О свойствах кодирований состояний автомата

С. Б. Родин (МГУ имени М. В. Ломоносова, Москва)

Изучается сложность реализации автоматов посредством кодирований его состояний. Рассматриваются всевозможные равномерные кодирования, т.е. кодирования состояний наборами одинаковой длины. На длину кода не накладывается ограничение сверху. Получена верхняя оценка сложности реализации автомата. Получена верхняя оценка длины кода, при котором достигается линейная реализуемость автомата.

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

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 $E_2 = \{0, 1\}$.

При этом важно выбрать кодирование, при котором достигается возможно меньшая сложность схемы.

С формальной точки зрения автомат — это пятерка $V = (A, Q, B, \varphi, \psi)$, где A — входной алфавит, Q — алфавит состояний, B — выходной алфавит, φ — функция, которая по текущему входу и состоянию определяет состояние автомата в следующий момент времени, ψ — выходная функция, которая по текущему входу и состоянию определяет выход автомата в текущий момент времени. Кодирование алфавита состояний — это отображение алфавита Q в E_2^k, при котором каждому состоянию из Q ставится в соответствие вектор из E_2^k. Кодирование

входного алфавита — это отображение алфавита A в E_2^p, при котором каждому элементу из A ставится в соответствие вектор из E_2^p. Кодирование выходного алфавита — это отображение алфавита B в E_2^l, при котором каждому элементу из B ставится в соответствие вектор из E_2^l. Кодирования алфавита состояния, входного алфавита и выходного алфавита порождают булев оператор $\phi : E_2^{k+p} \to E_2^{k+l}$, где p — длина кодового набора для символов множества A, k — длина кодового набора для символов множества Q, l — длина кодового набора для символов множества B.

Оператор ϕ можно рассматривать как набор $k+l$ булевых функций от $k+p$ переменных. Сложность такого оператора можно определить как максимальную сложность получающихся булевых функций. Как известно [1], каждой булевой функции единственным образом соответствует полином Жегалкина. Мы будем понимать сложность оператора как максимальную из сложностей полиномов Жегалкина функций, задающих этот оператор, т. е. как максимальную степень полиномов, а сложность автомата — как сложность оператора ϕ. Таким образом, установив связь между автоматом, кодировкой и возникающими полиномами, можно найти минимальную сложность реализации автомата.

Для автомата можно ввести понятие внутренней полугруппы. Внутренняя полугруппа определяется как замыкание отображений множества состояний в себя, определяемых входными символами [5]. Таким образом, на переходную систему автомата можно смотреть как на набор отображений, и сложность реализации автомата определяется сложностью реализации этих отображений.

В работе [9] изучались неизбыточные кодирования и линейная реализуемость автоматов. Неизбыточные кодирования характеризуются тем, что длина кода строго определена мощностью множества состояний автомата. В то же время за счет удлинения кода сложность автомата может уменьшиться. В статье изучается сложность реализации автоматов посредством кодирований, у которых не наложено ограничение на длину кода.

В разделе 2 рассматриваются вопросы сложности реализации отображений множества $E_n = \{0, \ldots, n-1\}$ в себя. В разделе 3 изучается сложность реализации переходной системы автомата.

В статье изучаются переходные с входным алфавитом $A = E_2$. Обозначим через P_n множество всех отображений множества $E_n = \{0, \ldots, n-1\}$ в себя, не обязательно взаимно-однозначных. Данное множество образует полугруппу преобразований множества E_n относитель-

но операции суперпозиции отображений. Взаимно-однозначные преобразования множества E_n образуют группу подстановок на этом множестве [2].

Сложность реализации элементов P_n

Определение 1. Пусть $\phi : E_2^m \to E_2^k$ — булев оператор. Его можно рассматривать как набор k булевых функций, 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 $\mathcal{F}_\phi = \{f_0, f_1, \ldots, f_{k-1}\}$.

Определение 2. Пусть $\mathcal{F} = \{f_0, f_1, \ldots, f_{k-1}\}$ — набор булевых функций, зависящих от k 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 $\alpha_i \in E_2$.

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 $L_{deg}(\phi) = max\{deg_{f_i \in \mathcal{F}_\phi} f_i\}$

Определение 4. *Кодированием множества* $E_n = \{0, \ldots, n-1\}$ назовем взаимно-однозначное отображение (вложение) $F : \{0, \ldots, n-1\} \to E_2^k$, где $k \ge]\log_2^n[$.

Определение 5. Пусть задано кодирование $F : \{0, \ldots, n-1\} \to E_2^k$, где $k \ge]\log_2 n[$. Кодирование $\hat{F} : \{0, \ldots, 2^k-1\} \to E_2^k$ назовем *доопределением кодирования* F, если для каждого $q \in \{0, \ldots, n-1\}$

$$F(q) = \hat{F}(q).$$

Определение 6. Пусть $s : E_n \to E_n$ — отображение множества $E_n = \{0, \ldots, n-1\}$ в себя. Кодирование $F : Q \to E_2^k$ множества E_n сопоставляет отображению s булев оператор $\phi_s^F : R \to R$, где $R \subseteq E_2^k$, по правилу

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

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

Определение 7. 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

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

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

Определение 9. Кодирование $F : \{0, \ldots, n-1\} \to E_2^n$, определяемое равенством $F(i) = (0 \ldots \underset{i+1}{1} \ldots 0)$, где «1» стоит в i-м разряде, а в остальных разрядах «0», назовем простым позиционным кодированием. Будем обозначать такое кодирование через F_{pos}.

Пример 1. Приведем пример простого позиционного кодирования F_{pos} множества $E_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

q	0	1	2	3	4	5	6	7
$F_{pos}(q)$	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000

Лемма 1. *Отображение $s : E_n \to E_n$ является линейно реализуемым посредством простого позиционного кодирования.*

Доказательство. Обозначим через $s(Q)$ полный образ множества Q отображения s, а через $s^{-1}(q)$ полный прообраз одно-элементного множества $\{q\}$ отображения s. Покажем, что множество

$$\mathcal{F} = \{f_j(\alpha_1, \ldots, \alpha_{k-1}) = \sum_{i \in s^{-1}(j)} \alpha_i, 0 \le j \le k-1\}$$

задает оператор ϕ, являющийся доопределением $\phi_s^{F_{pos}}$.

Рассмотрим значение оператора $\phi_s^{F_{pos}}$ на кодах элементов множества Q. Пусть $s(i) = j$, тогда согласно определению 2

$$\phi_s^F(0, \ldots, \underset{i}{1}, \ldots, 0) = F_{pos}(s(F_{pos}^{-1}(0, \ldots, \underset{i}{1}, \ldots, 0))) =$$

$$= F_{pos}(s(i)) = F_{pos}(j) = (0, \ldots, \underset{j}{1}, \ldots, 0).$$

Заметим, что $f_j(0,\dots,\underset{i}{1},\dots,0) = \sum_{i\in s^{-1}(j)} \alpha_i = 1$, так как $i \in s^{-1}(j)$, и в наборе $(0,\dots,\underset{i}{1},\dots,0)$ ровно одна «1».

С другой стороны $f_l(0,\dots,\underset{i}{1},\dots,0) = \sum_{i\in s^{-1}(j)} \alpha_i = 0$, где $l \neq j$, т.е.

$$\phi(0,\dots,\underset{i}{1},\dots,0) = (0,\dots,\underset{j}{1},\dots,0).$$

□

Пример 2. Булев оператор, сопоставляемый простым позиционным кодированием подстановке

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

есть

q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Оператор, задаваемый функциями,

$$f_0(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_1$$
$$f_1(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_2$$
$$f_2(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_3$$
$$f_3(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_4$$
$$f_4(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_5$$
$$f_5(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_6$$
$$f_6(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_7$$
$$f_7(q_0,q_1,q_2,q_3,q_4,q_5,q_6,q_7) = q_0$$

является доопределением построенного частично определенного оператора. Заметим, что p не является линейно реализуемой посредством неизбыточного кодирования.

Сложность реализации переходных систем

В этом разделе будут рассмотрены переходные системы.

Определение 10. Каждое кодирование F множества Q нумерованной переходной системы (A, Q, φ) порождает булев оператор $\phi_V^F : E_2 \times R \to R$, где $R \subseteq E_2^k$, по правилу

$$\phi_V^F(a, \alpha_1, \ldots, \alpha_k) = F(\varphi(a, F^{-1}(\alpha_1, \ldots, \alpha_k))),$$

где $a \in E_2, (\alpha_1, \ldots, \alpha_k) \in R$.

Определение 11. Назовем переходную систему *линейно реализуемой посредством кодирования* F, или просто *линейно реализуемой*, если для заданной нумерованной переходной системы V существует такое кодирование F, что для оператора ϕ_V^F существует доопределение $\widehat{\phi}_V^F$, у которого все элементы $\mathcal{F}_{\widehat{\phi}_V^F}$ являются линейными функциями алгебры логики.

Пример 3. Рассмотрим переходную систему V, изображенную на рисунке 1.

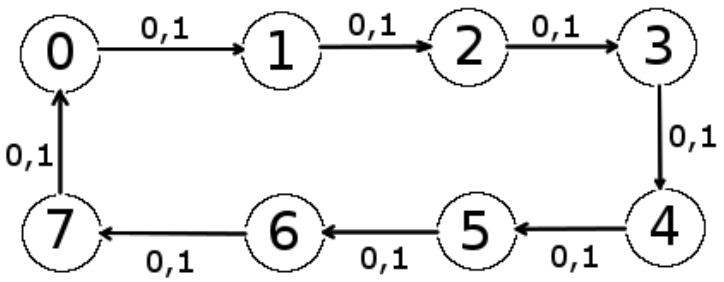

Рис. 1: Линейно реализуемая переходная система

Заметим,что переходная система V не является линейно реализуемой посредством неизбыточных кодирований. Данная переходная система и кодирование F_{pos}

q	0	1	2	3	4	5	6	7
$F_{pos}(q)$	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000

порождают булев оператор

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_3(t)$	$q_4(t)$	$q_5(t)$	$q_6(t)$	$q_7(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$	$q_3(t+1)$	$q_4(t+1)$	$q_5(t+1)$	$q_6(t+1)$	$q_7(t+1)$
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
1	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

Можно видеть, что канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = q_3(0) = q_4(0) = q_5(0) = q_6(0) = q_7(0) = 0 \\ q_0(t+1) = q_1(t) \\ q_1(t+1) = q_2(t) \\ q_2(t+1) = q_3(t) \\ q_3(t+1) = q_4(t) \\ q_4(t+1) = q_5(t) \\ q_5(t+1) = q_6(t) \\ q_6(t+1) = q_7(t) \\ q_7(t+1) = q_0(t) \end{cases}$$

Определение 12. Пусть заданы булев оператор $\phi(a, \alpha_0, \ldots, \alpha_{k-1}) = (\beta_0, \ldots, \beta_{k-1})$, где $a, \alpha_i, \beta_i \in E_2$, $k = \log_2 n$, и кодирование F. Определим переходную систему $V_\phi^F = (E_2, E_n, \varphi)$, в которой функция переходов φ определяется следующим правилом

$$\varphi(a, q) = F^{-1}(\phi(a, F(q)).$$

В работе [9] была доказана лемма

Лемма 2. *Пусть задан булев оператор* $\phi(a, \alpha_0, \ldots, \alpha_{k-1}) = (\beta_0, \ldots, \beta_{k-1})$, *где* $a, \alpha_i, \beta_i \in E_2$, $k = \log_2 n$. *Оператор, порождаемый кодированием* F *и переходной системой* V_ϕ^F, *равен оператору* ϕ .

Определение 13. Пусть задана переходная система $V = (E_2, \{0, \ldots, n-1\}, \varphi)$. Переходную систему $\hat{V} = (E_2, \{0, \ldots, \hat{n}-1\}, \hat{\varphi})$, где $\hat{n} > n$ назовем *доопределением переходной системы* V, если для каждого $a \in E_2$ и $q \in \{0, \ldots, n-1\}$

$$\varphi(a, q) = \hat{\varphi}(a, q).$$

Лемма 3. *Пусть нумерованная переходная система* $V = (E_2, Q = \{0, \ldots, n-1\}, \varphi)$ *линейно реализуема посредством кодирования* $F : \{0, \ldots, n-1\} \to E_2^k$, *где* $k \geq]\log_2 n[$. *Обозначим* $R = F(Q)$. *Тогда существует такое доопределение* $\hat{V} = (E_2, \{0, \ldots, 2^k - 1\}, \hat{\varphi})$ *переходной системы* V, *что переходная система* $\hat{V}$ *является линейно реализуемой.*

Доказательство. Из определения линейной реализуемости следует, что для оператора ϕ_V^F существует такое доопределение $\hat{\phi}_V^F$, что все элементы $\mathcal{F}_{\hat{\phi}_V^F}$ являются линейными функциями. Рассмотрим произвольное доопределение $\hat{F} : \{0, \ldots, 2^k - 1\} \to E_2^k$ кодирования F. По оператору $\hat{\phi}_V^F$ и кодированию $\hat{F}$ построим переходную систему $V_{\hat{\phi}_V^F}^{\hat{F}}$ согласно определению 12. Покажем, что данная переходная система является доопределением V. Множество состояний переходной системы $V_{\hat{\phi}_V^F}^{\hat{F}}$ есть множество $\{0, \ldots, 2^k - 1\}$ и поскольку $k \geq]\log_2 n[$, то $2^k - 1 \geq n - 1$. Согласно определению 12 для функции переходов $V_{\hat{\phi}_V^F}^{\hat{F}}$ верно равенство

$$\varphi_{\hat{\phi}_V^F}^{\hat{F}}(a, q) = \hat{F}^{-1}(\hat{\phi}_V^F(a, \hat{F}(q))).$$

Найдем значение этого оператора на элементах $q \in Q$. Поскольку $\hat{F}$ — доопределение кодирования F, для каждого $q \in Q$ верно равенсво $\hat{F}(q) = F(q)$. Следовательно для всех $q \in Q$

$$\varphi_{\hat{\phi}_V^F}^{\hat{F}}(a, q) = \hat{F}^{-1}(\hat{\phi}_V^F(a, F(q))).$$

Оператор $\hat{\phi}_V^F$ является доопределением оператора ϕ_V^F, значит для всех $q \in Q$ верно

$$\hat{\phi}_V^F(a, F(q)) = \phi_V^F(a, F(q)),$$

так как согласно определению 7 значения этих операторов совпадают на множестве определения оператора ϕ_V^F. Следовательно для всех $q \in Q$

$$\varphi_{\hat{\phi}_V^F}^{\hat{F}}(a, q) = \hat{F}^{-1}(\phi_V^F(a, F(q))).$$

Поскольку согласно определению 6 для любого $q \in Q$ его образ $\phi_V^F(a, F(q))$ принадлежит R, то для каждого $q \in Q$

$$\hat{F}^{-1}(\phi_V^F(a, F(q))) = F^{-1}(\phi_V^F(a, F(q))).$$

Значит для каждого $q \in Q$

$$\varphi^{\hat{F}}_{\hat{\phi}_V^F}(a, q) = F^{-1}(\phi_V^F(a, F(q))).$$

По построению оператора ϕ_V^F для всех $a \in E_2$ и $q \in Q$ верно равенство

$$\varphi^{\hat{F}}_{\hat{\phi}_V^F}(a, q) = F^{-1}(F(\varphi(a, F^{-1}(F(q))))) = \varphi(a, q).$$

Значит, переходная система $V^{\hat{F}}_{\hat{\phi}_V^F}$ является доопределением переходной системы V.

Согласно лемме 2 кодирование $\hat{F}$ по переходной системе $V^{\hat{F}}_{\hat{\phi}_V^F}$ порождает оператор $\hat{\phi}_V^F$. По условию леммы все элементы $\mathcal{F}_{\hat{\phi}_V^F}$ являются линейными функциями, значит переходная система $V^{\hat{F}}_{\hat{\phi}_V^F}$ является линейно реализуемой.

□

Определение 14. Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$, где $Q = \{0, \ldots, n-1\}$. *Сложностью переходной переходной системы* V назовем минимальную сложность среди всех операторов, являющихся доопределениями операторов ϕ_V^F, порождаемых переходной системой V и всевозможными кодированиями F. Обозначим сложность переходной системы через $L_{deg}(V)$.

Теорема 1. *Пусть задана нумерованная переходная система* $V = (E_2, Q, \varphi)$, *где* $Q = \{0, \ldots, n-1\}$. *Тогда* $L_{deg}(V) \leq 2$.

Доказательство. Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$. Обозначим ее порождающие через p_0 и p_1. Согласно лемме 1 они линейно реализуемы посредством простого позиционного кодирования F_{pos}. Рассмотрим линейные доопределения ϕ_{p_0} и ϕ_{p_1} булевых операторов, сопоставляемые отображениям p_0 и p_1 кодированием F_{pos}. Рассмотрим множества функций

$$\mathcal{F}_{\phi_{p_0}} = \{f_0^0(q_0, q_1, \ldots, q_{n-1}), \ldots, f_{n-1}^0(q_0, q_1, \ldots, q_{n-1})\}$$

и

$$\mathcal{F}_{\phi_{p_1}} = \{f_0^1(q_0, q_1, \ldots, q_{n-1}), \ldots, f_{n-1}^1(q_0, q_1, \ldots, q_{n-1})\},$$

определяемых операторами ϕ_{p_0} и ϕ_{p_1}. Покажем, что функции

$$\mathcal{F} = \{x \cdot (f_0^0(q_0, q_1, \ldots, q_{n-1}) \oplus f_0^1(q_0, q_1, \ldots, q_{n-1})) \oplus f_0^0(q_0, q_1, \ldots, q_{n-1}),$$

$$\ldots$$

$$x \cdot (f_{n-1}^0(q_0, q_1, \ldots, q_{n-1}) \oplus f_{n-1}^1(q_0, q_1, \ldots, q_{n-1})) \oplus f_{n-1}^0(q_0, q_1, \ldots, q_{n-1})\}$$

задают оператор ϕ, являющийся доопределением оператора $\phi_V^{F_{pos}}$.

Согласно определению порождающих внутренней полугруппы переходной системы верны равенства $\varphi(0, q) = p_0(q), \varphi(1, q) = p_1(q)$. Пусть $(\alpha_0, \ldots, \alpha_{n-1})$ код некоторого состояния $q \in Q$ при кодировании F_{pos}. Рассмотрим значение оператора $\phi_V^{F_{pos}}$ на наборах $(0, \alpha_0, \ldots, \alpha_{n-1})$.

$$\phi_V^{F_{pos}}(0, \alpha_0, \ldots, \alpha_{n-1}) = F_{pos}(\varphi(0, F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) =$$

$$= F_{pos}(p_0(F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) = \phi_{p_0}(\alpha_0, \ldots, \alpha_{n-1}) =$$

$$= (f_0^0(q_0, q_1, \ldots, q_{n-1}), \ldots, f_{n-1}^0(q_0, q_1, \ldots, q_{n-1})) = \phi(0, \alpha_0, \ldots, \alpha_{n-1}).$$

Рассмотрим значение оператора $\phi_V^{F_{pos}}$ на наборах $(1, \alpha_0, \ldots, \alpha_{n-1})$

$$\phi_V^{F_{pos}}(1, \alpha_0, \ldots, \alpha_{n-1}) = F_{pos}(\varphi(1, F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) =$$

$$= F_{pos}(p_1(F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) = \phi_{p_1}(\alpha_0, \ldots, \alpha_{n-1}) =$$

$$= (f_0^1(q_0, q_1, \ldots, q_{n-1}), \ldots, f_{n-1}^1(q_0, q_1, \ldots, q_{n-1})) = \phi(0, \alpha_0, \ldots, \alpha_{n-1}).$$

Из полученных равенств следует, что оператор ϕ совпадает с $\phi_V^{F_{pos}}$ на области определения оператора $\phi_V^{F_{pos}}$. Поскольку функции из наборов $\mathcal{F}_{\phi_{p_0}}$ и $\mathcal{F}_{\phi_{p_1}}$ линейные, функции из набора $\mathcal{F}$ задаются полиномами Жегалкина степени не выше 2. □

Следствие 1. *Нумерованная переходная система $V = (E_2, Q, \varphi)$, у которой функция переходов фиктивным образом зависит от входа, т.е. переходная система типа часы, является линейно реализуемой.*

Пример 4. Рассмотрим переходную систему V, изображенную на рисунке 2.

Данная переходная система и кодирование

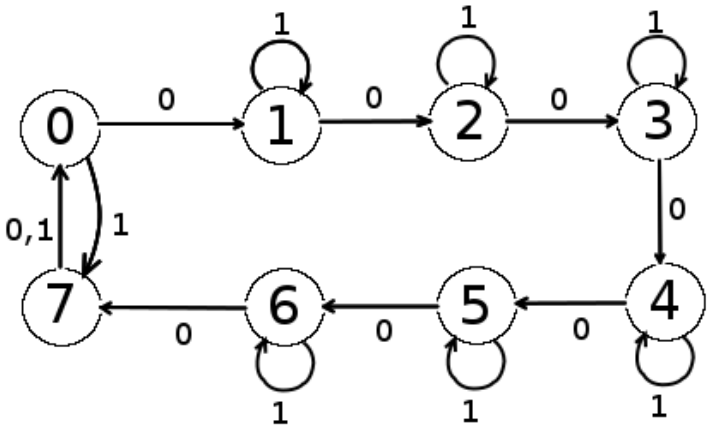

Рис. 2: Переходная система

q	0	1	2	3	4	5	6	7
$F_{pos}(q)$	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000

порождают булев оператор

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_3(t)$	$q_4(t)$	$q_5(t)$	$q_6(t)$	$q_7(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$	$q_3(t+1)$	$q_4(t+1)$	$q_5(t+1)$	$q_6(t+1)$	$q_7(t+1)$
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0
1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
1	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Можно видеть, что канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = q_3(0) = q_4(0) = q_5(0) = q_6(0) = q_7(0) = 0 \\ q_0(t+1) = x(t) \cdot q_1(t) + x(t) \cdot q_7(t) + q_1(t) \\ q_1(t+1) = x(t) \cdot q_2(t) + x(t) \cdot q_1(t) + q_2(t) \\ q_2(t+1) = x(t) \cdot q_3(t) + x(t) \cdot q_2(t) + q_3(t) \\ q_3(t+1) = x(t) \cdot q_4(t) + x(t) \cdot q_3(t) + q_4(t) \\ q_4(t+1) = x(t) \cdot q_5(t) + x(t) \cdot q_4(t) + q_5(t) \\ q_5(t+1) = x(t) \cdot q_6(t) + x(t) \cdot q_5(t) + q_6(t) \\ q_6(t+1) = x(t) \cdot q_7(t) + x(t) \cdot q_6(t) + q_7(t) \\ q_7(t+1) = x(t) \cdot q_0(t) + x(t) \cdot q_0(t) + q_0(t) \end{cases}$$

Теорема 2. *Пусть задана линейно реализуемая нумерованная переходная система $V = (E_2, Q, \varphi)$, где $Q = \{0, \ldots, n-1\}$. Тогда существует такое кодирование $F : Q \to E_2^k$, где $k \leq 2^n$, что переходная система V линейно реализуема посредством F.*

Доказательство. Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$, где $Q = \{0, \ldots, n-1\}$, линейно реализуемая посредством кодирования $F : Q \to E_2^k$, где $k > 2^n$. Рассмотрим матрицу кодов, задаваемых кодированием F,

$$T = \begin{pmatrix} F(0) \\ F(1) \\ \ldots \\ F(n-1) \end{pmatrix}.$$

Столбцы этой матрицы имеют длину n и состоят из 0 и 1. Число различных векторов длины n из 0 и 1 равно 2^n. Число столбцов в матрице равно k. Так как $k > 2^n$, то в данной матрице найдутся два равных столбца. Без ограничения общности считаем, что равны первый и второй столбцы, т.е. для любого $q \in Q$, из условия $(\alpha_0, \alpha_1, \ldots, \alpha_{k-1}) = F(q)$ следует, что $\alpha_0 = \alpha_1$.

Обозначим через ϕ_L линейное доопределение оператора ϕ_V^F. Согласно определению 7 доопределения оператора для всех $a \in E_2$ и $q \in Q$

$$\phi_L(a, F(q)) = \phi_V^F(a, F(q)).$$

Следовательно для функций $f_i \in \mathcal{F}_{\phi_L}, g_i \in \mathcal{F}_{\phi_V^F}$ для всех $a \in E_2$ и $q \in Q$

$$f_i(a, F(q)) = g_i(a, F(q)).$$

Причем f_i - линейные функции, где $0 \le i \le k-1$, т.е.

$$f_i(x, q_0, q_1, \ldots, q_{k-1}) = c \cdot x + \sum_{l=0}^{k-1} c_l \cdot q_l.$$

Согласно определению оператора 6 $\phi_V^F(a, F(q)) \in F(Q)$. Значит, для всех $a \in E_2$ и $q \in Q$

$$g_0(a, F(q)) = g_1(a, F(q)),$$

где $g_0, g_1 \in \mathcal{F}_{\phi_V^F}$. Поскольку для всех $a \in E_2$ и $q \in Q$

$$g_0(a, F(q)) = f_0(a, F(q)),$$

$$g_1(a, F(q)) = f_1(a, F(q)),$$

где $f_0 \in \mathcal{F}_{\phi_L}, g_0 \in \mathcal{F}_{\phi_V^F}, f_1 \in \mathcal{F}_{\phi_L}, g_1 \in \mathcal{F}_{\phi_V^F}$, верно, что для всех $a \in E_2$ и $q \in Q$

$$f_0(a, F(q)) = f_1(a, F(q)).$$

По кодированию $F : Q \to E_2^k$ построим кодирование $F' : Q \to E_2^{k-1}$ по следующему правилу: если $F(q) = (\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$, то $F'(q) = (\alpha_1, \ldots, \alpha_{k-1})$. Заметим, что по определению кодирования, если $q \ne q'$, то $F(q) = (\alpha_0, \alpha_1, \ldots, \alpha_{k-1}) \ne (\alpha'_0, \alpha'_1, \ldots, \alpha'_{k-1}) = F(q')$. Значит существует такое i, что $\alpha_i \ne \alpha'_i$.

Если $i > 0$, то $(\alpha_1, \ldots, \alpha_{k-1}) \ne (\alpha'_1, \ldots, \alpha'_{k-1})$.

Если $i = 0$, то заметим, что $\alpha_0 = \alpha_1$ и $\alpha'_0 = \alpha'_1$, и следовательно, $\alpha_1 \ne \alpha'_1$, что означает $(\alpha_1, \ldots, \alpha_{k-1}) \ne (\alpha'_1, \ldots, \alpha'_{k-1})$. Таким образом показано, что отображение F' взаимно-однозначно на Q.

По построению кодирования F' видно, что если набор $(\alpha_1, \ldots, \alpha_{k-1}) \in F'(Q)$, то набор $(\alpha_1, \alpha_1, \ldots, \alpha_{k-1}) \in F(Q)$ и $F'(\alpha_1, \ldots, \alpha_{k-1}) = F(\alpha_1, \alpha_1, \ldots, \alpha_{k-1})$.

Рассмотрим оператор переходной системы, построенный посредством кодирования F'.

$$\phi_V^{F'}(a, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}) = F'(\varphi(a, F'^{-1}(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}))) =$$

$$= F'(\varphi(a, F^{-1}(\alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}))) =$$

$$= (g_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots, g_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})),$$

где $g_i \in \mathcal{F}_{\phi_V^F}$. Последнее равенство следует из построения кодирования F' и равенства

$$F(\varphi(a, F^{-1}(\alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}))) =$$

$$= (g_0(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), g_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots,$$

$$g_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})).$$

Как было показано раннее, функции f_i и g_i равны для всех $a \in E_2$ и $q \in Q$. Следовательно, верно равенство

$$(g_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots, g_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})) =$$

$$= (f_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots, f_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})),$$

где $f_i \in \mathcal{F}_{\phi_L}$. То есть множество $\mathcal{F}_{\phi_V^{F'}}$ составляют функции, полученные из линейных операцией отождествления первого и второго аргументов. При такой операции функции остаются линейными[1].

Таким образом показано, что если переходная системы линейно реализуема посредством кодирования, которое кодирует состояния кодами длины k больше чем 2^n, то можно построить кодирование, которое кодирует состояния кодами длины $k-1$, посредством которого переходная система линейно реализуема. Повторяя данные построения, придем к кодированию, которое кодирует состояния кодами длины 2^n. □

В заключение автор выражает благодарность Алёшину Станиславу Владимировичу, чьи советы оказали неоценимую помощь в получении результатов, изложенных в данной работе.

Список литературы

[1] Яблонский С.В., *Введение в дискретную математику.* - М.:Наука,1979.

[2] А. Клиффорд, Г. Престон *Алгебраическая теория полугрупп, Том 1* -М.:Мир, 1972.

[3] Р. Лидл, Г. Нидеррайтер *Конечные поля.* - М.:Мир, 1988.

[4] М.И. Карагаполов, Ю.И. Мерзляков *Основы теории групп.* - 3-е издание-М.:Наука, 1982.

[5] М.А. Арбиб *Декомпозиция автоматов и расширение полугрупп* Алгебраическая теория автоматов, языков и полугрупп-М.“Статистика“, 1975, С.46-64

[6] Родин С.Б., *Переходные системы с максимальной вариантностью относительно кодирования состояний.* Интеллектуальные системы. Т.4, вып. 3-4. С.335-352.

[7] Родин С.Б., *О связи линейно реализуемых автоматов и автоматов с максимальной вариативностью относительно кодирования состояний.* Интеллектуальные системы. Т.20, вып. 2. С.337-347.

[8] С.В. Алешин *Алгебраические системы автоматов* -М.:МАКС Пресс, 2016

[9] Родин С.Б., *Линейно реализуемые автоматы* Дискретная математика. Т. 29, вып. 1, С.59–79