

О конечных автоматах с максимальной степенью различимости состояний

В. А. Орлов

Рассматривается оценка одного из параметров конечных автоматов — степень различимости состояний. В работе рассматриваются множества конечных автоматов с произвольными функциями выхода и переходов.

Состояния конечного автомата называются g -эквивалентными, если соответствующие им автоматные функции одинаковы на словах длины g . Состояния называются g -различимыми, если они $(g-1)$ -эквивалентны и соответствующие им автоматные функции различаются на словах длины g . Максимальная степень различимости состояний автомата называется его степенью различимости. При отсутствии ограничений известна достижимая верхняя оценка степени различимости равная $s-1$, где s — число состояний автомата. В каждом своем состоянии конечный автомат реализует функцию, аргументы которой (значения которой) суть элементы входного (выходного) алфавита. Число различных таких функций будем называть статической функциональностью автомата. Рассматриваются автоматы с заданной статической функциональностью. Получена достижимая верхняя оценка степени различимости, равная $s+1-F$, где F — статическая функциональность автомата.

Множество $\{s_1, s_2, \dots, s_F\}$, где s_i , $1 \leq i \leq F$, — мощность i -го класса 1-эквивалентности будем называть спектром конечного автомата. Показана зависимость максимальной степени различимости состояний конечного автомата от его спектра.

Ключевые слова: конечный автомат, автоматная функция, различимость состояний.

Математической моделью большинства устройств обработки цифровой информации — последовательностных устройств — являются конечные автоматы. Одним из параметров конечного автомата является его степень различимости. Этот параметр влияет на длину диагностического и установочного экспериментов для автоматов с известным поведением, а также на длину расшифровки «черных ящиков» (автоматов с неизвестными функциями выхода и переходов). В первом случае желательны автоматы с малой степенью различимости. При создании криптостойких конечно автоматных систем шифрования желательны автоматы с высокой степенью различимости.

Известно [1], что степень различимости может быть очень высокой, равной $s - 1$, где s — число состояний. С другой стороны доказано [2], что почти все автоматы имеют степень различимости $\log_m \log_n s$, где n (m) — мощность входного (выходного) алфавита.

В работе рассматриваются множества конечных автоматов с произвольными функциями выхода и переходов.

Состояния конечного автомата называются g -эквивалентными, если соответствующие им автоматные функции одинаковы на словах длины g . Состояния называются g -различимыми, если они $(r-1)$ -эквивалентны и соответствующие им автоматные функции различаются на словах длины g . Максимальная степень различимости состояний автомата называется его степенью различимости. При отсутствии ограничений известна достижимая верхняя оценка степени различимости равная $s - 1$, где s — число состояний автомата. В каждом своем состоянии конечный автомат реализует функцию, аргументы которой (значения которой) суть элементы входного (выходного) алфавита. Число различных таких функций будем называть статической функциональностью автомата. Рассматриваются автоматы с заданной статической функциональностью. Получена достижимая верхняя оценка степени различимости, равная $s + 1 - F$, где F — статическая функциональность автомата.

Множество $\{s_1, s_2, \dots, s_F\}$, где s_i , $1 \leq i \leq F$, — мощность i -го класса 1-эквивалентности будем называть спектром конечного автомата. Показана зависимость максимальной степени различимости состояний конечного автомата от его спектра.

Конечный автомат является имеющим вход и выход устройством, которое в каждый момент времени находится в одном из своих состояний. Конечный автомат осуществляет преобразование информации в дискретные моменты времени. На вход автомата поступает последовательность символов входного алфавита $X = (x_1, x_2, \dots, x_n)$; эту последовательность называют входным словом. В каждый момент времени конечный автомат находится в одном из своих s (внутренних) состояний, образующих множество $Q = \{q_1, q_2, \dots, q_s\}$ (алфавит состояний). В каждый момент времени значением выхода автомата является элемент выходного алфавита $Y = \{y_1, y_2, \dots, y_m\}$. В работе, в основном, будет использовано задание (описание) функционирования конечного автомата системой его ns команд. Каждая команда имеет вид $x_i q_j \rightarrow y_k q_r$, где x_i — входная буква, q_j — состояние, y_k — выходная буква и q_r — состояние в следующий за текущим моментом времени (следующее состояние).

Функционирование конечного автомата задают также кортежем $\langle X, Y, Q, V, P \rangle$, где $V : X \times Q \rightarrow Y$ (функция выхода), $P : X \times Q \rightarrow Q$ (функция переходов).

Конечный автомат с фиксированным состоянием в начальный момент времени называется *инициальным автоматом*. В соответствии со своей системой команд инициальный автомат реализует *автоматную функцию*, которая произвольное входное слово в алфавите X преобразует в выходное слово в алфавите Y той же длины.

Состоянию q_i конечного автомата M поставим в соответствие автоматную функцию M_i , реализуемую автоматом M с начальным состоянием q_i . Если автоматные функции M_i и M_j одинаковы, то состояния q_i и q_j называются *эквивалентными* или *неотличимыми*. В противном случае состояния q_i и q_j называются *различимыми*. Состояния q_i и q_j являются k -эквивалентными, если соответствующие им автоматные функции совпадают на словах длины k . Заметим, что k -эквивалентные состояния являются m -эквивалентными для любого $m \leq k$.

Различимые состояния классифицируют по *степени различимости*: состояния q_i и q_j являются r -различимыми, если они являются $(r - 1)$ -эквивалентными, но не являются r -эквивалентными. Таким образом, степень различимости пары состояний конечного автомата определяется однозначно. *Степень различимости конечного автомата* считается максимум степеней различимости пар его состояний.

Степень различимости играет важную роль в диагностических и установочных экспериментах над последовательностными устройствами, а также при расшифровке конечных автоматов.

Известно ([1] [3, с. 184] [4, с. 314] [5, с. 17]) следующее

Утверждение. *Степень различимости конечного автомата не превосходит уменьшенного на единицу числа его состояний. Более того, для любого натурального числа $s \geq 2$ существует имеющий s состояний конечный автомат, степень различимости которого равна $s - 1$.*

При доказательстве этого утверждения использовалось свойство отношений эквивалентности.

Бинарным отношением R на множестве A называется произвольное подмножество декартового произведения $A \times A$ (множества всех упорядоченных пар элементов множества A).

Бинарные отношения на множестве A могут иметь следующие свойства:

рефлексивность (для любого $x \in A$ пара $(x, x) \in R$),

симметричность (из $(x, y) \in R$ следует, что $(y, x) \in R$),

транзитивность (из $(x, y) \in R$ и $(y, z) \in R$ следует, что $(x, z) \in R$).

Нетрудно проверить, что для любого k отношение k -эквивалентности на множестве состояний конечного автомата является рефлексивным, симметричным и транзитивным. Такие отношения называются *отношениями эквивалентности*.

Разбиением множества называется множество его непустых попарно не пересекающихся подмножеств такое, что множество является объединением этих подмножеств.

Известно, что любому отношению эквивалентности соответствует *разбиение* множества, на котором оно определено. Элементы этого разбиения называют *классами эквивалентности*.

Конечный автомат с s состояниями, имеющий n входных, m выходных символов и F классов 1-эквивалентности, будем называть (n, m, s, F) -автоматом. Заметим, что число классов 1-эквивалентности равно статической функциональности конечного автомата.

О конечных автоматах с максимальной степенью различимости состояний

В дальнейшем не будем оговаривать выполнение следующих условий $n \geq 2, m \geq 2, s \geq 2, F \leq s$ и $F \leq m^n$ (статическая функциональность (n, m, s) -автомата не превосходит m^n).

Пусть $MSR(n, m, s, F)$ — максимальная степень различимости состояний (n, m, s, F) -автоматов.

Справедливо следующее утверждение.

Теорема 1. $MSR(n, m, s, F) = s + 1 - F$.

Доказательство теоремы 1 будет приведено ниже.

Состояние q_r конечного автомата, имеющего команду $xq_j \rightarrow yq_r$, называют x -потомком состояния q_j и обозначают q_j^x .

Лемма 1. Если в автомате есть r -различимые состояния, $r \geq 2$, то при любом $t, 1 \leq t \leq r - 1$, в нем имеются t -различимые состояния.

Доказательство. Пусть (q_i, q_j) — пара r -различимых состояний конечного автомата и пусть $a_1 a_2 \dots a_r$ — слово, различающее эту пару. Заметим, что на словах меньшей длины эти состояния неотличимы. Пусть $q_{t,1} = q_t^{a_1}$, пусть $q_{t,2} = q_{t,1}^{a_2}$ и т.д. Состояния $q_{i,1}$ и $q_{j,1}$ ($r - 1$)-различимы, так как они $(r - 2)$ -эквивалентны и различимы на слове $a_2 \dots a_r$ длины $r - 1$.

Индукцией по $t, 1 \leq t \leq r - 1$, нетрудно показать, что состояния $q_{i,t}$ и $q_{j,t}$ являются $(r - t)$ -различимыми. Лемма 1 доказана.

Пусть E_k — разбиение множества состояний конечного автомата, соответствующее отношению k -эквивалентности. Если автомат содержит $(k + 1)$ -различимые состояния, то, по крайней мере, один из классов k -эквивалентности перестанет быть классом $(k + 1)$ -эквивалентности, т.е. $|E_{k+1}| > |E_k|$.

Пусть автомат M имеет степень различимости, равную g , и пусть $|E_1| = F$. Из леммы 1 получаем следующую цепочку неравенств $|E_1| < |E_2| < \dots < |E_r|$. Отсюда в случае $r > s + 1 - F$ получаем противоречие с очевидным неравенством $|E_r| \leq s$.

Первая часть теоремы 1 доказана.

Докажем вторую часть теоремы 1.

Пусть $M1$ — (n, m, s, F) -автомат, у которого не более одного не одноэлементного класса 1-эквивалентности. Состояния автомата $M1$ в одноэлементных (не одноэлементных) классах 1-эквивалентности обозначим как p_1, p_2, \dots, p_{F-1} (как q_1, q_2, \dots, q_t , где $t = s - F + 1$). Автомат

$M1$ имеет следующий граф переходов. Из вершины $q_i, 1 \leq i \leq t-1$, все дуги идут в вершину q_{i+1} . Из вершины $p_i, 1 \leq i \leq N-2$, все дуги идут в вершину p_{i+1} . Из вершины q_t все дуги идут в вершину p_1 . Из вершины p_{F-1} все дуги идут в вершину q_1 .

Нетрудно проверить, что состояния q_1 и q_2 являются $(s+1-F)$ -различимыми. Вторая часть теоремы 1 доказана.

Замечание. Автомат $M1$ выбран из условия простоты описания.

Рассмотрим теперь подмножества множества (n, m, s, F) -автоматов, имеющие одинаковый спектр.

Под (n, m, s, F, D) -автоматом будем понимать (n, m, s, F) -автомат со спектром D .

Вначале докажем достаточное условие на разбиение D , при котором $MSR(n, m, s, F, D) = MSR(n, m, s, F)$.

Теорема 2. *Если не более чем один класс 1-эквивалентности разбиения D имеет мощность большую 2, то*

$$MSR(n, m, s, F, D) = MSR(n, m, s, F).$$

Доказательство. Пусть разбиение D состоит из a одноэлементных множеств, b двухэлементных множеств и одного множества из $c \geq 3$ элементов ($s = a + 2b + c$). Для простоты описания рассмотрим случай $a \geq 2, b \geq 2, c \geq 2$.

Пусть $M2$ — автономный (n, m, s, F, D) -автомат и пусть $q_i^1, 1 \leq i \leq a, (q_j^3, 1 \leq j \leq c)$ — его состояния из одноэлементных множеств (из множества, содержащего более 2 элементов) разбиения D . Пусть $q_{t,1}^2, q_{t,2}^2, 1 \leq t \leq b$, — состояния из двухэлементных множеств разбиения D . Автомат $M2$ имеет следующую систему переходов

$$\begin{aligned} q_i^1 &\Rightarrow q_{i+1}^1, 1 \leq i \leq a-1; q_a^1 \Rightarrow q_{1,1}^2; \\ q_j^3 &\Rightarrow q_{j+1}^3, 1 \leq j \leq c-1; q_c^3 \Rightarrow q_1^1; \\ q_{t,1}^2 &\Rightarrow q_{t+1,1}^2, q_{t,2}^2 \Rightarrow q_{t+1}^2, \quad 1 \leq t \leq b-1; \\ q_{b,1}^2 &\Rightarrow q_1^3; \quad q_{b,2}^2 \Rightarrow q_2^3. \end{aligned}$$

Нетрудно проверить, что состояния $q_{1,1}^2$ и $q_{1,2}^2$ $(s+1-F)$ -различимы. Теорема 2 доказана.

Покажем, что условие теоремы 2 не является необходимым.

О конечных автоматах с максимальной степенью различимости состояний

Для упрощения изложения рассмотрим случай автономных $(2, a + b, 2, \{a, b\})$ -автоматов, у которых $Y = \{0, 1\}$. Пусть $q_i^0, 1 \leq i \leq a, (q_j^1, 1 \leq j \leq b)$ — состояния, в которых реализуется константа 0 (константа 1).

Лемма 2. $MSR(2, 2, 8, 2, \{3, 5\}) = 7$.

Доказательство. Пусть $M3$ — $(2, 8, 2, \{3, 5\})$ -автомат со следующей системой переходов

$$q_i^0 \Rightarrow q_i^1, 1 \leq i \leq 3; q_1^1 \Rightarrow q_2^0; q_2^1 \Rightarrow q_3^0;$$

$$q_3^1 \Rightarrow q_4^1; q_4^1 \Rightarrow q_1^0; q_5^1 \Rightarrow q_1^1.$$

Нетрудно проверить, что состояния q_3^1 и q_5^1 являются 7-различимыми.

Покажем зависимость максимальной степени различимости состояний от спектра. Для простоты изложения ограничимся рассмотрением автономных автоматов.

Пусть $MSRa(m, s, F)$ (Пусть $MSRa(m, s, F, D)$) — максимальная степень различимости состояний автономных автоматов с F классами 1-эквивалентности (со спектром D), у которых $|Y| = m, |Q| = s$.

Теорема 3. *Существуют спектры D , для которых*

$$MSRa(m, s, F, D) \neq MSRa(m, s, F).$$

Доказательство следует из равенства

$$MSRa(2, 9, 2, \{3, 6\}) = 7.$$

Пусть $q_i^0, 1 \leq i \leq 3, (q_i^1, 1 \leq i \leq 6)$ — состояния, в которых реализуется константа 0 (константа 1).

Нижняя оценка. Пусть $M4$ — $(2, 9, 2, \{3, 6\})$ -автомат, отличающийся от автомата $M3$ добавлением состояния q_6^1 и команды $q_6^1 \Rightarrow q_5^1$. Нетрудно проверить, что состояния q_3^1 и q_5^1 являются 7-различимыми.

Верхнюю оценку получаем методом перебора. Граф переходов связанного автономного автомата имеет один цикл, в вершины которого могут входить деревья. Перебор проводим по длине цикла.

Анализ автоматов, не являющихся связными, сводится к анализу их компонент связности.

Список литературы

- [1] Mealy G.Y. Method for Synthesizing Sequential Circuits // Bell System Tech. J., vol. 34, 1955, pp. 1054–1079.
- [2] Коршунов А.Д. О степени различимости автоматов. // Дискретный анализ, Новосибирск, 1967, №10, с. 39–60.
- [3] Фомичев В.М. Дискретная математика и криптология, М. ДИАЛОГ-МИФИ, 2003, 397 с.
- [4] Z.Kohavi, Niraj K. Jha Switching and Finite Automata Theory. Cambridge University Press , 2010, 617 pp.
- [5] Бабаш А.В. Синтез шифрующих автоматов. М.: НИУ ВШЭ; МЭ-СИ, 2014. – 257 с.