О максимально сложно реализуемых отображениях

С. Б. Родин*

Данная работа продолжает изучение вопроса сложности реализуемости автоматов посредством кодирований алфавита состояний. Ранее изучался вопрос «простой реализуемости» как автоматов, так и отображений на конечном множестве. В данной работе изучаются «сложно реализуемые» отображения на конечном множестве, т. е. такие отображения, что любое неизбыточное кодирование приводит к булеву оператору максимальной сложности с точки зрения степени полинома Жегалкина. Доказано, что для любой мощности множества $n = 2^k$ существуют «сложно реализуемые» отображения. Существование таких отображений позволит в дальнейшем доказать существование «сложно реализуемых» автоматов.

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].

Возникающий 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

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

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

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

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 заметить, что максимальность мощности множества возникающих 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 $V = (E_2, E_n, \varphi)$ посредством неизбыточного кодирования F. Данный критерий был сформулирован в терминах порождающих внутренней полугруппы переходной системы. Обозначим через p_0 отображение на n-элементном множестве, 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, выполнение свойства «аддитивного сдвига» [5] на отображениях p_0 и p_1 [3]. В работах [6] и [7] изучался вопрос линейной реализуемости отображений и было показано, что при удлинении кода любое отображение является линейно реализуемым. Однако, если ограничить длину кода минимально возможной, то сложность реализации отображения увеличится и, в общем случае, будет определяться выбором кодирования.

Данная работа посвящена вопросу существования «максимально» сложных отображений, т. е. таких что при любом кодировании оператор, построенный по отображению, имеет максимальную сложность в смысле полинома Жегалкина.

2. Основные понятия и определения

Основным объектом изучения являются отображения на множестве $E_n = \{0, \ldots, n-1\}$, где $n = 2^k$.

2.1. Булев оператор и его сложность

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

Определение 1. Пусть $\varphi : E_2^m \to E_2^k$ — булев оператор. Его можно рассматривать как набор k булевых функций, зависящих от m пе-

ременных, а именно, если $\varphi(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = (\beta_0, \beta_1, \ldots, \beta_{k-1})$, то $f_j(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = \beta_j$, где $0 \leqslant j \leqslant k-1$. Обозначим этот набор через $\mathcal{F}_\varphi = \big(f_0, f_1, \ldots, f_{k-1}\big)$.

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

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

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

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

где $\alpha_i \in E_2$.

Пример 2. Пусть дана пара функций $f_0(x_0, x_1, x_2) = x_0 \oplus x_1 \cdot x_2$

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 $f_1(x_0, x_1, x_2) = x_0 \cdot x_1 \oplus x_1 \cdot x_2 \oplus x_2$

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

Заметим, что сложность оператора из примера 1 равна 3 и сложность оператора из примера 2 равна 2.

2.2. Реализуемость отображения посредством кодирования

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

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

В данной работе будут изучаться только неизбыточные кодирования, т. е. кодирования, у которых $k =]\log_2 n[$.

Пример 3. В качестве примера неизбыточного 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	110	111	011

Выделим из всех кодирований «стандартное » кодирование.

Определение 5. Кодирование $F_0 : \{0, \dots, n-1\} \to E_2^k$ назовем *стандартным*, если код элемента есть его двоичное представление.

Пример 4. 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 $E_n = \{0, \dots, n-1\}$ по правилу $s_F(i) = F_0^{-1}(F(i))$.

Кодированию F из примера 3 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 $F_s(i) = F_0(s(i))$.

Замечание 1. *Заметим, что для неизбыточного кодирования F верно $F_{s_F} = F$.*

Замечание 2. *Заметим, что для подстановки s верно $s_{F_s} = s$.*

Пример 5. 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

Определение 6. Пусть $p : E_n \to E_n$ — отображение множества $E_n = \{0, \ldots, n-1\}$ в себя, где $n = 2^k$. Неизбыточное кодирование $F : E_n \to E_2^k$ множества E_n сопоставляет отображению p булев оператор $\varphi_p^F : E_2^k \to E_2^k$, по правилу

$$\varphi_p^F(\alpha_0, \ldots, \alpha_{k-1}) = F(p(F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))),$$

где $\alpha_0, \ldots, \alpha_{k-1} \in E_2$.

Пример 6. 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
$F(q)$	000	001	010	100	110	011	101	111

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 следующий булев оператор φ

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

Определение 7. Пусть задано отображение $p : E_n \to E_n$ и неизбыточное кодирование F множества E_n. Степенной сложностью $L_{\deg}(p, F)$ реализации отображения p посредством кодирования F назовем сложность булева оператора φ_p^F, т. е. $L_{\deg}(p, F) = L_{\deg}(\varphi_p^F)$.

Определение 8. Пусть задано отображение $p : E_n \to E_n$. Обозначим через $\mathbb{F}^{irr}$ множество всех неизбыточных кодирований множества E_n. Степенной сложностью реализации отображения p назовем минимум среди степенных сложностей реализации отображения p посредством всех неизбыточных кодирований, т. е. $L_{\deg}^{irr}(p) = \min_{F \in \mathbb{F}^{irr}}\{L_{\deg}(p, F)\}$.

Если $n = 2^k$, то отображения множества $E_n = \{0, \ldots, n-1\}$ в себя могут быть представлены как многочлены над полем Галуа $\mathbb{F}_n$ [8].

Замечание 3. *Умножение отображений осуществляется «слева направо», т. е. если заданы отображения p_1 и p_2, то значение их произведения на элементе i определяется равенством $(p_1 \cdot p_2)(i) = p_2(p_1(i))$.*

3. Основные результаты

В работе [3] была доказана лемма

Лемма 1. *Пусть задано отображение p множества $E_n = \{0, \ldots, n-1\}$ в себя, где $n = 2^k$. Булев оператор, сопоставляемый кодированием F отображению p, совпадает с булевым оператором, который кодирование F_0 сопоставляет отображению $s_F^{-1} \cdot p \cdot s_F$.*

Данная лемма утверждает, что для получения всех булевых операторов для данного отображения вместо перебора всевозможных кодирований можно рассмотреть только стандартное кодирование для отображений, полученных сопряжением с помощью всевозможных перестановок, т. е. перестановка, задающая сопряжение, и кодирование в некотором смысле «эквивалентны». С помощью этой леммы докажем утверждение, что для двух отображений, являющихся сопряжением друг друга, можно найти кодирования, которые сопоставляют им одинаковый булев оператор, т. е. такие отображения порождают «одинаковое» множество операторов.

Лемма 2. *Пусть заданы отображение p на множестве E_n, взаимнооднозначное отображение $s : E_n \to E_n$ и неизбыточное кодирование F множества E_n. Тогда верно, что булев оператор φ_p^F, получаемый по отображению p посредством кодирования F, равен булеву оператору $\varphi_{s^{-1}\cdot p\cdot s}^{\tilde{F}}$, получаемому по отображению $s^{-1}\cdot p\cdot s$ посредством кодирования $\tilde{F} = F_{s^{-1}\cdot s_F}$.*

Доказательство. Согласно лемме 1 булев оператор, сопоставляемый неизбыточным кодированием F отображению p, совпадает с булевым оператором, который кодирование F_0 сопоставляет отображению $s_F^{-1}\cdot p\cdot s_F$.

Также согласно этому утверждению булев оператор, сопоставляемый неизбыточным кодированием $\tilde{F} = F_{s^{-1}\cdot s_F}$ отображению $s^{-1}\cdot p\cdot s$ совпадает с булевым оператором, который кодирование F_0 сопоставляет отображению $s_{\tilde{F}}^{-1}\cdot s^{-1}\cdot p\cdot s\cdot s_{\tilde{F}}$. Заметим, что $s_{\tilde{F}} = s^{-1}\cdot s_F$, так как кодирование $\tilde{F}$ определяется перестановкой $s^{-1}\cdot s_F$ (см. замечание 1).

Следовательно, верно, что

$$s_{\tilde{F}}^{-1}\cdot s^{-1}\cdot p\cdot s\cdot s_{\tilde{F}} = (s^{-1}\cdot s_F)^{-1}\cdot s^{-1}\cdot p\cdot s\cdot s^{-1}\cdot s_F =$$

$$= s_F^{-1}\cdot s\cdot s^{-1}\cdot p\cdot s\cdot s^{-1}\cdot s_F = s_F^{-1}\cdot p\cdot s_F.$$

Следовательно, булев оператор, сопоставляемый неизбыточным кодированием $\tilde{F} = F_{s^{-1}\cdot s_F}$ отображению $s^{-1}\cdot p\cdot s$ совпадает с булевым оператором, который кодирование F_0 сопоставляет отображению $s_F^{-1}\cdot p\cdot s_F$. Отсюда следует утверждение леммы. □

Пусть задано отображение p на множестве E_n. Обозначим через Φ_p^{irr} множество всех операторов, сопоставляемых всевозможными неизбыточными кодированиями отображению p.

Следствие 1. *Пусть заданы отображение p на множестве $E_n = \{0,\dots,n-1\}$ и взаимно-однозначное отображение $s : E_n \to E_n$. Множества булевых операторов Φ_p^{irr} и $\Phi_{\tilde{p}}^{irr}$, где $\tilde{p} = s^{-1}\cdot p\cdot s$, совпадают.*

Доказательство. Поскольку $\tilde{p} = s^{-1} \cdot p \cdot s$, то согласно лемме 2 $\Phi_p^{irr} \subseteq \Phi_{\tilde{p}}^{irr}$. Поскольку $p = s \cdot \tilde{p} \cdot s^{-1}$, то согласно лемме 2 $\Phi_{\tilde{p}}^{irr} \subseteq \Phi_p^{irr}$. А следовательно эти два множества равны. □

Определение 9. Весом булевой функции $f(x_0, x_1, \ldots, x_{k-1}) : E_2^k \to E_2$ назовем число наборов, на которых она принимает значение 1.

Лемма 3. *Полином Жегалкина булевой функции* $f(x_0, x_1, \ldots, x_{k-1}) : E_2^k \to E_2$ *веса 1 имеет степень* k.

Доказательство. Поскольку вес функции f равен 1, то она принимает значение 1 на одном наборе. Обозначим этот набор через $(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$. Тогда СДНФ функции f имеет вид

$$f(x_0, x_1, \ldots, x_{k-1}) = x_0^{\alpha_0} \cdot x_1^{\alpha_1} \cdot \ldots \cdot x_{k-1}^{\alpha_{k-1}}.$$

Каждый множитель есть либо x_i, если $\alpha_i = 1$, либо $x_i \oplus 1$, если $\alpha_i = 0$. Обозначим через $(\beta_0, \beta_1, \ldots, \beta_{k-1})$ такой набор, что $\beta_i = \overline{\alpha_i},\ i \in \{0, \ldots, k-1\}$. Тогда формулу для f можно переписать как

$$f(x_0, x_1, \ldots, x_{k-1}) = (x_0 \oplus \beta_0) \cdot (x_1 \oplus \beta_1) \cdot \ldots \cdot (x_{k-1} \oplus \beta_{k-1}).$$

Многочлен такого вида содержит слагаемое $x_0 \cdot x_1 \cdot \ldots \cdot x_{k-1}$. Данное утверждение можно доказать по индукции.

База индукции: Если $k = 1$, то многочлен имеет вид либо x, либо $x \oplus 1$ и утверждение верно.

Шаг индукции: Пусть утверждение доказано для $k-1$, тогда произведение первых $k-1$ скобок можно записать как $x_0 \cdot x_1 \cdot \ldots \cdot x_{k-2} \oplus g(x_0, x_1, \ldots, x_{k-2})$, где $\deg(g(x_0, x_1, \ldots, x_{k-2})) < k-1$. Произведение всех k скобок можно записать как

$$(x_0 \cdot x_1 \cdot \ldots \cdot x_{k-2} \oplus g(x_0, x_1, \ldots, x_{k-2})) \cdot (x_{k-1} \oplus \beta_{k-1}),$$

где $\deg(g(x_0, x_1, \ldots, x_{k-2})) < k-1, \beta_{k-1} \in \{0, 1\}$. В результате раскрытия скобок получим выражение

$$x_0 \cdot x_1 \cdot \ldots \cdot x_{k-2} \cdot x_{k-1} \oplus g(x_0, x_1, \ldots, x_{k-2}) \cdot x_{k-1} \oplus$$
$$\oplus \beta_{k-1} \cdot x_0 \cdot x_1 \cdot \ldots \cdot x_{k-2} \oplus \beta_{k-1} \cdot g(x_0, x_1, \ldots, x_{k-2}).$$

При этом степень второго, третьего и четвертого слагаемых меньше чем k, а следовательно полученное выражение содержит слагаемое $x_0 \cdot x_1 \cdot \ldots \cdot x_{k-1}$, т. е. полином Жегалкина функции f имеет степень k. □

Следствие 2. *Полином Жегалкина булевой функции* $f(x_0, x_1, \ldots, x_{k-1}) : E_2^k \to E_2$ *веса* $2^k - 1$ *имеет степень* k.

Доказательство. Поскольку вес функции f равен $2^k - 1$, то функция f принимает значение 0 только на одном наборе, а на остальных наборах — значение 1. Тогда функция $\overline{f}$ принимает значение 1 только на одном наборе, а на остальных наборах — значение 0. Обозначим ее через g. Согласно лемме 3 полином Жегалкина функции g содержит слагаемое $x_0 \cdot x_1 \cdot \ldots \cdot x_{k-1}$, т. е.

$$g(x_0, x_1, \ldots, x_{k-1}) = x_0 \cdot x_1 \cdot \ldots \cdot x_{k-1} \oplus h(x_0, x_1, \ldots, x_{k-1}),$$

где $deg(h) < k$. Поскольку $g(x_0, x_1, \ldots, x_{k-1}) = \overline{f}(x_0, x_1, \ldots, x_{k-1})$, то верно равенство

$$\begin{aligned} f(x_0, x_1, \ldots, x_{k-1}) &= g(x_0, x_1, \ldots, x_{k-1}) \oplus 1 = \\ &= x_0 \cdot x_1 \cdot \ldots \cdot x_{k-1} \oplus h(x_0, x_1, \ldots, x_{k-1}) \oplus 1, \end{aligned}$$

где $deg(h) < k$. □

Теорема 1. *Пусть задано отображение* p *на множестве* $E_n = \{0, \ldots, n-1\}$, *где* $n = 2^k$, *соответствующее полиному Галуа* $c \cdot x^{n-1} + a$, *где* $c, a \in E_n, c \neq 0$. *Степенная сложность реализации отображения* p *посредством любого неизбыточного кодирования* F *равна* k, *т. е.* $L_{deg}^{irr}(p) = k$.

Доказательство. Заметим, что согласно операции умножения в поле Галуа, $0^{n-1} = 0$. Поскольку ненулевые элементы поля Галуа образуют относительно операции умножения циклическую группу порядка $n-1$, любой ненулевой элемент поля Галуа в степени $n-1$ есть 1. Следовательно, многочлен x^{n-1} соответствует отображению

$$p_{x^{n-1}} = \begin{pmatrix} 0 & 1 & 2 & \ldots & n-1 \\ 0 & 1 & 1 & \ldots & 1 \end{pmatrix}.$$

Многочлен $c \cdot x^{n-1} + a$ соответствует отображению

$$p_{c \cdot x^{n-1} + a} = \begin{pmatrix} 0 & 1 & 2 & \ldots & n-1 \\ a & b & b & \ldots & b \end{pmatrix},$$

где $b = c + a$. Заметим, что поскольку $c \neq 0$, то $b \neq a$.

Пусть задано неизбыточное кодирование $F : E_n \to E_2^k$. Введем обозначения: $F(0) = (\gamma_0, \gamma_1, \ldots, \gamma_{k-1})$, $F(a) = (\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$, $F(b) = (\beta_0, \beta_1, \ldots, \beta_{k-1})$. По отображению $p_{c \cdot x^{n-1} + a}$ и кодированию F построим таблицу

x_0	x_1	$\dots$	x_{k-1}	y_0	y_1	$\dots$	y_{k-1}
0	0	$\dots$	0	β_0	β_1	$\dots$	β_{k-1}
0	0	$\dots$	1	β_0	β_1	$\dots$	β_{k-1}
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
γ_0	γ_1	$\dots$	γ_{k-1}	α_0	α_1	$\dots$	α_{k-1}
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
1	1	$\dots$	1	β_0	β_1	$\dots$	β_{k-1}

Множество индексов $\{0, 1, \dots, k-1\}$ можно разделить на два подмножества. Первое множество M_1 содержит такие i, что $\alpha_i = \beta_i$. Второе множество M_2 содержит такие i, что $\alpha_i \neq \beta_i$. Множество M_2 не пусто в силу определения кодирования и неравенства $b \neq a$.

Для $i \in M_1$ верно, что $y_i = \alpha_i$, т. е. функция константа.

Если $i \in M_2$, то функция $y_i = f_i(x_0, \dots, x_{k-1})$ обладает тем свойством, что на одном наборе она принимает значение α_i, на остальных β_i, причем $\alpha_i \neq \beta_i$. Согласно лемме 3 и следствию 2 полином Жегалкина функции $f_i(x_0, \dots, x_{k-1})$ содержит слагаемое $x_0 \cdot x_1 \cdot \ldots \cdot x_{k-1}$. А значит $L_{deg}(p_{c \cdot x^{n-1}+a}, F) = k$. В силу произвольности выбора кодирования F верно, что $L^{irr}_{deg}(p_{c \cdot x^{n-1}+a}) = k$. □

Следствие 3. *Пусть задано отображение p на множестве $E_n = \{0, \dots, n-1\}$, где $n = 2^k$, соответствующее полиному Галуа $c \cdot x^{n-1} + a$, $c \neq 0$. Тогда для любого взаимно-однозначного отображения $s : E_n \to E_n$ степенная сложность реализации отображения $s^{-1} \cdot p \cdot s$ равна k.*

Доказательство. Утверждение следует из теоремы 1 и следствия 1. □

4. Заключение

В работе изучался вопрос степенной сложности реализации отображения посредством неизбыточных кодирований. В ходе исследования были получены следующие основные результаты:

- Доказана лемма об эквивалентности множеств булевых операторов для сопряженных отображений. Показано, что если два отображения изоморфны с точностью до перестановки элементов (являются сопряженными), то порождаемые ими классы булевых операторов полностью совпадают, а их минимальные степенные сложности равны ($L^{irr}_{\deg}(p) = L^{irr}_{\deg}(s^{-1} \cdot p \cdot s)$). Это свойство позволяет существенно сузить пространство поиска при классификации отображений по их сложности.

- На основе полученных свойств веса функций найдена точная нижняя оценка сложности для специального класса мономов над конечными полями Галуа $\mathbb{F}_n$ (где $n = 2^k$). Доказано, что для любого отображения, представимого в виде полинома $c \cdot x^{n-1} + a$ ($c \neq 0$), степенная сложность реализации равна k при *любом* выборе неизбыточного двоичного кодирования.

Предметом дальнейшего исследования будет задача нахождения всех отображений, имеющих максимальную сложность реализации, а также поиск критерия данного свойства.

Заметим, что для задания переходной системы с одним бинарным входом достаточно указать пару отображений: одно — соответствующее входному символу 0, другое — соответствующее входному символу 1. Сложность реализации переходной системы будет не ниже, чем сложность каждого из отображений. А потому представляется возможным доказать существование «максимально сложных» переходных систем с использованием построенных отображений.

Также планируется продолжить исследование в области линейной реализации отображений. Ранее в работах [6] и [7] было показано, что при использовании кода длины n, любое отображение на n-элементном множестве является линейно реализуемым. Следовательно, и отображения, построенные в данной работе и имеющие максимальную степенную сложность при неизбыточном кодировании, также являются линейно реализуемыми при использовании кода длины n.

Рассмотрим отображение $p_{x^{n-1}}$ для $n = 8$

$$p_{x^7} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Можно заметить, что при использовании кодирования F, задаваемого таблицей:

q	0	1	2	3	4	5	6	7
$F(q)$	1111	0000	0010	0100	0110	1000	1010	1100

отображение p_{x^7} является линейно реализуемым, так как соответствующий оператор имеет вид:

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	1	0	0	0	0	0
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	1	1	0	0	0	0	0
1	0	1	0	0	0	0	0
1	1	1	1	1	1	1	1

и может быть доопределен как:

$$\begin{aligned} y_0 &= x_3, \\ y_1 &= x_3, \\ y_2 &= x_3, \\ y_3 &= x_3. \end{aligned}$$

Соответственно, возникает задача найти минимальное удлинение кода, при котором отображение допускает линейную реализуемость.

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 (2017), 59–79.

[4] Родин С.Б., “О связи линейно реализуемых автоматов и автоматов с максимальной вариативностью относительно кодирования состо-

яний", *Интеллектуальные системы. Теория и приложения*, **20**:2 (2016), 337–347.

[5] Родин С.Б., "О свойстве аддитивного сдвига для линейной реализуемости автоматов", *Интеллектуальные системы. Теория и приложения*, **28**:2 (2024), 52–66.

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

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

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

Статья поступила 28 апреля 2026 г.

Mappings with maximum implementation complexity

S. B. Rodin

The paper continues the investigation into the complexity of automata implementation via state encoding. Previous research was focused on the identification of "simple implementations" of automata and mappings on a finite set. This paper is devoted to mappings with "complex implementations", i.e., mappings for which any irredundant encoding yields a Boolean operator of maximum complexity in terms of the Zhegalkin polynomial degree. It is proved that for any set cardinality $n = 2^k$ such mappings exist. These mappings can be used in future research to prove that automata admitting only "complex implementations" also exist.

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 (in Russian).

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

[3] Sergey B. Rodin., "Linearly realizable automata", *Discrete Mathematics and Applications*, **27**:6 (2017), 387–402. DOI: 10.1515/dma-2017-0039.

[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 (in Russian).

[5] Rodin S.B., "On the additive shift property for the linear realizability of automata", *Intelligent systems. Theory and Applications*, **28**:2 (2024), 52–66 (in Russian).

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

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

[8] R. Lidl, H. Niederreiter, *Finite fields*. V. 1, Mir, Moscow, 1988 (in Russian), 430 pp.

Received on April 28, 2026