Автоматы с линейными переходами

Бабин Д.Н.

Рассматривается проблема полноты системы автоматных функций с линейными переходами относительно операции суперпозиции. Эта система не является полной, более того, любая дополняющая ее до базиса система автоматов бесконечна.

Ключевые слова: конечный автомат, полнота, суперпозиция, замкнутый класс.

Теория линейных автоматов с операцией суперпозиции естественным образом использует аппарат линейной алгебры, смотри, например "Линейные последовательные машины"[1] — перевод на русский язык статьи Гилла [2]. Там показано, что линейные автоматы — это замкнутый класс, все полные системы в нем бесконечны, а система состоящая из одноместных функций и сумматора по модулю 2 — полна.

Относительно двух операций: суперпозиции и обратной связи линейные автоматы — это также замкнутый класс, в нем есть конечные полные системы, а также алгоритм проверки конечных систем на полноту, смотри работу Часовских А.А. [3].

Ранее автор показал [4], что линейный автомат может быть разложен в суперпозицию линейных автоматов с двумя состояниями и автомата с безусловными переходами (не обязательно линейного). В настоящей статье приводится явная формула такого разложения, а также доказан факт о бесконечной высоте и глубине класса линейных автоматов в классе всех автоматов.

Системы автоматов, имеющих линейные функции переходов, замкнутого класса не образуют. Эта система автоматов не полна, более того, до полной системы необходимо добавить к ним бесконечно много автоматов. Простое доказательство этих фактов приводится в этой статье.

Полное описание функциональных систем автоматов приведено в [5].

Пусть $E_2 = \{0, 1\}$, $g\colon E_2^n \to E_2^m$ булевая вектор-функция, их множество обозначается через $\mathbf{P_2}$. Пусть

$$E_2^\infty = \{a(1)a(2)\dots | a(j) \in E_2, j = 1, 2, \dots\}$$

— множество всех сверхслов.

$$f\colon (E_2^\infty)^n \to (E_2^\infty)^m$$

— автоматная функция (a-функция), т.е. она задается рекуррентно соотношениями

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi(q(t), a_1(t), ..., a_n(t)), \\ b_j(t) = \psi_j(q(t), a_1(t), ..., a_n(t)), \quad j = 1, ..., m. \end{cases}$$

где $q \in Q = \{q_1, \dots, q_r\}$. Параметр q называется состоянием a-функции f, q_1 — ее начальным состоянием, вектор-буквы $\mathbf{a} = (a_1, \dots, a_n)$ и $\mathbf{b} = (b_1, \dots, b_m)$ называются входной и выходной буквами, φ и ψ функцией переходов и выходов, соответственно, а сверхслова $\mathbf{a}(1)\mathbf{a}(2)...$ и $\mathbf{b}(1)\mathbf{b}(2)...$ — входным и выходным сверхсловами, соответственно. Класс всех a-функций обозначим через $\mathbf{P}$. Если функции φ и ψ_j линейны, автоматная функция называется линейной. Класс всех линейных a-функций обозначим через $\mathbf{L}$. Если функция φ линейна, то автоматная функция называется функцией с линейными переходами. Множество a-функций с линейными переходами обозначим через L. Если функция φ при фиксированных $a_1(t), ..., a_n(t)$, является взаимно-однозначным отображением Q в Q, то автоматная функция называется групповой. Класс всех групповых a-функций обозначим через $\mathbf{G}$. Автоматная функция, выдающая одно и то же выходное слово на всех входных словах, называется константной. Класс всех константных a-функций обозначим через $\mathbf{K}$.

Пусть $\nu \subseteq \mathbf{P}$, обозначим через $[\nu]$ множество всех a-функций, получающихся из ν с помощью операций суперпозиции. Множество ν называется полным, если $[\nu] = \mathbf{P}$. Проблема полноты для P состоит в описании всех полных множеств ν.

Функция

$$\mathbf{f_{Sh}}(x, y) = min(x, y) \oplus 1$$

называется функцией Шеффера. Известно, что $\mathbf{P_2} = [\{\mathbf{f_{Sh}}\}]$, т.е. функция $\mathbf{f_{Sh}}$ образует полную систему в классе булевых функций. Здесь $\oplus$ — сложение по модулю 2.

Линейная автоматная функция $d_0\colon E_2^\infty \to E_2^\infty$, задаваемая уравнениями

$$\begin{cases} q(1) = 0, \\ q(t+1) = x(t), \\ b(t) = q(t), \end{cases}$$

называется a-функцией задержки с нулевым начальным состоянием. Если в этих уравнениях $q(1) = 1$, то это задержка $d_1\colon E_2^\infty \to E_2^\infty$ с единичным начальным состоянием.

Линейная автоматная функция $w_0\colon E_2^\infty \to E_2^\infty$, задаваемая уравнениями

$$\begin{cases} q(1) = 0, \\ q(t+1) = q(t) + x(t), \\ b(t) = q(t), \end{cases}$$

называется a-функцией переключатель с нулевым начальным состоянием. Если в этих уравнениях $q(1) = 1$, то это переключатель $w_1\colon E_2^\infty \to E_2^\infty$ с единичным начальным состоянием.

Перепишем уравнения автоматной функции f в виде

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi(q(t), \mathbf{a}(t)), \\ \mathbf{b}(t) = \psi(q(t), \mathbf{a}(t)) \end{cases}$$

Запишим уравнения автоматной функции с линейными переходами ввиде

$$\begin{cases} q(1) = q_0, \\ q(t+1) = A(q(t)) + B(x(t)) + c, \\ \mathbf{b}(t) = \psi(q(t), \mathbf{a}(t)), \end{cases}$$

где A, B линейные операторы, а c вектор подходящей размерности. Матрица A называется основной матрицей автомата. Известно [1], что линейной заменой переменных матрица A приводится к клеточно-диагональному виду (Жордановой нормальной форме).

$$\begin{pmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & J_k \end{pmatrix}$$

Здесь Жорданова клетка J_i- это матрица вида

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 \\ a_0 & a_1 & a_2 & \dots & a_{n-1} \end{pmatrix}$$

ассоциированная с многочленом

$$\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0,$$

который является степенью некоторого неприводимого многочлены над полем Z_2.

Получилась

Лемма 1.

Автомат с линейными переходами получается суперпозицией булевых функций и автоматов с линейными переходами, основные матрицы которых — Жордановы клетки.

Лемма 2.

Если $\det(J) = 0$, то автомат с основной матрицей жордановой клеткой J выразим суперпозициями автоматов $\mathbf{f_{Sh}}, d_0, d_1$.

Доказательство: В самом деле: разложением по последней строке определителя получаем, что $\det(J_i) = a_0$, но если многочлен

$$\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0,$$

это степень непроводимого многочлена и $a_0 = 0$, то многочлен делится на λ, а значит этот многочлен λ^n, и ассоциированная с ним матрица это J_0.

$$J_0 = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Тогда канонические уравнения такого автомата имеют вид

$$\begin{cases} q_1(1) = q_{1,0}, \\ q_2(1) = q_{2,0}, \\ \dots \\ q_n(1) = q_{n,0}, \\ q_1(t+1) = q_2(t) + B_1(\mathbf{a}(t)) + c_1, \\ q_2(t+1) = q_3(t) + B_2(\mathbf{a}(t)) + c_2, \\ \dots \\ q_{n-1}(t+1) = q_n(t) + B_{n-1}(\mathbf{a}(t)) + c_n, \\ q_n(t+1) = \quad B_n(\mathbf{a}(t)) + c_n, \\ \mathbf{b}(t) = \psi(q_1(t), q_2(t), \dots, q_n(t), \mathbf{a}(t)), \end{cases}$$

$$\begin{array}{l} q_n(t) = d_{q_{n,0}}(B_n(\mathbf{a}(t)) + c_n), \\ q_{n-1}(t) = d_{q_{n-1,0}}(q_n(t) + B_{n-1}(\mathbf{a}(t)) + c_{n-1}) \\ \dots \\ q_1(t) = d_{q_{1,0}}(q_2(t) + B_1(\mathbf{a}(t)) + c_1) \\ \mathbf{b}(t) = \psi(q_1(t), q_2(t), \dots, q_n(t), \mathbf{a}(t)). \end{array}$$

Таким образом, выходная буква при всех t вычисляется по выходам задержек и булевых функций при тех же t. •

Лемма 3.

Если $\det(A) \neq 0$, то автомат с линейными переходами и основной матрицей A выразим суперпозициями автоматов из $K, \mathbf{f_{Sh}}, w_0, w_1$.

Доказательство: Пусть линейный автомат имеет уравнения

$$\begin{cases} q(1) = q_0, \\ q(t+1) = Aq(t) + Bx(t) + c, \\ \mathbf{b}(t) = q(t), \end{cases}$$

где $c = 0$. Пусть n порядок матрицы A, т.е. $A^n = E$, где E единичная матрица. Рассмотрим уравнения функции $\mathbf{b}(x)$,

$$\begin{cases} p(1) = 1 \\ z(1) = 00\dots0 \\ p(t+1) = p(t) + 1 \mid mod\ n \\ W = A^{-p-1}Bx \\ z(t+1) = z(t) + W \\ \mathbf{b}(t) = Wz, \end{cases} .$$

Это суперпозиция автоматной функции $W(x)$ с безусловными переходами, имеющей уравнения

$$\begin{cases} p(1) = 1 \\ p(t+1) = p(t) + 1 \mid \, mod \; n \\ W = A^{-p-1}Bx \end{cases}$$

и линейной автоматной функции $b(W)$ с уравнениями

$$\begin{cases} z(1) = 00\ldots0 \\ z(t+1) = z(t) + W \\ \mathbf{b}(t) = Wz, \end{cases} .$$

которая является суперпозицией (параллельным соединением) нескольких автоматных функций w_0, здесь вектор z имеет ту же размерность, что и q. Автоматная функция $W(x)$ получается суперпозицией константной функции

$$\begin{cases} p(1) = 1 \\ p(t+1) = p(t) + 1 \mid \, mod \; n \\ y = p \end{cases}$$

и булевых функций.

Уравнения для $\mathbf{b}(x)$ в первом и втором случае, это одни и те же рекурентные соотношения. В самом деле:

$$\begin{gathered} q(t+1) = A^{p(t+1)}z(t+1) = A^{p(t)+1}(z(t) + A^{-p(t)-1}Bx(t)) = \\ = A(A^{p(t)}z(t)) + Bx(t) = A(q(t)) + Bx(t) \end{gathered}$$

Автоматная функция с линейными переходами

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi(q(t), \mathbf{a}(t)), \\ \mathbf{b}(t) = \psi(q(t), \mathbf{a}(t)) \end{cases}$$

получается из линейной автоматной функции

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi(q(t), \mathbf{a}(t)), \\ \mathbf{b}(t) = q(t) \end{cases}$$

и булевых функций.

Случай $c \neq 0$ сводится к случаю $c = 0$ заменой переменных состояний. В самом деле: уравнения

$$\begin{cases} q(1) = q_0, \\ q(t+1) = Aq(t) + Bx(t) + c, \end{cases}$$

равносильны уравнениям

$$\begin{cases} r(1) = c, \\ q(1) = q_0, \\ r(t+1) = r(t), \\ q(t+1) = Aq(t) + r(t) + Bx(t), \end{cases}$$

Лемма 3 доказана •

Для функции f

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi(q(t), \mathbf{a}(t)), \\ \mathbf{b}(t) = \psi(q(t), \mathbf{a}(t)) \end{cases}$$

рассмотрим другую автоматную функцию f^s с уравнениями

$$\begin{cases} \tilde{q}(1) = q_1, \\ \tilde{q}(t+1) = \varphi(\tilde{q}(t), \mathbf{a}((t-1)*s+1)\mathbf{a}((t-1)*s+2)\dots\mathbf{a}(t*s)) \\ \mathbf{b}((t-1)*s+1)\dots\mathbf{b}(t*s)) = \psi(\tilde{q}(t), \mathbf{a}((t-1)*s+1)\dots \\ \dots\mathbf{a}(t*s)), \end{cases}$$

которая согласно тем же уравнениям за один такт перерабатывает s входных букв и выдает s выходных букв. Назовем новую автоматную функцию f^s в s раз ускоренной функцией f. Для множества автоматных функций $F = \{f_i\}$ обозначим через $F^s = \{f_i^s\}$. Операция перехода к ускоренной функцией f^s , была рассмотрена автором ранее под названием вербальной операции над автоматами [6]. Имеет место теорема о перестановочности операций ускорения и суперпозиции.

Теорема 1. [6] $[F]^s \subseteq [F^s]$

Имеет место

Утверждение 1.

Пусть для натурального T система всех автоматов μ такова, что число состояний каждого автомата не превосходит T. Тогда найдется автоматная функция f_T, такая что $\mu \subseteq [f_T, \mathbf{f_{Sh}}]$.

Доказательство:

В самом деле: рассмотрим в качестве f_T автоматную функцию с T состояниями, у которой каждая подстановка из полной полугруппы P_T подстановок на T элементах задается одной входной буквой [5]. Пусть входной алфавит f_T это P_T, а множество состояний и выходной алфавит $\{1, 2, \dots T\}$ в бинарном виде. На выход f_T будет выдавать номер своего состояния.

Для автоматной функции $f \in \mu$ с входным алфавитом A, выходным алфавитом B и T состояниями, определим булевую функцию $\omega : A \to P_T$, $\omega(a) = \varphi_a$ тогда функция $\psi(f_T(\omega(a)), a) = f$.•

Следствие 1.

Для любой автоматной функции f, множество $\{f^s | s \in \mathbf{N}\}$ порождается двумя автомтными функциями.

В самом деле, каждая из функций f^s имеет не больше состояний, чем функция f, по утверждению 1 получаем доказательство следствия.

Следствие 2.

$\mathbf{P_2}^s \subseteq \mathbf{P_2}$ и $\{w_0, w_1\}^s \subseteq [\mathbf{P_2} \cup \{w_0, w_1\}]$

Теорема 2.

Пусть Ω конечное множество a-функций, тогда $[\Omega \cup \mathsf{L}] \subsetneq \mathbf{P}$.

Доказательство:

Рассмотрим автоматную функцию $f \in [\Omega \cup \mathsf{L}]$, она получилась конечной схемой операций суперпозиции из функций $\Omega \cup \mathsf{L}$. Каждая автоматная функция $l_i \in \mathsf{L}, i = 1, \dots t$ участвующая в суперпозиции выражается суперпозицией автоматной функции с безусловными переходами $k_i, i = 1, \dots t$ и функций $\mathbf{f_{Sh}}, w_0, w_1, d_1, d_0$ по леммам 2 и 3. Пусть p_i период функции перходов k_i и $s = p_1 \cdot p_2 \cdot \dots \cdot p_t$, тогда

$$l_i^s \in [\mathbf{f_{Sh}}, w_0, w_1, d_1, d_0],$$

а

$$f_i^s \in [\mathbf{f_{Sh}}, w_0, w_1, d_1, d_0, f_T],$$

где T максимальное число состояний автоматных функций из Ω.

Значит, для любой автоматной функции из $f \in [\Omega \cup \mathsf{L}]$ найдется натуральное s, такое что f_i^s порождается одним и тем же конечным множеством автоматных функций не зависящим от s

$$[\mathbf{f_{Sh}}, w_0, w_1, d_1, d_0, f_T].$$

Функция из утверждения 1 $f_n \in [\mathbf{f_{Sh}}, {f_n}^s]$ при всех s. Если предположить, что система $[\Omega \cup \mathsf{L}]$ полна, то мы получим, что для любого n, автоматная функция $f_n \in [\mathbf{f_{Sh}}, w_0, w_1, d_1, d_0, f_T]$. Известно [5], что $\mathbf{P} = [\mathbf{f_{Sh}}, f_n | n \in \mathbf{N}]$.

Предположение о полноте $[\Omega \cup \mathsf{L}]$ приводит к полноте конечного множества

$$[\mathbf{f_{Sh}}, w_0, w_1, d_1, d_0, f_T].$$

что противоречиво. •

Полученные результаты верны также для линейных автоматов над другими конечными полями.

Список литературы

[1] Гилл А., *Линейные последовательные машины*, М. Наука, 1974.

[2] Gill A., *Linear sequential circuits*, McGraw-Hill, 1966.

[3] Часовских А.А., "О полноте в классе линейных автоматов", *Математическме вопросы кибернетики*, **3** (1995), 140–166.

[4] Бабин Д.Н., "Задача выразимости в некоторых классах автоматов", *Комбинаторно-алгебраическин методы в прикладной математике.*, 1985, 21–45.

[5] Кудрявцев В.Б., Алешин С.В., Подколзин А.С., *Введение в теорию автоматов*, М. Наука, 1985.

[6] Бабин Д.Н., "Вербальные подавтоматы и задача полноты", *Вестник московского университета*, **3** (1985), 52–54.

Automata with linear transition functions

Babin D.N.

The problem of completeness of the system of automaton functions with linear transitions with respect to the operation of superposition is considered. This system is not complete; moreover, any system of automata that complements it to the basis is infinite.

Keywords: finite automaton, completeness, superposition, closed class.