Об r-предсказуемости автоматных сетей

И. Ю. Самоненко

В данной работе вводится понятие r-предсказуемости конечных автоматов. Рассматривается связь r-предсказуемости с задачей синхронизации автомата и полугруппой автомата. Изучается свойство r-предсказуемости для автоматных сетей.

1. Свойство r-предсказуемости

Пусть $\mathfrak{A} = (A, Q, \varphi)$ — конечный автомат с входным алфавитом A, множеством состояний Q и функцией перехода $\varphi : Q \times A \to Q$.

Определение 1. Автомат $\mathfrak{A}$ называется r-предсказуемым, если существует функция $f : Q^{r+1} \to Q$ и состояния $q_1, \ldots, q_r \in Q$, такие что для любого слова $\alpha \in A^*$ и любого состояния $q \in Q$, верно

$$\varphi(q, \alpha) = f(q, \varphi(q_1, \alpha), \ldots, \varphi(q_r, \alpha)).$$

Состояния $q_1, \ldots, q_r$ называются базисными, функция f называется предсказывающей функцией.

Другими словами, автомат называется r-предсказуемым, если у него найдутся r состояний $q_1, \ldots, q_r \in Q$, таких что, зная только то, куда они перейдут по некоторому слову $\alpha \in A^*$, мы сможем определить (при помощи функции f), куда перейдет произвольное состояние $q \in Q$ по слову α.

Через $PR(n, r)$ обозначим класс всех r-предсказуемых автоматов с n состояниями. Через $K(n)$ обозначим класс всех автоматов с n состояниями.

Теорема 1. *При любом $n \geqslant 2$, справедлива следующая цепочка строгих включений*

$$PR(n, 1) \subsetneq PR(n, 2) \subsetneq \cdots \subsetneq PR(n, n-1) \subsetneq PR(n, n-1) = K(n)$$

Пусть $\mathfrak{A} = (A, Q, \varphi)$ произвольный автомат. Каждому слову $\alpha \in A^*$ можно сопоставить отображение $\widetilde{\alpha} : Q \to Q$ следующим образом:

$$\widetilde{\alpha}(q) = \varphi(q, \alpha)$$

Множество A^* относительно операции конкатенации образует полугруппу $H(A) = (A^*, \cdot)$. Введем на множестве A^* отношение эквивалентности $\sim$, такое что $\alpha \sim \beta$ тогда, и только тогда, $\widetilde{\alpha} \equiv \widetilde{\beta}$. Легко проверить, что $\widetilde{\alpha\beta} \equiv \widetilde{\alpha}(\widetilde{\beta})$, тем самым отношение эквивалентности $\sim$ корректно переносится на полугруппу $H(A)$. Фактор-полугруппа $H(A)/\sim$ называется *полугруппой автомата* $\mathfrak{A}$ и обозначается $SGr(\mathfrak{A})$. В том случае, если $SGr(\mathfrak{A})$ — группа, то автомат $\mathfrak{A}$ называется *групповым (перестановочным).*

Теорема 2. *Пусть автомат $\mathfrak{A} \in PR(n, r) \setminus PR(n, r-1)$, тогда*

$$|SGr(\mathfrak{A})| \leqslant n^r$$

Если при этом автомат $\mathfrak{A}$ групповой, то

$$r \leqslant |SGr(\mathfrak{A})|.$$

Рассмотрим критерий того, что автомат является r-предсказуемым.

Теорема 3. *Автомат $\mathfrak{A} = (A, Q, \varphi) \in Pr(n, r)$ тогда и только тогда, когда существуют состояния $q_1, \ldots, q_r \in Q$ со следующим свойством: для любых $\alpha, \beta \in A^*$ из того, что $\varphi(q_i, \alpha) = \varphi(q_i, \beta)$, $i = 1, \ldots, r$, следует, что для любого $q \in Q$ верно $\varphi(q, \alpha) = \varphi(q, \beta)$.*

Для групповых автоматов этот критерий упрощается.

Теорема 4. *Групповой автомат $\mathfrak{A} = (A, Q, \varphi) \in Pr(n, r)$ тогда и только тогда, когда существуют состояния $q_1, \ldots, q_r \in Q$ со следующим свойством: для любого $\alpha \in Q$ из того, что $\varphi(q_i, \alpha) = q_i$, $i = 1, \ldots, r$, следует, что для любого $q \in Q$ верно $\varphi(q, \alpha) = q$.*

Слово $\alpha \in A^*$ называется *синхронизирующим* для автомата $\mathfrak{A} = (A, Q, \varphi)$, если существует такое состояние $q_f \in Q$, что для любого состояния $q \in Q$ верно $\varphi(q.\alpha) = q_f$. Автомат называется *синхронизируемым*, если для него существует синхронизующее слово.

Пусть $\mathfrak{A} = (A, Q, \varphi) \in K(n)$ произвольный синхронизируемый автомат с n состояниями. Гипотеза Черни утверждает, что длина минимального синхронизующего слова для $\mathfrak{A}$ не превышает $(n-1)^2$ [3]. Эта проблема до сих пор открыта. Наилучшая известная на сегодняшний день верхняя оценка длины минимального синхронизующего слова равна $\frac{n^3-n}{6}$ [2].

Теорема 5. *Пусть автомат $\mathfrak{A} = (A, Q, \varphi) \in Pr(n, r)$ является синхронизуемым, тогда длина минимального синхронизующего слова не превосходит $\frac{r(r-1)(r-2)}{6} + n$.*

2. Автоматные сети

Пусть $G = (V, E, \rho)$ — конечный ориентированный граф со множеством вершин V, множеством ребер E и функцией $\rho : E \to V \times V$, сопоставляющей каждому ребру пару вершин (соответственно начальную и конечную). Через $Out(v)$ обозначим множество ребер выходящих из вершины v, то есть $Out(v) = \{e \in E | \exists v' \in V : \rho(v, v') = e\}$. Через $O_v = |Out(v)|$ обозначим число вершин, выходящих из вершины v.

Функцией разметки ребер графа G называется функция $\lambda_E : E \to \mathbb{N}$, такая что, для любой вершины $v \in V$, функция λ_E биективно отображает множество $Out(v)$ во множество $\{1, \ldots, O_v\}$. Другими словами, для каждой вершины v, функция разметки ребер λ_E однозначно нумерует ребра исходящие из этой вершины начальным отрезком натурального ряда. Пользуясь функцией λ_E, определим функцию $\lambda : V \times \mathbb{N} \to V$, такую что для любой вершины $v \in V$ и любого ребра $e \in Out(v)$, верно $\rho(v, \lambda(v, \lambda_E(e))) = e$. Другими словами значение функции $\lambda(v, t)$ есть та вершина, в которую идет ребро с меткой t из вершины v.

Пусть Q — некоторое конечное множество и $\mathbb{F}(Q) = \{f : Q^s \to Q | s \in \mathbb{N}_0\}$ — множество всех функций определенных на Q^s и действующих в Q. Функцией разметки вершин графа G относительно множества Q, называется функция $\lambda_V : V \to \mathbb{F}(Q)$, такая что для любого $v \in V$ число аргументов функции $\lambda_V(v)$ равно O_v.

Автономной автоматной сетью называется четверка $\mathfrak{R} = (Q, G, \lambda_E, \lambda_V)$, где Q — конечное множество состояний ячеек, $G = (V, E, \rho)$ —

конечный ориентированный граф, λ_E — функция разметки ребер графа G, λ_V — функция разметки вершин графа G относительно Q.

Множество всех автономных автоматных сетей, со множеством состояний ячеек Q и множеством вершин графа V обозначим через $ANet(Q, V)$.

Пусть $V = \{1, \ldots, n\}$ — множество вершин графа G. С каждой автономной автоматной сетью $\mathfrak{R} = (Q, G, \lambda_E, \lambda_V)$ можно связать отображение $\Phi : Q^n \to Q^n$ следующим образом:

$$\Phi_{\mathfrak{R}}(q_1, \ldots, q_r) = (f_1(q_{\lambda(1,1)}, \ldots, q_{\lambda(1,O_1)}), \ldots, f_n(q_{\lambda(n,1)}, \ldots, q_{\lambda(n,O_n))}),$$

где $f_i = \lambda_V(i)$, $i = 1, \ldots, n$.

Автоматной сетью называется четверка $\mathfrak{N} = (A, Q, V, \eta)$, где A — конечный входной алфавит, Q — конечно множество состояний ячеек, V — множество вершин графа, $\eta : A \to ANet(Q, V)$ — функция, сопоставляющая каждому входному символу некоторую автономную автоматную сеть.

С каждой автоматной сетью сетью $\mathfrak{N} = (A, Q, V, \eta)$ можно связать автомат $\mathfrak{A} = A(\mathfrak{N}) = (A, Q^n, \Phi)$, где $n = |V|$ и функция переходов Φ устроена следующим образом:

$$\Phi(a, (q_1, \ldots, q_n)) = \Phi_{\eta(a)}(q_1, \ldots, q_n)$$

Наглядно автоматную сеть можно интерпретировать следующим образом. Имеется множество V ячеек памяти, каждая из которых может находится в одном их Q состояний. При появлении внешнего сигнала $a \in A$ фиксируется автономная автоматная сеть $\eta(a)$ и состояние каждой ячейке $v \in V$ меняется путем вычисления функции $\lambda_V(v)$. Аргументами этой функции служат состояния ячеек, в которых ведут соответствующие ребра $Out(v)$ графа G сети $\eta(a)$. Ребра занумерованы, поэтому порядок аргументов вычисляется однозначно. Смена состояний происходит во всех ячейках одновременно.

3. r-предсказуемость автоматных сетей

В данном разделе мы дадим оценку r-предсказуемости автоматов, задаваемых автоматными сетями. В начале рассмотрим *однородные* автоматные сети.

Зафиксируем натуральные числа $d_1, \dots, d_k \in \mathbb{N}$, в качестве множества вершин рассмотрим k-мерный целочисленный параллелограмм со сторонами $d_1, \dots, d_k$, то есть $V = E_{d_1} \times \dots \times E_{d_k}$. Построим граф G следующим образом. Рассмотрим произвольный набор векторов $\overline{u}_1, \dots, \overline{u}_s \in \mathbb{Z}^k$. Из каждой вершины $\overline{v} = (l_1, \dots, l_k) \in V$ выходят s ребер в вершины вершины $(\overline{v} + \overline{u}_1)\ mod\ (d_1, \dots, d_k), \dots, (\overline{v} + \overline{u}_1)\ mod\ (d_1, \dots, d_k)$, где $(a_1, \dots, a_k)\, mod\, (d_1, \dots, d_k) = (a_1\, mod\, d_1, \dots, a_k\, mod\, d_k)$. Полученный граф обозначим через $G = G(V; \overline{u}_1, \dots, \overline{u}_k)$ и назовем однородным графом.

Построим функцию разметки ребер λ_E следующим образом: если ребро $e \in E$ идет из вершины $\overline{v}$ в вершину $(\overline{v} + \overline{u}_i)\ mod\ (d_1, \dots, d_k)$, то $\lambda_E(e) = i$.

Рассмотрим произвольную функцию $\varphi : Q^k \to Q$, и определим функцию заметки вершин $\lambda_V(v) = \varphi$.

Автономную автоматную сеть имеющую вид $\mathfrak{R} = (Q, G(E_{d_1} \times \dots \times E_{d_k}; \overline{u}_1, \dots, \overline{u}_s), \lambda_E, \varphi)$, где λ_E определена выше назовем *однородной автономной автоматной сетью.*

Через $HANet(Q; d_1, \dots, d_k)$ обозначим множество всех однородных автономных автоматные сетей со множеством состояний ячеек Q и множеством вершин $E_{d_1} \times \dots \times E_{d_k}$.

Однородной автоматной сетью размера $d_1 \times \dots \times d_k$ называет автоматная сеть $\mathfrak{N} = (A, Q, V, \eta)$, где $\eta : A \to HANet(Q; d_1, \dots, d_k)$.

Теорема 6. *Пусть $\mathfrak{N} = (A, Q, V, \eta)$ произвольная однородная автоматная есть размера $d_1 \times \dots \times d_k$, тогда автомат $A(\mathfrak{N}) \in PR(n, r(n))$, где $n = |Q|^{d_1 \dots d_k}$ и $r(n) \lesssim \frac{n}{\log_{|Q|}(n)}$ при $d_1, \dots, d_k \to \infty$.*

Пусть $\mathfrak{R} = (Q, G(V, E, \rho), \lambda_E, \lambda_V)$ — произвольная автономная автоматная сеть. Эндоморфизмом сети $\mathfrak{R}$ называется любое отображение $h : V \to V$, такое что:

1) Для любых вершин $v_1, v_2 \in V$, из того, что существует ребро $e \in E$, такое что $\rho(e) = (v_1, v_2)$, следует, что существует ребро $e' \in E$, такое что $\rho(e') = (h(v_1), h(v_2))$ и $\lambda_E(e) = \lambda_E(e')$. Другими словами, если вершины v_1 и v_2 были соединены ребром e, то найдется ребро e', которое соединяет вершины $h(v_1)$ и $h(v_2)$, и имеющее ту же самую метку.
2) Для любой вершины $v \in V$, $\lambda_V(h(v)) = \lambda_V(v)$. Другими словами, отображение h сохраняет разметку вершин.

Множество всех эндоморфизмов сети $\mathfrak{R}$ обозначим $End(\mathfrak{R})$. Очевидно $End(\mathfrak{R})$ — полугруппа относительно композиции.

Пусть $\mathfrak{N} = (A, Q, V, \eta)$ — произвольная автоматная есть. Множеством эндоморфизмов сети $\mathfrak{N}$ назовем множество

$$End(\mathfrak{N}) = \cap_{a \in A}(End(\eta(a)))$$

Пусть $V = 1, \ldots, n$ и $h : V \to V$ — произвольное отображение, тогда h задает отображение $\widetilde{h} : Q^n \to Q^n$ следующим образом:

$$\widetilde{h}(q_1, \ldots, q_n) = (q_{h(1)}, \ldots, q_{h(n)})$$

Таким образом, каждому эндоморфизму $h \in End(\mathfrak{N})$ можно сопоставить отображение $\widetilde{h}$ множества состояний автомата $A(\mathfrak{N})$ на себя. Подмножество состояний $Q' \subseteq Q^n$ автомата $A(\mathfrak{N})$ назовем *эндоморфно порождающим*, если для любого состояния $\overline{q} \in Q^n$ найдется такое состояний $\overline{q}' \in Q'$ и эндоморфизм $h \in End(\mathfrak{N})$, что $\overline{q}' = \widetilde{h}(\overline{q})$.

Теорема 7. *Пусть $\mathfrak{N} = (A, Q, V, \eta)$ — произвольная автоматная есть и Q' эндоморфно порождающее множество для автомата $A(\mathfrak{N})$, тогда $A(\mathfrak{N}) \in PR(n, |Q'|)$.*

4. Благодарности

Автор выражает глубокую благодарность своему научному руководителю профессору Бабину Дмитрию Николаевичу за помощь в решении задачи.

Список литературы

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

[2] Клячко А. А., Рысцов И. К., Спивак М. А. Об одной экстримальной комбинаторной задаче, связаной с оценкой длины возвратного слова в автомате // Кибернетика. 1987. 2.

[3] Černy J. Poznamka k homogennym eksperimentom s konechnymi automatami // Math.-Fiz. Cas. 14 (1964).