Теория автоматов и шифров.

Часть 1. Теория автоматов.

План лекции

- Состояния
- Определение основной модели конечного автомата
- Определение множества состояний по внутренней структуре
- Другая модель
- Предсказание поведения автомата
- Таблица переходов
- Перечисление автоматов
- Изоморфные автоматы
- Граф переходов
- Классификация состояний и подавтоматов

Конечный автомат

- Состояние системы – S ($S_v - t_v$)
- Пример с монетой, вывод

Конечный автомат

- Определение конечного автомата

  X=$\{\xi_1, \xi_2, \dots, \xi_p\}$

  Z= $\{\zeta_1, \zeta_2, \dots, \zeta_q\}$

  S= $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$

  $z_v = f_z(x_v, s_v)$

  $s_{v+1} = f_s(x_v, s_v)$

Опр: M=(X, Z, S, f_z, f_s)

- Примеры конечных автоматов (организм, текст, колесо)

Определение множества состояний по внутренней структуре

$$y_{\nu}^{(k)} = g_k\left(x_{\nu}^{(1)},\ x_{\nu}^{(2)},\ \ldots,\ x_{\nu}^{(u)},\ y_{\nu-1}^{(1)},\ y_{\nu-1}^{(2)},\ \ldots,\ y_{\nu-1}^{(r)}\right) \quad (1)$$

Входные переменные

$$X = X^{(1)} \otimes X^{2} \otimes \ \ldots \ \otimes X^{(u)} \quad (2)$$

Выходные переменные

$$Z = Z^{(1)} \otimes Z^{(2)} \otimes \ \ldots \ \otimes Z^{(w)} \quad (3)$$

Зависимые переменные

$$Y = Y^{(1)} \otimes Y^{(2)} \otimes \ \ldots \ \otimes Y^{(r)} \quad (4)$$

(5) $$y_v = g_y(x_v,\ y_{v-1})$$

(6) $$z_v = g_z(x_v,\ y_{v-1})$$

(7) $$s_v = y_{v-1}$$

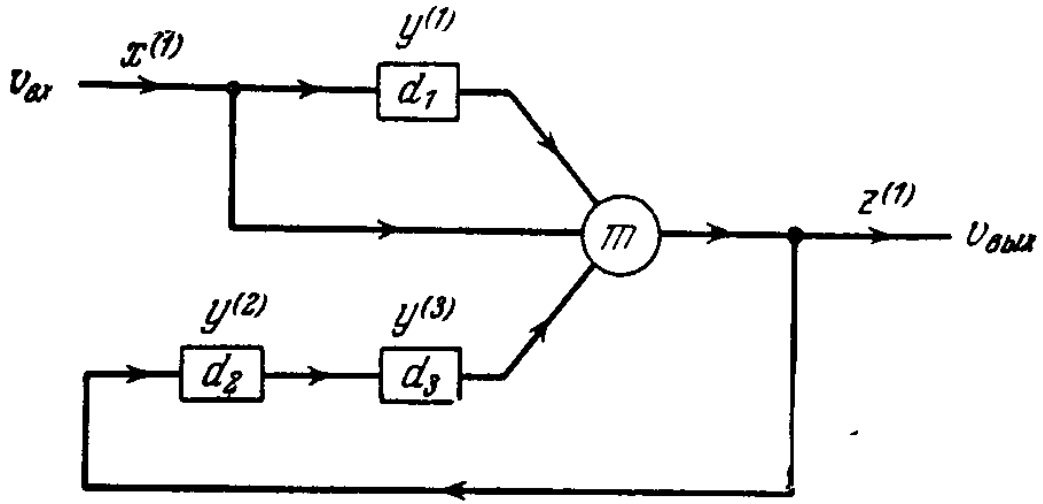
(8) $$y_v = f_s(x_v,\ s_v)$$

(9) $$z_v = f_z(x_v,\ s_v)$$

(10) $$s_{v+1} = f_s(x_v,\ s_v)$$

Пример

Схема с мажоритарным элементом



$$y_\nu^{(1)} = g_1\left(x_\nu^{(1)},\ y_{\nu-1}^{(1)},\ y_{\nu-1}^{(2)},\ y_{\nu-1}^{(3)}\right);$$
$$y_\nu^{(2)} = g_2\left(x_\nu^{(1)},\ y_{\nu-1}^{(1)},\ y_{\nu-1}^{(2)},\ y_{\nu-1}^{(3)}\right);$$
$$y_\nu^{(3)} = g_3\left(x_\nu^{(1)},\ y_{\nu-1}^{(1)},\ y_{\nu-1}^{(2)},\ y_{\nu-1}^{(3)}\right)$$

	s_ν			$s_{\nu+1}$		
$x_\nu^{(1)}$	$y_{\nu-1}^{(1)}$	$y_{\nu-1}^{(2)}$	$y_{\nu-1}^{(3)}$	$g_1 = y_\nu^{(1)}$	$g_2 = y_\nu^{(2)}$	$g_3 = y_\nu^{(3)}$
0	0	0	0	0	0	0
1	0	0	0	1	0	0
0	0	0	1	0	0	0
1	0	0	1	1	1	0
0	0	1	0	0	0	1
1	0	1	0	1	0	1
0	0	1	1	0	0	1
1	0	1	1	1	1	1
0	1	0	0	0	0	0
1	1	0	0	1	1	0
0	1	0	1	0	1	0
1	1	0	1	1	1	0
0	1	1	0	0	0	1
1	1	1	0	1	1	1
0	1	1	1	0	1	1
1	1	1	1	1	1	1

Другая модель

(1) $$S' = X \otimes S$$

(2) $$z_v = f'_z(s'_v)$$

(3) $$s'_{v+1} = (x_{v+1},\ s_{v+1}) = (x_{v+1},\ f_s(x_v,\ s_v)) = f'_s(x_{v+1},\ s'_v)$$

(4) $$z_v = f'_z(s'_v) = f'_z(f'_s(x_v,\ s'_{v-1})) = f_z(x_v,\ s_v)$$

(5) $$s_{v+1} = s'_v = f'_s(x_v,\ s'_{v-1}) = f_s(x_v,\ s_v)$$

Предсказание поведения автомата

Теорема 1.1. *Пусть дан нетривиальный автомат M с характеристическими функциями f_z и f_s. Тогда реакцию автомата M, находящегося в любом начальном состоянии σ_{i_0}, на любую входную последовательность $\xi_{j_1}\xi_{j_2}\ldots\xi_{j_l}$: (а) предсказать нельзя, если известны только f_z и f_s, (б) предсказать можно, если известны f_z, f_s и σ_{i_0}.*

Таблицы переходов

- Общая таблица переходов

x_v / s_v	z_v				s_{v+1}			
	ξ_1	ξ_2	...	ξ_p	ξ_1	ξ_2	...	ξ_p
σ_1 σ_2 . . . σ_n	В клетках таблицы помещаются значения из множества $\{\zeta_1, \zeta_2, \ldots, \zeta_q\}$				В клетках таблицы помещаются значения из множества $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$			

Таблицы переходов

s_ν \ x_ν	z_ν					$s_{\nu+1}$				
	d	n	u	π	λ	d	n	u	π	λ
1	0	0	0	0	0	2	2	3	1	2
2	0	0	0	0	0	2	2	2	1	2
3	0	0	0	0	0	2	4	2	1	2
4	0	0	0	0	0	5	4	4	1	4
5	0	0	0	1	0	5	4	4	1	4

Перечисление автоматов. Класс (n, p, q) - автоматов

1) Класс (n, p, q) - автоматов

X=$\{\xi_1, \xi_2, \dots, \xi_p\}$

Z= $\{\zeta_1, \zeta_2, \dots, \zeta_q\}$

S= $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$

Мощность $N_{n,\,p,\,q} = (qn)^{pn}$

2) Класс явно минимальных (n, p, q) – автоматов

$f_z(\xi_k,\ \sigma_i) \neq f_z(\xi_k,\ \sigma_j)$

Мощность $N'_{n,\,p,\,q} = n^{pn} \prod_{r=0}^{n-1} (q^p - r)$

3) Класс явно сократимых (n, p, q) – автоматов

$$N''_{n,\,p,\,q} \leqslant \prod_{r=0}^{n-1} [(qn)^p - r]$$

Изоморфные автоматы

Автомат, изоморфный автомату A1

s_ν \ x_ν	z_ν					$s_{\nu+1}$				
	d	*n*	*u*	π	λ	*d*	*n*	*u*	π	λ
1	0	0	0	1	0	1	2	2	5	2
2	0	0	0	0	0	1	2	2	5	2
3	0	0	0	0	0	4	2	4	5	4
4	0	0	0	0	0	4	4	4	5	4
5	0	0	0	0	0	4	4	3	5	4

- Лемма : мощность семейства перестановок явно минимального (n, p, q) – автомата равна n!

- Теорема : мощность класса явно минимальных (n, p, q) – автоматов, не содержащего изоморфных автоматов, определяется формулой

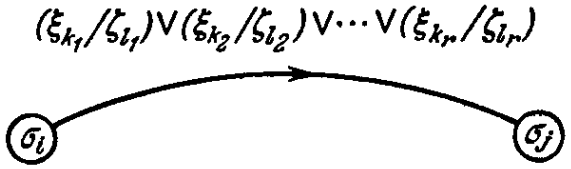
$$N^{(\text{ЯМ})}_{n,\ p,\ q} = \frac{n^{pn}}{n!} \prod_{r=0}^{n-1} (q^p - r)$$

где отрицательные значения $N^{(\text{ям})}_{n,p,q}$ принимаются равными нулю

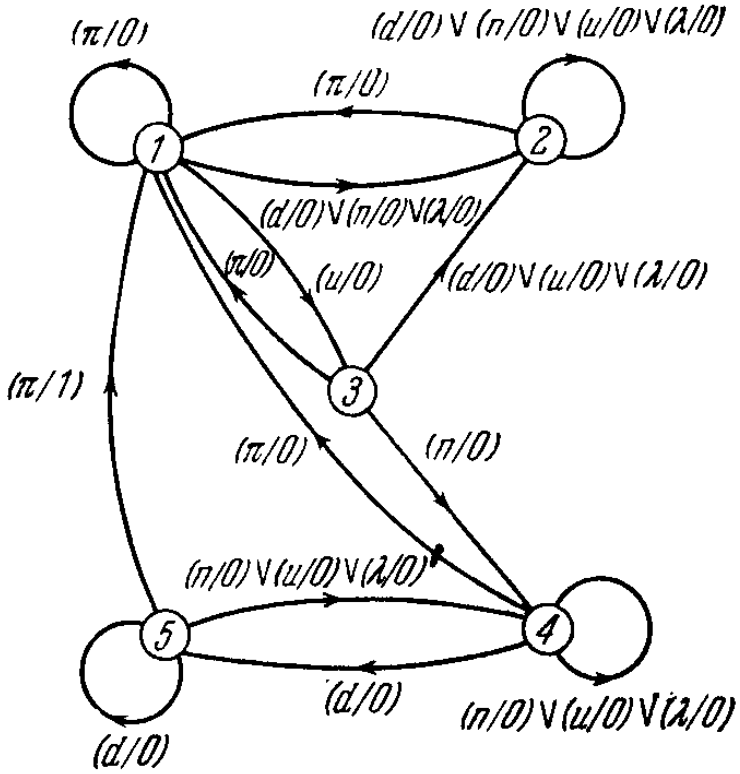
Доказательство :

Граф переходов

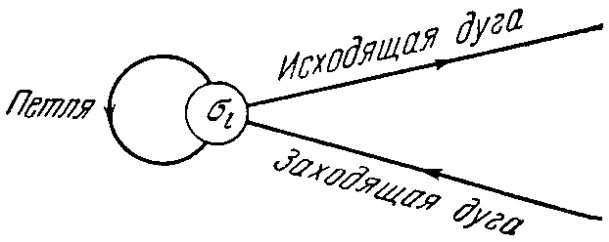
Обозначение дуги



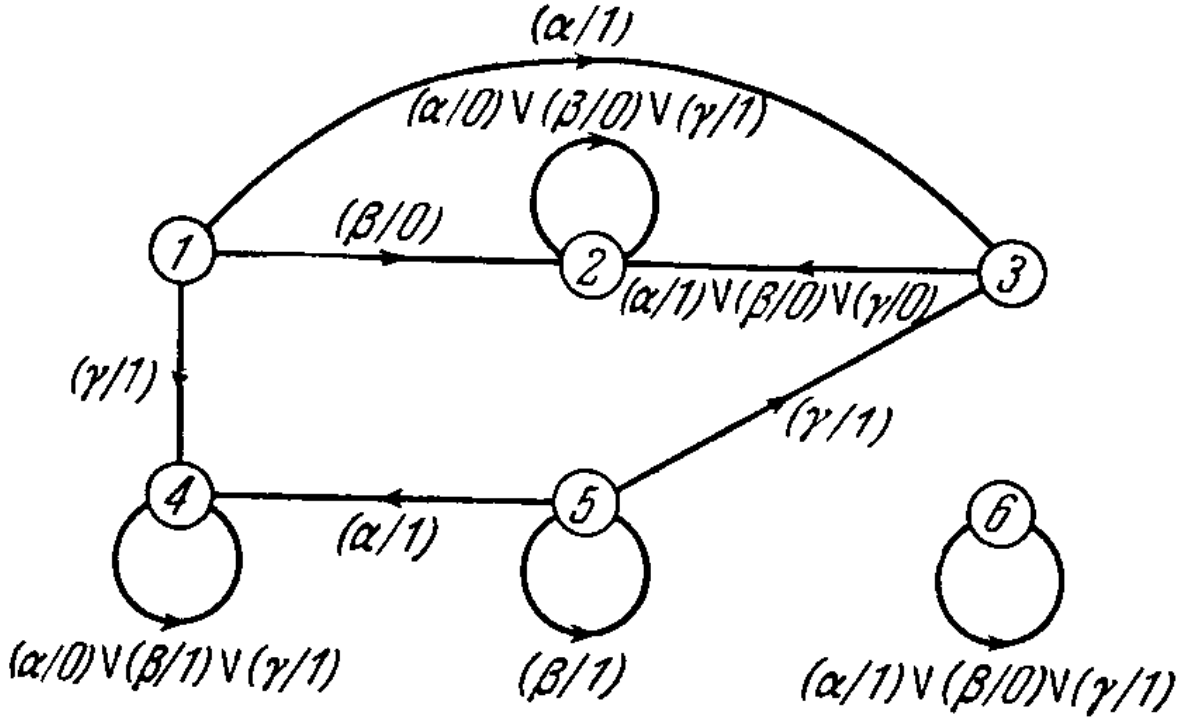
Автомат A1



Классификация состояний и подавтоматов



Автомат А2



Классификация состояний и подавтоматов

Автомат A3

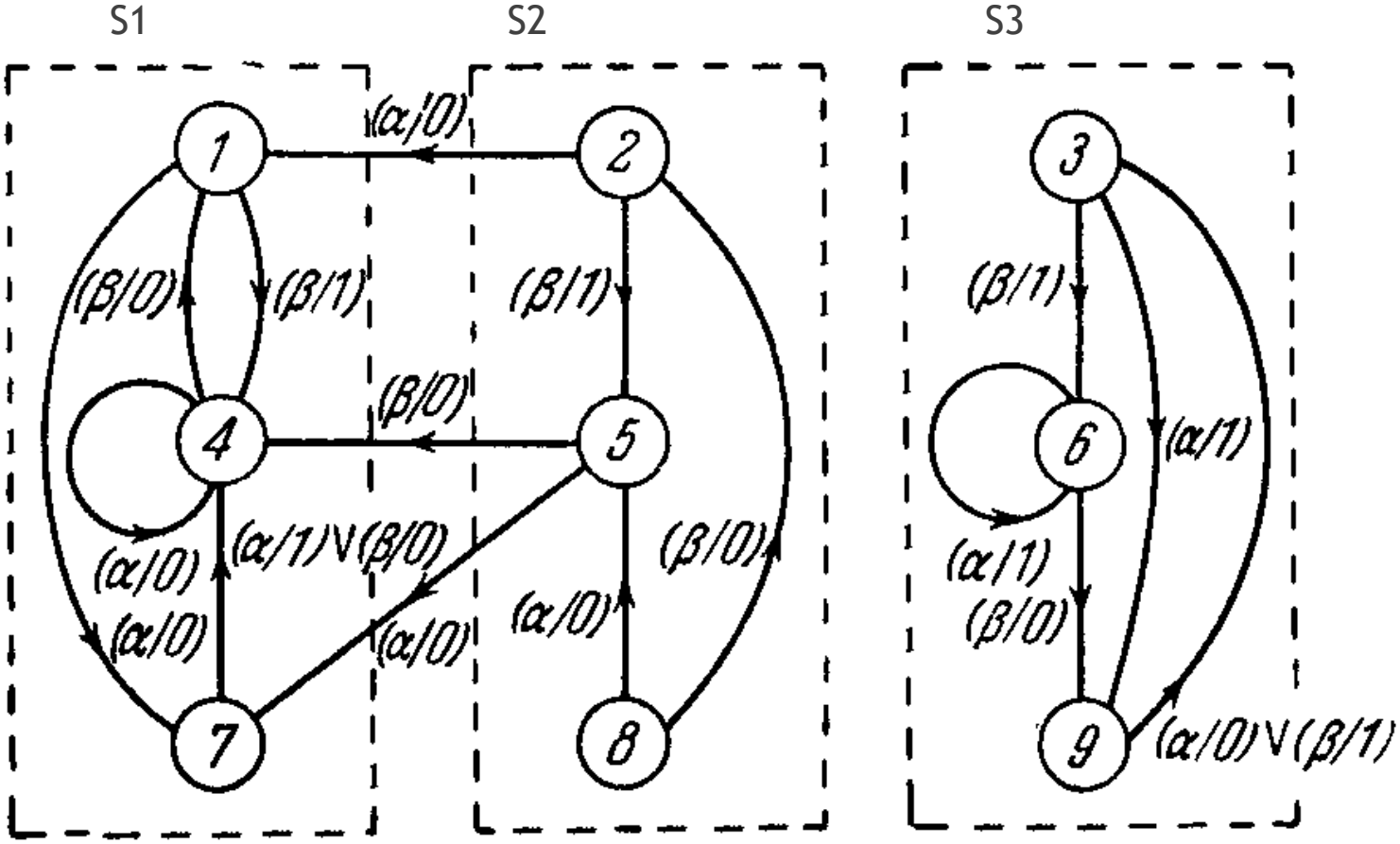


Таблица переходов автомата A3

s_ν \ x_ν	z_ν α	z_ν β	$s_{\nu+1}$ α	$s_{\nu+1}$ β	s_ν \ x_ν	z_ν α	z_ν β	$s_{\nu+1}$ α	$s_{\nu+1}$ β
1	0	1	7	4	6	1	0	6	9
2	0	1	1	5	7	1	0	4	4
3	1	1	9	6	8	1	0	5	2
4	0	0	4	1	9	0	1	3	3
5	0	0	7	4					

Спасибо за внимание!

- Переходим к выполнению практической работы №3

Задачи: практическая работа №3

2.1. Постройте таблицу переходов, граф переходов и матрицу переходов для случаев, сформулированных в задачах 1.2—1.9. Для каждого случая рассмотрите число возможных начальных состояний и входных последовательностей и подтвердите, что выходные последовательности, получаемые на основании различных представлений, соответствуют тем, которые предполагались соответствующими словесным описаниям.

2.2. Известно, что конечный автомат имеет входной алфавит $\{\alpha, \beta\}$, выходной алфавит $\{0, 1\}$ и множество состояний $\{1, 2, 3\}$. Начертите граф переходов, удовлетворяющий этим условиям.

2.3. Подсчитайте число различных: (а) (n, p, q)-автоматов, в которых реакция в настоящий момент зависит только от состояния в настоящий момент и не зависит от входного сигнала в настоящий момент; (б) (n, p, q)-автоматов, в которых $n = p$ и из каждого состояния можно перейти в любое другое, подав на автомат один входной символ; (в) (n, p, q)-автоматов, в которых нет изолированных состояний; (г) (n, p, q)-автоматов, в которых каждый из q выходных символов появляется в таблице переходов, по крайней мере, один раз (достаточно получить рекуррентную формулу для подсчета этого числа автоматов).