Неизбыточные кодирования автоматов

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

Данная работа посвящена изучению «линейно реализуемых» автоматов, то есть автоматов, обладающих тем свойством, что существует кодирование, при котором порождаемый кодированием, булевкий оператор является линейным. В работе приведен критерий линейной реализуемости автомата. Также приведены нижняя и верхняя оценка числа линейно реализуемых автоматов.

Ключевые слова: теория автоматов, автомат, переходные системы, перестановка, подстановка, кодирование, сложность.

1. 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 язык схем осуществляется с помощью кодирования алфавита состояний, входного алфавита и выходного алфавита в алфавите $\{0, 1\}$. 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 ${E_2}^k$. Кодирование входного алфавита — это отображение алфавита A в ${E_2}^p$. Кодирование выходного алфавита — это отображение алфавита B в ${E_2}^l$. Кодирования алфавита состояния, входного алфавита и выходного алфавита порождает булевский оператор $\phi : E_2^{k+p} \to E_2^{k+l}$. Оператор ϕ может быть рассмотрен как набор $k+l$ булевских функций от $n + k$ переменных. Сложность такого оператора можно определить как максимальную сложность получаемых булевских

функций. Как известно [1] каждой булевской функции единственным образом соответствует полином Жегалкина. Мы будем понимать сложность оператора как максимальную из сложностей полиномов Жегалкина функций, задающих этот оператор, то есть максимальная степень полиномов, а сложность автомата как сложность оператора ϕ. Таким образом, установив связь между автоматом, кодировкой и возникающими полиномами, можно установить минимальную сложность реализации автомата.

Естественно начинать такого рода исследования с «простейших», линейных полиномов. Основной задачей данной работы было изучение автоматов, у которых существует кодирование, такое что получаемые при данном кодировании, булевские функции являются линейными.

В работе изучались автоматы с входным алфавитом $A = E_2$ и выходным алфавитом $B = E_2$, а также числом состояний $n = 2^k$.

2. Основные понятия

Определение 1. Кодированием множества $Q = \{0 \dots n-1\}$ назовем взаимоднозначное отображение $F : \{0 \dots n-1\} \to {E_2}^m$, где $m \geqslant] \log_2^n [$.

В данной работе изучались кодирования $F : \{0 \dots n-1\} \to {E_2}^m$, где $m =] \log_2^n [$, или $m = k$, с учетом $n = 2^k$.

Определение 2. Пусть задана некоторая подстановка на множестве $Q = \{0, \dots, n-1\}$, $s : Q \to Q$. Кодирование F множества Q, определяет по подстановке s, булевский оператор ϕ_s по правилу

$$\phi_s(\alpha_0, \dots, \alpha_{k-1}) = F(s(F^{-1}(\alpha_0, \dots, \alpha_{k-1}))),$$

где $\alpha_0, \dots, \alpha_{k-1} \in E_2$,$k = \log_2(n)$. Данный оператор может быть рассмотрен как набор k булевских функций, зависящих от k переменных. Обозначим этот набор через $\mathcal{F}_s(F)$.

Определение 3. Подстановка называется линейно реализуемой, посредством кодирования F, если набор $\mathcal{F}_s(F)$ состоит из линейных булевских функций.

Выделим из всех кодирований «стандартное» кодирование.

Определение 4. Кодирование $F_0 : \{0 \dots n-1\} \to {E_2}^k$ назовем стандартным, если код элемента есть его двоичное представление. Каждому кодированию F можно сопоставить перестановку s_F на множестве $Q : \{0 \dots n-1\}$ по правилу $s_F(i) = {F_0}^{-1}(F(i))$.

Введем несколько обозначений.
Пусть $n = 2^k$, то подстановки на множестве $Q = \{0 \dots n-1\}$ могут быть представлены как многочлены над полем Галуа F_{2^k} [2].
Обозначим через H_+ перестановки, соответствующие многочленам $x+c$ над полем Галуа F_n, где $c \in E_n$ — константа.

Замечание. Порядок умножения подстановок слева направо. То есть если заданы перестановки p_1 и p_2, то значение их произведения на элементе i есть $(p_1 \cdot p_2)(i) = p_2(p_1(i))$.

Определение 5. Нумерованной переходной системой назовем тройку $V = (A, Q, \varphi)$, где A — входной алфавит, $Q = \{0 \dots n-1\}$, φ — функция переходов.

Определение 6. Каждое кодирование F на множестве Q порождает булевский оператор $\phi_V^F : E_2^{k+1} \to E_2^k$, где

$$\phi_V^F(a, \alpha_0, \dots, \alpha_{k-1}) = F(\varphi(a, F^{-1}(\alpha_0, \dots, \alpha_{k-1}))), a \in E_2, \alpha_i \in E_2.$$

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

Определение 7. Если для заданной 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.

Пусть задана переходная система $V = (E_2, Q, \varphi)$ и некоторое кодирование F. Обозначим через $X_V = \{s : Q \leftarrow Q | \exists a \in E_2, s(q) = \varphi(a, q) \quad \forall q\}$
А через $S_V =< X_V >$, замыкание множества X_V относительно операции умножения подстановок [5].

Определение 8. S_V назовем внутренней полугруппой переходной системы V. X_V порождающее множество внутреней полугруппы.

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.

Определение 9. Нумерованным автоматом назовем пятерку $\mathfrak{A} = (E_2, Q, E_2, \varphi, \psi)$, где $Q = \{0 \dots n-1\}$, φ — функция переходов, ψ — выходная функция [1].

Определение 10. Каждое кодирование F для автомата на множестве Q порождает булевский оператор $\phi^F_{\mathfrak{A}} : {E_2}^{k+1} \to {E_2}^{k+1}$, где

$$\phi(a, \alpha_0, \ldots, \alpha_{k-1}) = \\ = (F(\varphi(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))), \psi(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))), \\ a \in A, \alpha_i \in E_2.$$

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

Определение 11. Если для заданного нумерованного автомата $\mathfrak{A}$ существует кодирование F, такое что все элементы $\mathcal{F}_{\mathfrak{A}}(F)$ являются линейными функциями алгебры логики, назовем такой автомат линейно реализуемым посредством кодирования F или просто линейно реализуемым.

Определение 12. Пусть задан автомат $\mathfrak{A} = (E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$. Назовем тройку (E_2, Q, φ) — переходной системой автомата $\mathfrak{A}$. Переходную систему автомата $\mathfrak{A}$ обозначим через $V_{\mathfrak{A}}$.

Определение 13. Пусть задан линейно реализуемый автомат $\mathfrak{A} = (E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$. Определим выходной предикат $p^{out} : \{0, 1, \ldots, n-1\} \to E_2$ как $p^{out}(q) = \psi(0, q)$.

Определение 14. Пусть задан предикат $p^{out} : \{0, 1, \ldots, n-1\} \to E_2$. Каждое кодирование F для предиката p на множестве Q порождает булевский функцию $\phi^F_p : {E_2}^{k+1} \to E_2$, где

$$\phi^F_p(\alpha_0, \ldots, \alpha_{k-1}) = p(F^{-1}(\alpha_0, \ldots, \alpha_{k-1})), \quad \alpha_i \in E_2.$$

Определение 15. Пусть задан предикат $p^{out} : \{0, 1, \ldots, n-1\} \to E_2$. Если существует кодирование F, такое что функция ϕ^F_p является линейной функцией алгебры логики, назовем такой предикат линейно реализуемым посредством кодирования F или просто линейно реализуемым.

3. Основные результаты

Теорема 1. *Подстановка p линейно реализуема посредством кодирования F тогда и только тогда, когда $H^{s_F}_+ p \subset p H^{s_F}_+$.*

Теорема 2. *Пусть задана переходная система $V = (E_2, Q, \varphi)$. V линейно реализуема посредством кодирования F, тогда и только тогда, когда существует подстановка p линейно реализуемая посредством кодирования F такая, что $p(s_F^{-1}(0)) = s_F^{-1}(0)$, $p_0 = p \cdot h_1$, $p_1 = p \cdot h_2$, где $h_1, h_2 \in {s_F}^{-1} \cdot H_+ \cdot s_F$.*

Теорема 3. *Пусть задан автомат $\mathfrak{A} = (E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$, где $n = 2^k$. Автомат линейно реализуем посредством кодирования F тогда и только тогда, когда*

- *переходная система $V_{\mathfrak{A}} = (E_2, \{0, 1, \ldots, n-1\}, \varphi)$ линейно реализуема посредством кодирования F;*
- *существует $\alpha, \beta \in E_2$ и предикат $p^{out} : Q \to E_2$ такая, что $\psi(x, q) = p^{out}(q) + \alpha \cdot x + \beta, \forall q \in \{0, 1, \ldots, n-1\}$;*
- *предикат p^{out} линейно реализуем посредством кодирования F.*

Теорема 4. *Число автоматов с n состояниями с входными алфавитом E_2 и выходным алфавитом E_2 равно $(2n)^{2n}$.*

Теорема 5. *Число линейно реализумых автоматов с $n = 2^k$ состояниями с входными алфавитом E_2 и выходным алфавитом E_2 есть $o((2n)^{2n})$.*

Автор выражет благодарность Алёшину Станиславу Владимировичу, чьи советы оказали неоценимую помощь в достижении результатов, изложенных в данной работе.

Список литературы

[1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[2] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1979.

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

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

[5] Арбиб М. А. Декомпозиция автоматов и расширение полугрупп // Алгебраическая теория автоматов, языков и полугрупп. — М.: Статистика, 1975. —С. 46–64.

[6] Родин С. Б. Линейно реализуемые переходные системы // Интеллектуальные системы. — 2010. — Т. 14, вып. 1–4. — С. 491–502.