О связи линейно реализуемых автоматов и автоматов с максимальной вариативностью относительно кодирования состояний

С. Б. Родин

В работе изучается как связаны класс автоматов, являющихся «просто» реализуемыми, с классом автоматом, обладающим свойством, что все операторы, задаваемые всевозможными кодированиями, являются различными. Показывается, что указанные классы автоматов имеют не пустое пересечение, и ни один из классов не лежит в другом.

Ключевые слова: автомат, кодирование, свойство максимальности.

Введение

На практике часто необходимо 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 $\{0, 1\}$.

В работе изучаются автоматы специального вида, т.н. автоматы без выхода или переходные системы. С формальной точки

зрения переходная система это тройка $V = (A, Q, \varphi)$, где A-входной алфавит, Q-алфавит состояний, φ функция, которая по текущему входу и состоянию определяет состояние переходной системы в следующий момент времени. Кодирование алфавита состояния - это отображение алфавита Q в ${E_2}^k$, при котором каждому состоянию из Q ставится в соотвествие вектор из ${E_2}^k$. Соотвественно кодирование входного алфавита - это отображение алфавита A в ${E_2}^p$, при котором каждому элементу из A ставится в соотвествие вектор из ${E_2}^p$. При этом функции перехода φ преобразуется в булевский оператор $\phi : {E_2}^{p+k} \to {E_2}^k$, где p-длина кодового набора символов множества A, k-длина кодового набора символов множества Q.

С одной стороны можно рассмотреть переходные системы, у которых существует кодирование, такое что получаемые при данном кодировании, булевские функции являются линейными. Такие переходные системы называются линейно реализуемыми. В работе [6] были изучены такие переходные системы. В частности доказано необходимое условие линейной реализуемости в терминах порождающих внутренней полугруппы автомата.

С другой стороны интерес представляют такие переходные системы, что все операторы, задаваемые всевозможными кодированиями, являются различными. Данное свойство называется свойством максимальности. В работе [5] изучаются переходные системы со свойством «максимальности», в ней приведен критерий этого свойства в терминах порождающих внутренней полугруппы автомата.

Основной задачей данной работы было установить как взаимосвязаны классы автоматов, обладающих данными свойствами. Было показано, что данные классы имеют не пустое пересечение, и ни один из классов не лежит в другом.

Основные понятия и определения

Определение 1. *Нумерованной переходной системой назовем тройку* (A, Q, φ)*, где* A*-входной алфавит,* $Q = \{0...n-1\}$*,*

φ - функция переходов.

В работе изучаются нумерованные переходные системы с входным алфавитом $A = E_2$ и числом состояний $n = 2^k$.

Определение 2. *Кодированием множества $Q = \{0...n-1\}$ назовем взаимоднозначное отображение $F : \{0...n-1\} \to {E_2}^k$*

Каждое кодирование F для переходной системы на множестве Q
порождает булевский оператор [1] $\phi : {E_2}^{k+1} \to {E_2}^k$,где

$$\phi(a, \alpha_1, ..., \alpha_k) = F(\varphi(a, F^{-1}(\alpha_1, ..., \alpha_k))), a \in A, \alpha_i \in E_2.$$

Данный оператор может быть рассмотрен как набор k булевских функций, зависящих от $k+1$ переменной. Обозначим этот набор через $\mathcal{F}_V(F)$.

Определение 3. *Если для заданной нумерованной переходной системы V существует кодирование F, такое что все элементы $\mathcal{F}_V(F)$ являются линейными функциями алгебры логики, назовем такую переходную систему линейно реализуемой посредством кодирования F,или просто линейно реализуемой.*

Обозначим через $L(n)$ множество линейно реализуемых нумерованных переходных систем с n состояниями.

Выделим из всех кодирований "стандартное"кодирование.

Определение 4. *Пусть $n = 2^k$. Кодирование $F_0 : \{0...n-1\} \to {E_2}^k$ назовем стандартным, если код элемента есть его двоичное представление.*

Обозначим через $X_V = \{s : Q \to Q | \exists a \in E_2, s(q) = \varphi(a,q)$ для $\forall q \in Q\}$ А через $S_V =< X_V >$, замыкание множества X_V относительно операции умножения подстановок. [4]
Замечание: Отображение $p : Q \to Q$ будем называть подстановкой. Биективное отображение $s : Q \to Q$ будем назвать перестановкой.

Определение 5. *S_V назовем внутренней полугруппой переходной системы V. X_V порождающее множество внутренней полугруппы. [4]*

Поскольку входной алфавит E_2, то множество X_V состоит из двух элементов. Обозначим через p_0 подстановку, соответствующую входному символу 0, через p_1 подстановку, соответствующую входному символу 1.

По аналогии с булевским оператором, построенным по заданной переходной системе с помощью некоторого кодирования, можно определить булевский оператор для отдельной подстановки. И ввести понятие линейной реализуемости подстановки.

Определение 6. *Пусть задана некоторая подстановка на множестве $Q = \{0, ..., n-1\}$, $s : Q \to Q$. Кодирование F множества Q, определяет по подстановке s, булевский оператор ϕ_s по правилу*

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

где $\alpha_1, ..., \alpha_{k-1} \in E_2$,$k = log_2(n)$. Данный оператор может быть рассмотрен как набор k булевских функций, зависящих от k переменной. Обозначим этот набор через $\mathcal{F}_s(F)$.

Определение 7. *Подстановка называется линейно реализуемой, посредством кодирования F, если набор $\mathcal{F}_s(F)$ состоит из линейных булевских функций.*

Введем несколько обозначений.
Пусть $n = 2^k$, то подстановки на множестве $Q = \{0...n-1\}$ могут быть представлены как многочлены над полем Галуа F_{2^k} [1]. Обозначим через H_+ перестановки, соответствующие многочленам $x + c$ над полем Галуа F_n, где $c \in E_n$ - константа.
Порядок умножения подстановок слева направо. То есть если заданы перестановки p_1 и p_2, то значение их произведения на элементе i есть $(p_1 \cdot p_2)(i) = p_2(p_1(i))$.

Сформулируем необходимое условие линейной реализуемости нумерованной переходной системы, полученное в работе [6].

Теорема 1. *Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$, где $Q = \{0, \ldots, n-1\}$, где $n = 2^k$. Если V линейно реализуема посредством кодирования $F : Q \to E_2^k$, то существует подстановка c и перестановка s такие, что $p_0 = c \cdot h_1$, $p_1 = c \cdot h_2$, где $h_1, h_2 \in s^{-1} \cdot H_+ \cdot s$.*

Определение 8. *Будем говорить, что нумерованная переходная система $V = (E_2, Q, \varphi)$ с n состояниями обладает свойством максимальности, если все операторы, задаваемые всевозможными ее кодированиями, различны.*

Обозначим через $M(n)$ множество нумерованных переходных систем с n состояниями, обладающих *свойством максимальности*.

Сформулируем результаты, полученные в работе [5].

Теорема 2. *Нумерованная переходная система $V = (E_2, Q, \varphi)$ не обладает свойством максимальности, тогда и только тогда, существует нетривиальная перестановка s, такая что $s \cdot p_0 = p_0 \cdot s$ и $s \cdot p_1 = p_1 \cdot s$.*

Следствие 1. *Нумерованная переходная система $V = (E_2, Q, \varphi)$ обладает свойством максимальности, тогда и только тогда, не существует нетривиальной перестановки s, такой что $s \cdot p_0 = p_0 \cdot s$ и $s \cdot p_1 = p_1 \cdot s$.*

Лемма 1. *Пусть задана перестановка* $s = (i_1, ..., i_l)$, *где* $Q_1 = \{i_1, ..., i_l\}$. *Обозначим через* $Q_2 = Q \setminus Q_1$. *Тогда подстановка* p, *с ней коммутирующая, имеет один следующих видов:либо*

$$p = \begin{pmatrix} \dots i_1 \dots i_l \dots \\ \dots s^m(i_1) \dots s^m(i_l) \dots \end{pmatrix},$$

$$\textit{где } 0 \leq m \leq l-1, \forall j \in Q_2, s(j) \in Q_2; \qquad (1)$$

либо

$$p = \begin{pmatrix} \dots i_1 \dots i_l \dots \\ \dots k \dots k \dots \end{pmatrix}, \textit{где } k \in Q_2, \forall j \in Q_2, s(j) \in Q_2 6; \qquad (2)$$

Основные результаты

$M(n) \setminus L(n)$

Для произвольного $n = 2^k$ приведем пример переходной системы обладающей *свойством максимальности*, но не являющейся линейно реализуемой. Рассмотрим нумерованную переходную систему
$V = (E_2, \{0, 1, \dots, n-1\}, \varphi)$, чья функция переходов определяется как:

$$\varphi(0,0) = 1$$

$$\varphi(0,1) = 0$$

$$\varphi(0,q) = q, 3 \leq q \leq n-1$$

$$\varphi(1,q) = q + 1 \, mod \, n$$

Нетрудно видеть,что порождающие внутренней полугруппы имееют вид:

$$p_0 = (0\,1)$$

$$p_1 = (0\,1\,\dots\,n-1)$$

Ниже изображена диаграмма переходов данной переходной системы.

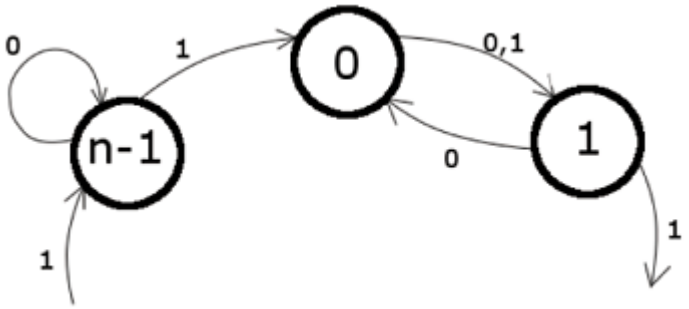

Рис. 1. Переходная система, обладающая *свойством максимальности*, но не являющейся линейно реализуемой

Согласно теореме 2 переходная система не обладает *свойством максимальности*, если найдется нетривиальная перестановка s, коммутирующая с p_0 и p_1. Согласно лемме 1 перестановка s_{p_0}, коммутирующая с p_0, обладает следующим свойством, либо $s_{p_0}(0) = 0, s_{p_0}(1) = 1$, либо $s_{p_0}(0) = 1, s_{p_0}(1) = 0$. Согласно лемме 1 перестановка s_{p_1}, коммутирующая с p_1, обладает следующим свойством, $s_{p_0}(i) = p_1^k(i)$. С учетом данных замечаний построим перестановку s, коммутирующую с p_0 и p_1. Из условия, что s коммутирует с p_0, либо $s(0) = 0, s(1) = 1$, тогда из условия, что перестановка s коммутирует с p_1, имеем $s(i) = i, \forall i \in Q$. Следовательно перестановка s тождественная. Еще один возможный случай $s(0) = 1, s(1) = 0$, но из условия, что перестановка s коммутирует с p_1 имеем, что $s(1) = p_1(1) = 2$. Мы пришли к противоречию. Единственная перестановка, коммутирующая с p_0 и p_1, это тождественная перестановка. Согласно Следствию из теоремы 2, данная переходная система обладает *свойством максимальности*.

Теперь покажем, что данная переходная система не является линейно реализуемой. Согласно теореме 1 если переходная система V линейно реализуема, то $p_0 = c \cdot h_1$, $p_0 = c \cdot h_2$, где $h_1, h_2 \in s^{-1}H_+s$. Тогда $p_0^{-1} \cdot p_1 \in s^{-1}H_+s$. Для заданной переходной системы $p_0^{-1} \cdot p_1 = (0\,1)(0 \ldots n-1) = (0\,2 \ldots n-1)$, то

есть это цикл длины $n-1$. Перестановки принадлежащие H_+ представляют произведение $n/2$ транспозиций. Поскольку при сопряжении цикловая структура перестановок сохраняется [3], $\nexists s, \nexists h \in H_+$ таких, что $p_0^{-1} \cdot p_1 = s^{-1} \cdot h \cdot s$. Откуда следует, что данная переходная система не является линейно реализуемой.

$L(n) \setminus M(n)$

Для произвольного $n = 2^k$ приведем пример линейно реализуемой переходной системы, но не обладающей *свойством максимальности*. Рассмотрим нумерованную переходную систему $V = (E_2, Q = \{0, 1, \ldots, n-1\}, \varphi)$, чья функция переходов определяется как:

$$\varphi(0, q) = 0, \forall q \in Q$$

$$\varphi(1, q) = 1, \forall q \in Q$$

На рисунке 2 приведена диаграмма переходов данной переходной системы.

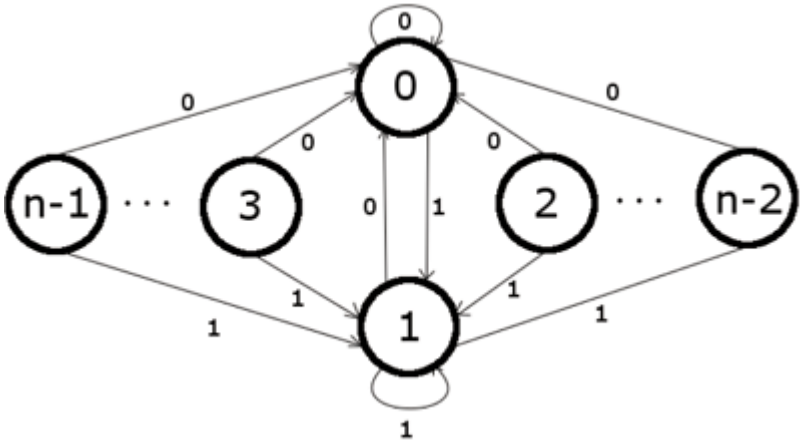

Рис. 2. Линейно реализуемая переходная система, не обладающая *свойством максимальности*

Построим булевский оператор для "стандартного"кодирования F_0. Нетрудно видеть, что $\mathcal{F}_V(F_0) = \{f_i(x, q_0, q_1, \ldots, q_{n-1}) =$

$x, 0 \leq i \leq k-1\}$, где $x \in E_2$ - входная буква, $(q_0, q_1, \ldots q_{n-1})$ - код состояния при "стандартном"кодировании F_0.
Теперь покажем, что перестановка $s = (2\,3 \ldots n-1)$ коммутирует с p_0 и p_1. Действительно $s(p_0(i)) = s(0) = 0, \forall i \in Q$. С другой стороны $p_0(s(i)) = 0, \forall i \in Q$, так образ любого элемента при действии подстановки p_0 есть 0. Аналогично $s(p_1(i)) = s(1) = 1 = p(s(i)), \forall i \in Q$. Следовательно переходная система не обладает *свойством максимальности*.

$M(n) \bigcap L(n)$

Для произвольного $n = 2^k$ приведем пример линейно реализуемой переходной системы, обладающей *свойством максимальности*. Обозначим через c перестановку, соответствующую многочлену $2 \cdot x$ над полем Галуа F_n. Данная перестановка представляет собой цикл длины $n-1$. Обозначим через h перестановку, соответствующую многочлену $x+1$ над полем Галуа F_n. Данная перестановка имеет следующий вид $(0\,1)(2\,3)\ldots(n-2\,n-1)$
Рассмотрим нумерованную переходную систему
$V = (E_2, \{0, 1, \ldots, n-1\}, \varphi)$, чья функция переходов определяется как:

$$\varphi(0, q) = c(q)$$

$$\varphi(1, q) = h(c(q))$$

В работе [6] при доказательстве теоремы 5 было показано, что подстановка, линейно реализуема посредством стандартного кодирования F_0, тогда и только тогда, когда соответствующий ему многочлен над полем Галуа F_{2^k} является линейной комбинацией многочленов вида x^{2^i}, где $i = 0, .., k-1$ и константы $c \in F_{2^k}$. Следовательно набор $\mathcal{F}_c(F_0) = \{f_i^c(q_0, q_1, \ldots, q_{n-1}), 0 \leq i \leq k-1\}$, где $(q_0, q_1, \ldots q_{n-1})$ - код состояния при «стандартном» кодировании F_0, состоит из линейных функций. Принимая во внимание, что $\mathcal{F}_h(F_0) = \{f_i^h(q_0, q_1, \ldots, q_{n-1}) = x + h_i, 0 \leq i \leq k-1\}$, где $(h_0, h_1, ...h_k) = F_0(1)$, несложно видеть, что $\mathcal{F}_V(F_0) = \{f_i(x, q_0, q_1, \ldots, q_{n-1}) = f_i^c(x, q_0, q_1, \ldots, q_{n-1}) + h_i, 0 \leq i \leq k-1\}$, где $x \in E_2$ - входная буква, $(q_0, q_1, \ldots q_{n-1})$ - код состояния при

«стандартном» кодировании F_0. Отсюда следует, что заданная переходная система является линейно реализуемой.

Согласно лемме 1 все перестановки, коммутирующие с c, есть c^l, где $0 \leq l \leq n-2$. Покажем, что ни одна из этих перестановок, кроме тождественной не коммутирует с h. Несложно видеть, что $c(0) = 0$. Имеем $h(c^l(0)) = h(0) = 1$. С другой стороны $c^l(h(0)) = c^l(1)$. Если $l \neq 0$, то c^l есть цикл длины $n-2$, и следовательно $c^l(1) \neq 1$. Отсюда следует, что переходная система обладает *свойством максимальности*.

На рисунке изображена переходная система, построенная описанным выше способом, для $n = 8$

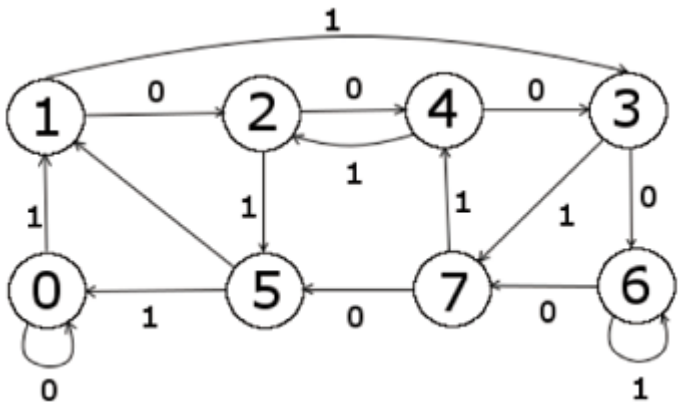

Рис. 3. Линейно реализуемая переходная система, обладающая *свойством максимальности*

Список литературы

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

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

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

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

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

[6] Родин С.Б., *Линейно реализуемые переходные системы*.. Интеллектуальные системы. Т.14, вып. 1-4. С.491-502.