятия и определения

Основным объектом изучения являются отображения на множестве E_n, задающие аддитивный сдвиг, где $n = 2^k$. Так же будет рассмотрен вопрос реализации таких отображений булевыми операторами [2].

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 [2], 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	y_0	y_1	y_2
0	*0*	*0*	*0*	*0*	*1*
0	*0*	*1*	*0*	*1*	*0*
0	*1*	*0*	*0*	*0*	*0*
0	*1*	*1*	*1*	*0*	*0*
1	*0*	*0*	*1*	*0*	*1*
1	*0*	*1*	*1*	*0*	*1*
1	*1*	*0*	*1*	*1*	*1*
1	*1*	*1*	*0*	*1*	*1*

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

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

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 $f_0(x_0, x_1, x_2) = x_0 + x_1 \cdot x_2$*

x_0	x_1	x_2	f_0
0	*0*	*0*	*0*
0	*0*	*1*	*0*
0	*1*	*0*	*0*
0	*1*	*1*	*1*
1	*0*	*0*	*1*
1	*0*	*1*	*1*
1	*1*	*0*	*1*
1	*1*	*1*	*0*

и $f_1(x_0, x_1, x_2) = x_0 \cdot x_1 + x_1 \cdot x_2 + x_2$

x_0	x_1	x_2	f_1
0	*0*	*0*	*0*
0	*0*	*1*	*1*
0	*1*	*0*	*0*
0	*1*	*1*	*0*
1	*0*	*0*	*0*
1	*0*	*1*	*1*
1	*1*	*0*	*1*
1	*1*	*1*	*1*

Данные функции определяют булев оператор оператор ϕ, задаваемый таблицей

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

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 $L_{deg}(\phi) = max_{f_i \in \mathcal{F}_\phi}\{deg f_i\}$*

Заметим, что сложность оператора из примеров 1 и 2 равна 2.

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*	*0*	*0*
1	*0*	*0*	*1*	*0*
1	*1*	*0*	*1*	*1*

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*	*0*	*0*
0	*1*	*1*	*0*	*1*
1	*0*	*0*	*1*	*0*
1	*0*	*1*	*1*	*1*
1	*1*	*0*	*1*	*1*
1	*1*	*1*	*1*	*0*

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*	*000*	*100*	*101*	*101*	*111*	*011*

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

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

Каждой подстановке $s : E_n \to E_n$ сопоставим кодирование F_s по правилу $F_s(i) = F_0(s(i))$.

Пример 6. *Пусть задана подстановка*

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

Данной подстановке соответствует кодирование

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

Заметим, что для неизбыточного F верно, кодирование $F_{s_F} = F$, для подстановки s верно $s_{F_s} = s$.

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 7. *Пусть задано отображение*

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

Рассмотрим кодирование

q	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
$F(q)$	*0000*	*0001*	*0010*	*0100*	*1000*	*0011*	*0101*	*1111*

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

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

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	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	1	1
0	0	1	1	0	0	1	0
0	1	0	0	0	1	0	1
0	1	0	1	0	1	0	0
1	0	0	0	1	1	1	1
1	1	1	1	1	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 8. *Заметим,что оператор ϕ из примера 7*

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

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

$$\begin{aligned} y_0 &= x_0 \\ y_1 &= x_0 + x_1 \\ y_2 &= x_0 + x_2 \\ y_3 &= x_0 + x_1 + x_2 + x_3 \end{aligned}$$

Следовательно подстановка p *из примера 7 является линейной реализуемой посредством кодирования* F*.*

2.3. Отображения, задающие аддитивный сдвиг

Если $n = 2^k$, то отображения множества $E_n = \{0, \ldots, n-1\}$ в себя могут быть представлены [2] как многочлены над полем Галуа F_n [10].

Обозначим через $H_+ \subset P_n$ множество подстановок, соответствующих многочленам вида $x + c$ над полем Галуа F_n, где $c \in E_n$ — константа.

Пример 9. *Приведем пример множеств* H_+ *для* $n = 8$*. Обозначим отображение, соответствующее многочлену* f *над полем Галуа, через* h_f*.*

$$H_+ = \{h_x = e, h_{x+1} = (0\,1)(2\,3)(4\,5)(6\,7), h_{x+2} = (0\,2)(1\,3)(4\,6)(5\,7),$$

$$h_{x+3} = (0\,3)(1\,2)(4\,7)(5\,6), h_{x+4} = (0\,4)(1\,5)(2\,6)(3\,7), h_{x+5} = (0\,5)(1\,4)(2\,7)(3\,6),$$

$$h_{x+6} = (0\,6)(1\,7)(2\,4)(3\,5), h_{x+7} = (0\,7)(1\,6)(2\,5)(3\,4)\},$$

Замечание. *Умножение отображений осуществляется «слева направо», т.е. если заданы отображения p_1 и p_2, то значение их произведения на элементе i определяется равенством $(p_1 \cdot p_2)(i) = p_2(p_1(i))$.*

Определение 9. *Отображение $h : E_n \to E_n$ определяет аддитивный сдвиг, если существует такое взаимнооднозначное отображение $s : E_n \to E_n$, что $h \in H_+^s = s^{-1} \cdot H_+ \cdot s$.*

3. Основные результаты

Лемма 1. *Пусть задано отображение $h : E_n \to E_n$, отличное от тождественного, такое, что верно*

- *если $h(q_1) = h(q_2)$, то $q_1 = q_2$, $\forall q_1, q_2 \in E_n$*
- *$h(q) \neq q$, $\forall q \in E_n$*
- *$h(h(q)) = q$, $\forall q \in E_n$*

тогда существует такое разбиение множества $E_n = Q_1 \sqcup Q_2 \sqcup \ldots \sqcup Q_m$, что верно

- *$m = \frac{n}{2}$*
- *$Q_i \bigcap Q_j = \emptyset$, если $i \neq j$*
- *$|Q_i| = 2$, $\forall i \in \{1, \ldots, m\}$*
- *$h(Q_i) = Q_i$, $\forall i \in \{1, \ldots, m\}$*

Доказательство. Построим указанное разбиение множества E_n явным образом по индукции.

База индукции. Обозначим через Q_1 множество $\{0, h(0)\}$.

Шаг индукции. Пусть построены множества Q_1, Q_2,…,Q_l. Пусть q минимальный элемент из $E_n \setminus (Q_1 \bigcup Q_2 \bigcup \ldots \bigcup Q_l)$. Тогда через Q_{l+1} обозначим множество $\{q, h(q)\}$.

Рассмотрим множество Q_i. По построению найдется элемент $q \in E_n$ такой, что $Q_i = \{q, h(q)\}$.

В силу свойства $h(q) \neq q$, $\forall q \in E_n$, следует, что мощность множества Q_i равна 2.

В силу свойства отображения $h(h(q)) = q$, $\forall q \in E_n$, следует, что $h(Q_i) = Q_i$.

Предположим, что найдутся такие i и j, что $Q_i \bigcap Q_j \neq \emptyset$. Без ограничения общности считаем, что $i < j$. Тогда по построению в множестве Q_j лежит элемент q, не лежащий в множестве Q_i. И поскольку,

пересечение множеств не пусто, а мощность каждого множества равна 2, то $h(q) \in Q_i = \{q_1, q_2\}$. Без ограничения общности будем считать, что $h(q) = q_1$. С другой стороны в силу того, что $h(Q_i) = Q_i$, а также свойства $h(q) \neq q$, $\forall q \in E_n$, верно $h(q_2) = q_1$. Это противоречит взаимной однозначности отображения h.

В силу доказанного выше на каждом шаге индукции множество из которого выбираем минимальный элемент уменьшается ровно на 2. Следовательно, таких шагов будет сделано равно $\frac{n}{2}$. □

Теорема 1. *Пусть задано взаимнооднозначное отображение $s : E_n \to E_n$. Отображение h, отличное от тождественного, принадлежит H_+^s тогда и только тогда, когда верно*

- *если $h(q_1) = h(q_2)$, то $q_1 = q_2$, $\forall q_1, q_2 \in E_n$*
- $h(q) \neq q$, $\forall q \in E_n$
- $h(h(q)) = q$, $\forall q \in E_n$

Доказательство. Пусть отображение $h \in H_+$ и $h \neq e$. Тогда существует такое $0 \neq c \in E_n$, что $h(q) = q + c$, $\forall q \in E_n$, где сумма понимается в смысле суммы поля Галуа E_n. Пусть $h(q_1) = h(q_2)$. Это можно переписать как $q_1 + c = q_2 + c$. Прибавим c к правой и левой части. В результате получим $q_1 = q_1 + c + c = q_2 + c + c = q_2$. Так как $c \neq 0$, то верно, что $h(q) = q + c \neq q$, $\forall q \in E_n$. Так же заметим, что $h(h(q)) = h(q) + c = q + c + c = q$, $\forall q \in E_n$.

Таким образом утверждение верно, если s - тождественное отображение.

Теперь покажем, что при сопряжении сохраняются свойства

- если $h(q_1) = h(q_2)$, то $q_1 = q_2$, $\forall q_1, q_2 \in E_n$
- $h(q) \neq q$, $\forall q \in E_n$
- $h(h(q)) = q$, $\forall q \in E_n$

Пусть $h = s^{-1} \cdot h' \cdot s$, и $h' \in H_+$.

Пусть $h(q_1) = h(q_2)$. Это можно переписать как

$$s(h'(s^{-1}(q_1))) = s(h'(s^{-1}(q_2))).$$

В силу взаимнооднозначности s верно, что

$$h'(s^{-1}(q_1)) = h'(s^{-1}(q_2)).$$

Отсюда следует, что $s^{-1}(q_1) = s^{-1}(q_2)$, а значит и $q_1 = q_2$.

Пусть $h'(q) \neq q$, $\forall q \in E_n$, но $\exists q_0$ такое, что $h(q_0) = q_0$. Данное равенство можно переписать как

$$s(h'(s^{-1}(q_0))) = q_0.$$

Обозначим через

$$q_1 = s^{-1}(q_0),$$

а через

$$q_2 = h'(q_1).$$

Заметим, что поскольку $h' \in H_+$, то в силу доказанного выше $h(q_1) = q_2 \neq q_1$, но при этом в силу соотношений, представленных выше, $s(q_1) = q_0$ и $s(q_2) = q_0$. Что противоречит взаимнооднозначности s.

В силу доказанного выше для отображения $h' \in H_+$ имеет место равенство $h'(h'(q)) = q$, $\forall q \in E_n$.

Для произвольного $q \in E_n$ рассмотрим $h(h(q))$. Верна следующая цепочка равенств

$$h(h(q)) = s(h'(s^{-1}(s(h'(s^{-1}(q)))))) = s(h'(h'(s^{-1}(q)))) = s(s^{-1}(q)) = q.$$

Таким образом доказано, что и третье свойство сохраняется при сопряжении. Таким образом теорема доказана в одну сторону.

Пусть задано отображение $h : E_n \to E_n$ такое, что

- если $h(q_1) = h(q_2)$, то $q_1 = q_2$, $\forall q_1, q_2 \in E_n$
- $h(q) \neq q$, $\forall q \in E_n$
- $h(h(q)) = q$, $\forall q \in E_n$

Согласно лемме 1, существует разбиение множества $E_n = Q_1 \sqcup \ldots \sqcup Q_m$, такое что $h(Q_i) = Q_i$, $\forall i \in \{1, \ldots, m\}$. Обозначим, элементы множества Q_i через $q_1^{Q_i}$ и $q_2^{Q_i}$, где $q_1^{Q_i} < q_2^{Q_i}$. В силу свойств отображения h верно, $h(q_1^{Q_i}) = q_2^{Q_i}$ и $h(q_2^{Q_i}) = q_1^{Q_i}$, $\forall i \in \{1, \ldots, m\}$. Рассмотрим отображение $h' \in H_+$, отличное от тождественного. Как было показано выше оно обладает свойствами

- если $h'(q_1) = h'(q_2)$, то $q_1 = q_2$, $\forall q_1, q_2 \in E_n$
- $h'(q) \neq q$, $\forall q \in E_n$
- $h'(h'(q)) = q$, $\forall q \in E_n$

Согласно лемме 1, существует разбиение множества $E_n = Q'_1 \sqcup \ldots \sqcup Q'_m$, такое что $h'(Q'_i) = Q'_i$, $\forall i \in \{1, \ldots, m\}$. Обозначим, элементы множества

Q'_i через $q_1^{Q'_i}$ и $q_2^{Q'_i}$, где $q_1^{Q'_i} < q_2^{Q'_i}$. В силу свойств отображения h верно, $h'(q_1^{Q'_i}) = q_2^{Q'_i}$ и $h'(q_2^{Q'_i}) = q_1^{Q'_i}$, $\forall i \in \{1, \ldots, m\}$.

Построим отображение $s : E_n \to E_n$ по правилу

$$s(q_1^{Q'_i}) = q_1^{Q_i}, \forall i \in \{1, \ldots, m\}$$

$$s(q_2^{Q'_i}) = q_2^{Q_i}, \forall i \in \{1, \ldots, m\}$$

Заметим, что в силу $E_n = Q'_1 \sqcup \ldots \sqcup Q'_m$, отображение s определено на всем множестве E_n. Областью значений отображения s является множество $E_n = Q_1 \sqcup \ldots \sqcup Q_m$. А следовательно отображение s взаимнооднозначно.

Рассмотрим значение отображения $s^{-1} \cdot h' \cdot s$ на элементах $q_1^{Q_i}$ и $q_2^{Q_i}$. Верны равенство

$$s(h'(s^{-1}(q_1^{Q_i}))) = s(h'(q_1^{Q'_i})) = s(q_2^{Q'_i}) = q_2^{Q_i}$$

$$s(h'(s^{-1}(q_2^{Q_i}))) = s(h'(q_2^{Q'_i})) = s(q_1^{Q'_i}) = q_1^{Q_i}$$

С другой стороны верно, что

$$h(q_1^{Q_i}) = q_2^{Q_i}$$

$$h(q_2^{Q_i}) = q_1^{Q_i}.$$

Следовательно

$$s(h'(s^{-1}(q_1^{Q_i}))) = h(q_1^{Q_i})$$
$$s(h'(s^{-1}(q_2^{Q_i}))) = h(q_2^{Q_i}).$$

То есть $h = s^{-1} \cdot h' \cdot s$, где $h' \in H_+$.

□

Теорема 2. *Пусть задано взаимооднозначное отображение $s : E_n \to E_n$ и подстановка $h \in H_+^s$, тогда h линейно реализуема посредством кодирования F_s, причем верно $\mathcal{F}_h(F_s) = \{x + c_0, x + c_1, \ldots, x + c_{k-1}\}$, где $c_i \in E_2$, $i \in E_k$, $n = 2^k$.*

Доказательство. Поскольку $h \in H_+^s$, то найдется такое отображение $h_{x+c} \in H_+$, соответствующее многочлену $x + c$, что верно $h = s^{-1} \cdot h_{x+c} \cdot h$. Оператор, построенный по отображению h посредством кодирования F_s, имеет вид

$$\phi_h^{F_s}(q_0, \ldots, q_{k-1}) = F_s(h(F_s^{-1}(q_0, \ldots, q_{k-1}))) =$$

$$= F_s(s^{-1}(h_{x+c}(s(F_s^{-1}(q_0, \ldots, q_{k-1})))))).$$

В силу определения $F_s(i) = F_0(s(i))$, где $i \in E_n$ равенство может быть переписано как

$$\phi_h^{F_s}(q_0, \ldots, q_{k-1}) = F_s(s^{-1}(h_{x+c}(s(F_s^{-1}(q_0, \ldots, q_{k-1}))))) =$$

$$= F_0(s(s^{-1}(h_{x+c}(s(s^{-1}(F_0^{-1}(q_0, \ldots, q_{k-1}))))))) =$$

$$= F_0(h_{x+c}(F_0^{-1}(q_0, \ldots, q_{k-1}) = \phi_{h_{x+c}}^{F_0}(q_0, \ldots, q_{k-1}).$$

То есть построенный оператор совпадает с оператором, построенным по отображению h_{x+c} посредством кодирования F_0. В работе [3] было доказано утверждение

Утверждение. *Подстановки $h_{x+c} \in H_+$ линейно реализуемы посредством кодирования F_0 и $\mathcal{F}_{h_{x+c}}(F_0) = \{x_0 + c_0, x_1 + c_1, \ldots, x_{k-1} + c_{k-1}\}$, $(c_0, c_1, \ldots, c_{k-1}) = F_0(c)$.*

Следовательно множество функций, задающих оператор, построенный по отображению h посредством кодирования F_s, имеет вид $\mathcal{F}_h(F_s) = \{x + c_0, x + c_1, \ldots, x + c_{k-1}\}$, где $c_i \in E_2$, $i \in E_k$, $n = 2^k$. □

В заключение 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] Родин С.Б., “Переходные системы с максимальной вариантностью относительно кодирования состояний”, *Интеллектуальные системы*, **4**:3-4 (1999), 335–352.

[2] Яблонский С.В., *Введение в дискретную математику*, Наука, Москва, 1979, 272 с.

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

[4] Родин С.Б., “О связи линейно реализуемых автоматов и автоматов с максимальной вариативностью относительно кодирования состояний”, *Интеллектуальные системы. Теория и приложения*, **20**:2 (2016), 337–347.

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

[6] М.А. Арбиб, “Декомпозиция автоматов и расширение полугрупп”, *Алгебраическая теория автоматов, языков и полугрупп*, «Статистика», Москва, 1975, 46–64, 335 с.

[7] А. Клиффорд, Г. Престон, *Алгебраическая теория полугрупп*. Т. 1, Мир, Москва, 1972, 288 с.

[8] Родин С.Б., “О свойствах кодирований состояний автомата”, *Интеллектуальные системы. Теория и приложения*, **21**:1 (2017), 97–111.

[9] Родин С.Б., “О свойстве линейной реализуемости отображений”, *Интеллектуальные системы. Теория и приложения*, **28**:1 (2024), 107–119.

[10] Р. Лидл, Г. Нидеррайтер, *Конечные поля*. Т. 1, Мир, Москва, 1988, 430 с.

On the additive shift property for the linear realizability of automata

Rodin S.B.

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] Rodin S.B., “The most variable semiautomata with respect to the states encoding”, *Intelligent systems*, **4**:3-4 (1999), 335–352.

[2] Yablonskij S.V., *Introduction to the discrete math*, Nauka, Moscow, 1979, 272 pp.

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

[4] Rodin S.B., "On relation between the linearly realizable automata and the most variable automata with respect to the states encoding", *Intelligent systems. Theory and Applications*, **20**:2 (2016), 337–347.

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

[6] M.A. Arbib, "Automaton Decompositions and Semigroup Extensions", *Algebraic theory of machines, languages and semigroups*, «Statistika», Moscow, 1975, 46–64, 335 pp.

[7] Clifford A.H., Preston G.B., *The algebraic theory of semigroups.* V. 1, Mir, Moscow, 1972, 288 pp.

[8] Rodin S.B., "On automata states encoding properties", *Intelligent systems. Theory and Applications*, **21**:1 (2017), 97–111.

[9] Rodin S.B., "On the linear realizability property of the mappings", *Intelligent systems. Theory and Applications*, **28**:1 (2024), 107–119.

[10] R. Lidl, H. Niederreiter, *Finite fields.* V. 1, Mir, Moscow, 1988, 430 pp.