О линейной реализуемости переходных систем по входной переменной

С. Б. Родин*

Данная работа посвящена изучению вопроса «простой»реализации переходной системы посредством кодирования. В общем случае переход от абстрактного автомата к булеву оператору осуществляется с помощью кодирования входного алфавита, алфавита состояний и выходного алфавита. Входные переменные полученного оператора можно разбить на два множества: одно соответствует коду входного символа, второе — коду состояния. Это позволяет рассмотреть свойство линейной реализуемости по каждому множеству отдельно.

В статье исследуется вопрос линейной реализуемости относительно входной переменной. Доказан критерий, согласно которому свойство аддитивного сдвига [1] для порождающих внутренней полугруппы переходной системы является необходимым и достаточным условием линейной реализуемости по входной переменной независимо от длины кода.

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. Переход к описанию на языке схем осуществляется с помощью кодирования алфавита состояний, входного алфавита и выходного алфавита в алфавите $E_2 = \{0, 1\}$. 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 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

* *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

простейшими с точки зрения такой сложности являются операторы, полиномы Жегалкина которых имеют степень не выше первой, или линейные булевы функции.

В статье [3] был доказан критерий линейной реализуемости переходной системы $V = (E_2, E_n, \varphi)$ посредством неизбыточного кодирования F. Однако переходные системы, которые не являлись линейно реализуемыми для неизбыточных кодирований, при увеличении длины кода могут приводить к линейным булевым операторам. Множество переменных булева оператора можно разбить на два множества, первое соответствует коду входного символа, второе — коду состояния переходной системы. Вопрос линейной реализуемости можно рассмотреть по каждому из этих множеств отдельно. В данной работе изучается вопрос линейной реализуемости по переменным, соответствующим входному символу. При этом ограничений сверху на длину кодирования не накладывается.

2. Основные понятия и определения

Основным объектом изучения являются переходные системы $V = (E_2, E_n, \varphi)$, где $n = 2^k$.

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

Определение 2. Оператор $\widehat{\Phi} : E_2^m \to E_2^l$, $m, l \in \mathbb{N}$ назовем *доопределением оператора* $\Phi : R \to {E_2}^l$, где $R \subseteq E_2^m$, если для каждого $(\alpha_0, \ldots, \alpha_{m-1}) \in R$ верно $\Phi(\alpha_0, \ldots, \alpha_{m-1}) = \widehat{\Phi}(\alpha_0, \ldots, \alpha_{m-1})$.

Определение 3. *Кодированием множества* E_n назовем взаимно однозначное отображение (вложение) $F : E_n \to E_2^k$, где $k \geqslant]\log_2 n[$.

Определение 4. Каждое кодирование $F : E_n \to E_2^k$ множества E_n переходной системы (E_2, E_n, φ) порождает булев оператор $\Phi_V^F : E_2 \times R \to R$, где $R = F(E_n) \subseteq E_2^k$, по правилу $\Phi_V^F(x_0, x_1, \ldots, x_k) = F(\varphi(x_0, F^{-1}(x_1, \ldots, x_k)))$, где $x_0 \in E_2, (x_1, \ldots, x_k) \in R$.

Определение 5. Булева функция $f(x_0, x_1, \ldots, x_{k-1}) : E_2^k \to E_2$ от k переменных называется линейной по переменной x_i, если она представима в виде $f(x_0, x_1, \ldots, x_{k-1}) = a \cdot x_i \oplus g(x_0, \ldots x_{i-1}, x_{i+1}, \ldots, x_{k-1})$, где $a \in E_2$, g - булева функция, зависящая от переменных $x_0, \ldots x_{i-1}, x_{i+1}, \ldots, x_{k-1}$.

Определение 6. Назовем переходную систему *линейно реализуемой по входной переменной*, если для заданной переходной системы $V = (E_2, E_n, \varphi)$ 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 функциями алгебры логики, линейными по входной переменной x_0.

3. Основные результаты

Обозначим через P_n множество отображения E_n в себя. Если $n = 2^k$, то отображения множества E_n в себя могут быть представлены как многочлены над полем Галуа $\mathbb{F}_n$ [2]. Обозначим через $H_+ \subset P_n$ множество подстановок, соответствующих многочленам вида $x + c$ над полем Галуа $\mathbb{F}_n$, где $c \in E_n$ — константа.

Пусть задана переходная система $V = (E_2, E_n, \varphi)$. Обозначим через $X_V = \{s : E_n \to E_n \mid \exists a \in E_2, s(q) = \varphi(a, q) \quad \forall q \in E_n\}$. Заметим, что множество X_V состоит не более чем из двух элементов. Обозначим через p_0 отображение, задаваемое входным символом 0, а через p_1 — отображение, задаваемое входным символом 1.

Множество $S_V = \langle X_V \rangle$ называется *внутренней полугруппой* переходной системы V.

Определение 7. Пусть задана переходная система $V = (E_2, E_n, \varphi)$. Назовем порождающие p_0 и p_1 связанными посредством аддитивного сдвига, если существует взаимно однозначное отображение $s : E_n \to E_n$ такое, что для порождающих верно соотношение $p_1 = p_0 \cdot h$, где $h \in s^{-1} \cdot H_+ \cdot s$

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 $(p_1 \cdot p_2)(i) = p_2(p_1(i))$.

Теорема. *Пусть задана переходная система $V = (E_2, E_n, \varphi)$. Переходная система является линейно реализуемой по входной переменной тогда и только тогда, когда порождающие p_0 и p_1 связанны аддитивным сдвигом.*

Список литературы

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

[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.

Статья поступила 29 октября 2026 г.

Transition systems linearly realizable with respect to the input variable

S. B. Rodin

This paper continues the investigation into the complexity of semiautomata realization via states encoding, namely the property of linear realizability of semiautomaton. Encoding of the semiautomaton alphabets induces a Boolean operator. Arguments of the Boolean operator might be separated into two sets. The first one corresponds to the code of the input alphabet, the second one corresponds to the code of the alphabet of states. The property of the linear realizability with respect to each subset of variables can be studied separately.

This paper studies the property of linear realizability with respect to input variables. It is proven that "additive shift" [1] property for generators of the inner semigroup p_0 and p_1 is a necessary and a sufficient condition for semiautomaton to be linearly realizable by input variable regardless of the code length. This means that code length increasing will not induce linear realizability if "additive shift" property is not fulfilled for generators of the inner semigroup.

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

References

[1] 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).

[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.

Received on October 29, 2026