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

Таблицы переходов

- Общая таблица переходов

	z_ν				$s_{\nu+1}$			
x_ν / s_ν	ξ_1	ξ_2	$\dots$	ξ_p	ξ_1	ξ_2	$\dots$	ξ_p
σ_1 σ_2 . . . σ_n	В клетках таблицы помещаются значения из множества $\{\zeta_1, \zeta_2, \dots, \zeta_q\}$				В клетках таблицы помещаются значения из множества $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$			

Таблицы переходов

s_ν \ x_ν	z_ν: d	n	u	π	λ	$s_{\nu+1}$: 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 А1

x_ν / s_ν	z_ν: d	z_ν: n	z_ν: u	z_ν: π	z_ν: λ	$s_{\nu+1}$: d	$s_{\nu+1}$: n	$s_{\nu+1}$: u	$s_{\nu+1}$: π	$s_{\nu+1}$: 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

x_ν / s_ν	z_ν: d	z_ν: n	z_ν: u	z_ν: π	z_ν: λ	$s_{\nu+1}$: d	$s_{\nu+1}$: n	$s_{\nu+1}$: u	$s_{\nu+1}$: π	$s_{\nu+1}$: 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

- 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

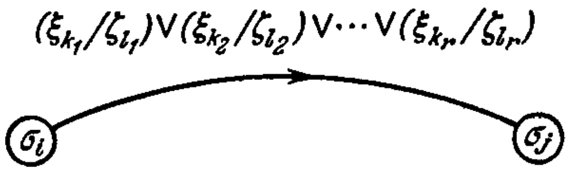
$$N_{n,\,p,\,q}^{(\text{ЯМ})} = \frac{n^{pn}}{n!} \prod_{r=0}^{n-1} (q^p - r)$$

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

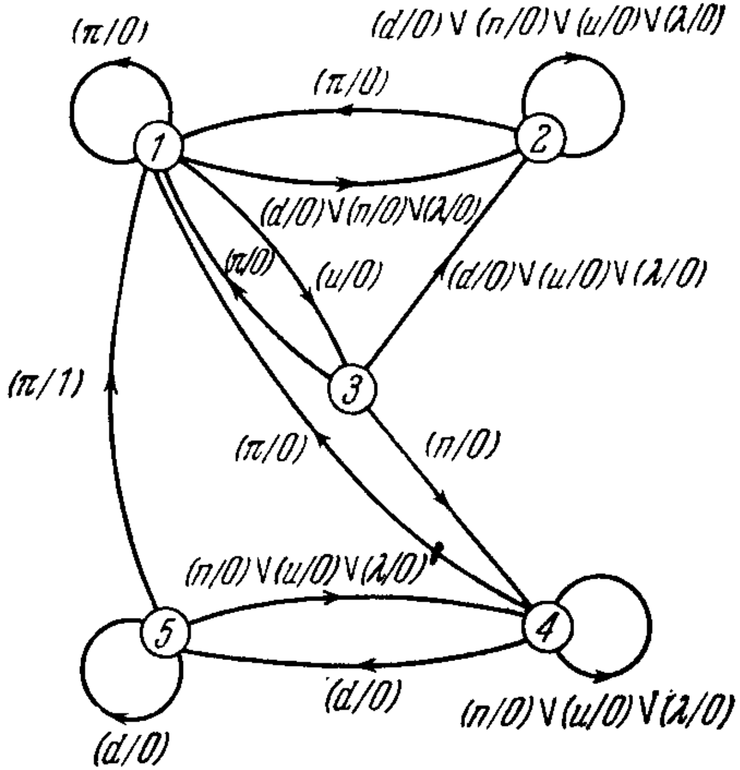
Доказательство :

Граф переходов

Обозначение дуги

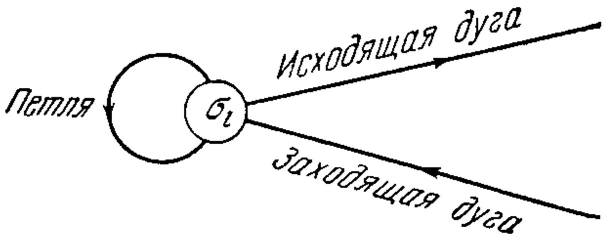


Автомат А1



s_ν \ x_ν	z_ν: d	n	u	π	λ	$s_{\nu+1}$: 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

Классификация состояний и подавтоматов



Автомат А2

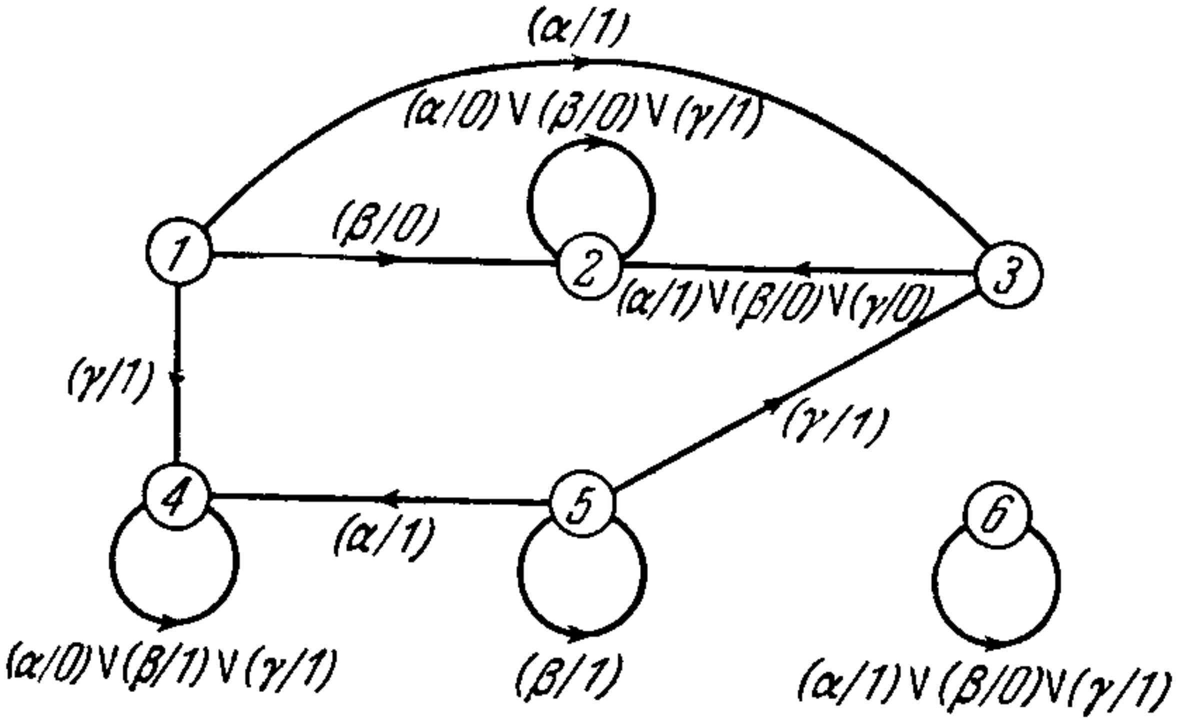
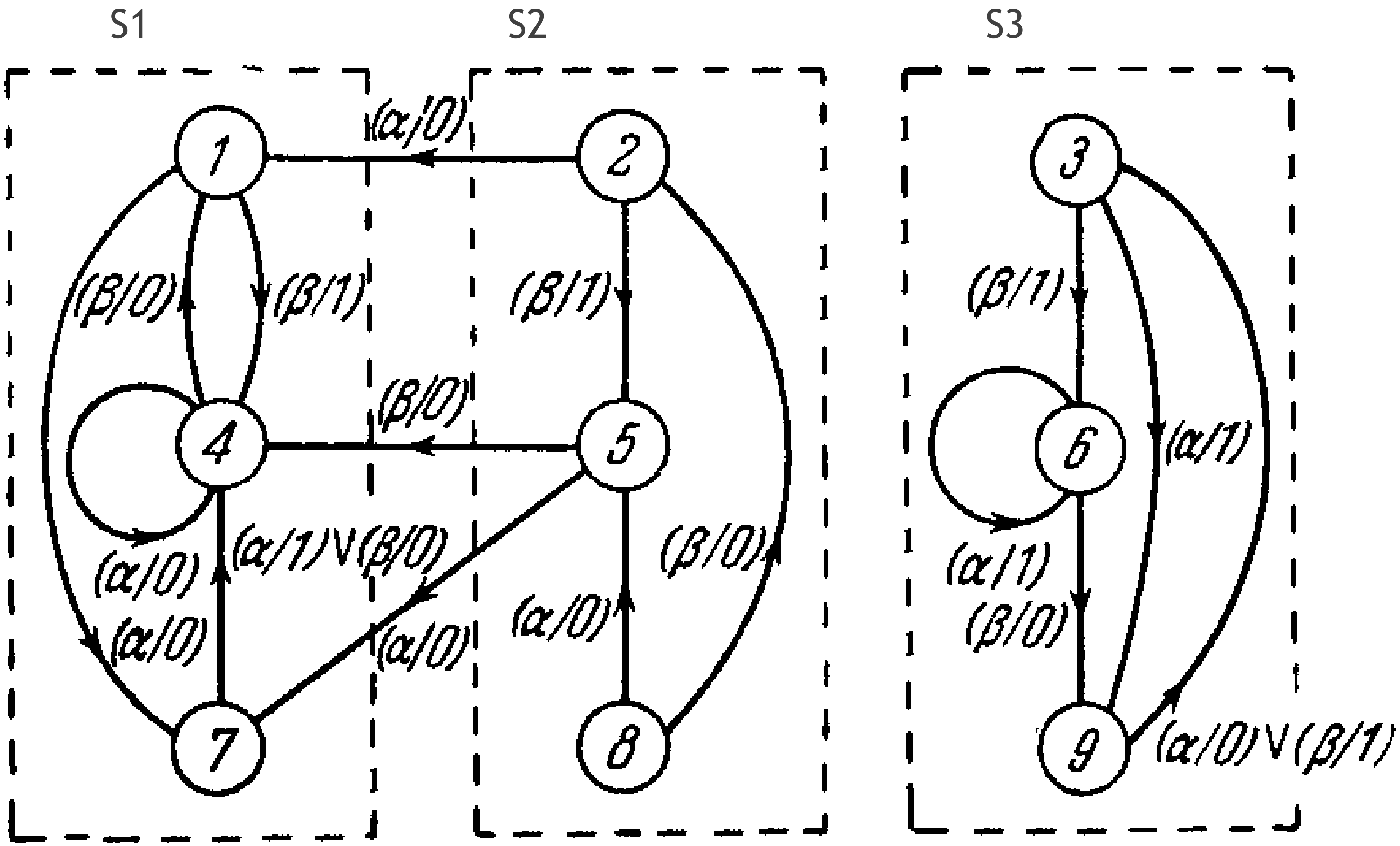


Таблица переходов автомата А3

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

Классификация состояний и подавтоматов

Автомат А3

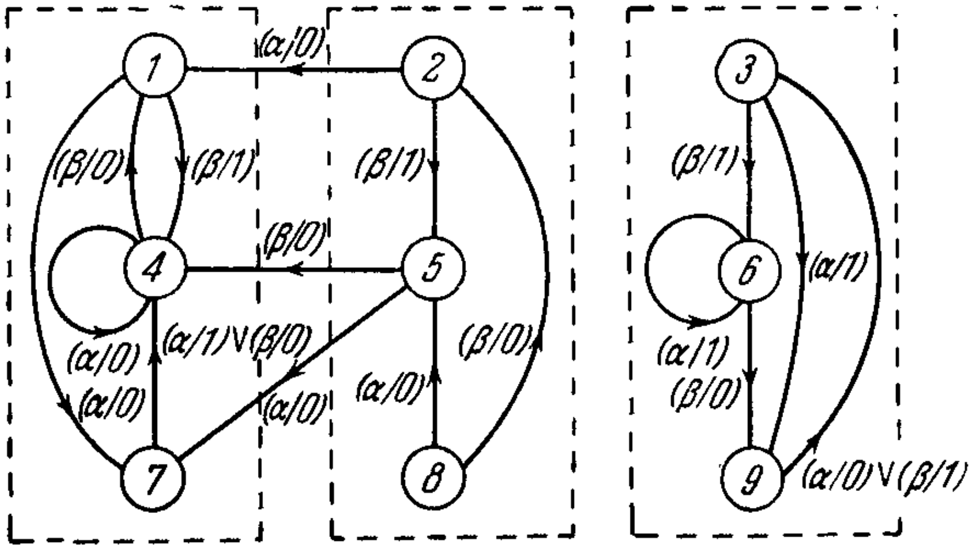


Классификация состояний и подавтоматов

Автомат А3

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

S1 S2 S3



Алгоритм определения множества всех состояний G(S_i)

Дано S_i

Найти G(S_i)

(1) Пусть $G_0(S_i) = \bar{S}_i$. Полагаем $k = 1$

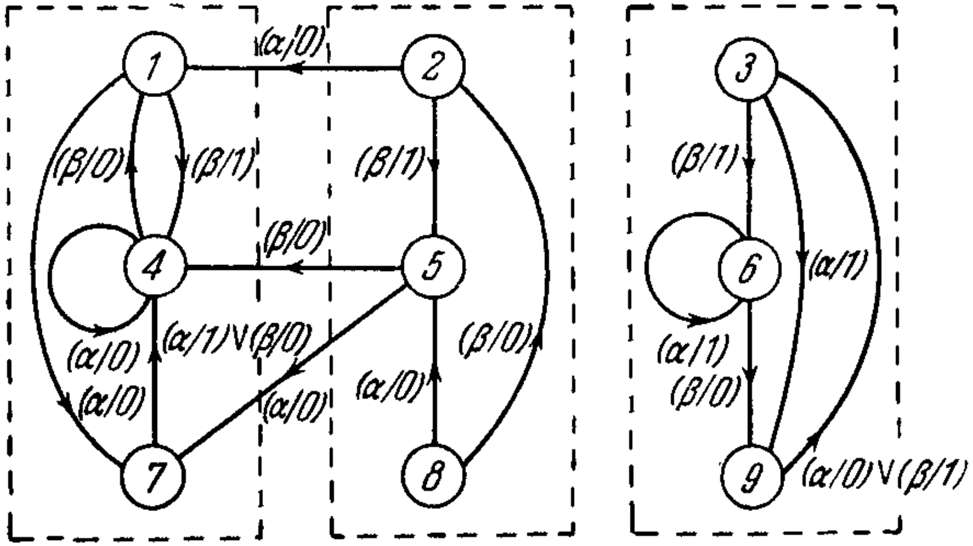
(2) Полагаем $G_k(S_i) = G_1(G_{k-1}(S_i))$

(3) (а) Если $G_k(S_i) \neq G_{k-1}(S_i)$, увеличиваем к на 1 и возвращаемся к (2)

(б) Если $G_k(S_i) = G_{k-1}(S_i)$, то $G_k(S_i)$=G(S_i)

Алгоритм для автомата А3 и состояния $S_i = \{5; 6\}$

k	$\sigma_k(S_i) = \sigma_1(\sigma_{k-1}(S_i))$
0	5, 6
1	4, 5, 6, 7, 9
2	1, 3, 4, 5, 6, 7, 9
3	1, 3, 4, 5, 6, 7, 9



Теорема. *Пусть σ_i и σ_j — два состояния в автомате с n состояниями. Если σ_j вообще достижимо из σ_i, то оно достижимо при подаче входной последовательности длиной не более $n - 1$.*

Матрица переходов

$$e_{ij} = \begin{cases} b_{ij}, & \text{если } b_{ij} \text{ существует,} \\ 0, & \text{если } b_{ij} \text{ не существует.} \end{cases}$$

Матрица переходов для автомата А1:

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array}
\begin{array}{c}
\begin{array}{ccccc} \quad 1 \quad & \quad 2 \quad & \quad 3 \quad & \quad 4 \quad & \quad 5 \quad \end{array} \\
\begin{bmatrix}
(\pi/0) & (d/0)\vee(n/0)\vee(\lambda/0) & (u/0) & 0 & 0 \\
(\pi/0) & (d/0)\vee(n/0)\vee(u/0)\vee(\lambda/0) & 0 & 0 & 0 \\
(\pi/0) & (d/0)\vee(u/0)\vee(\lambda/0) & 0 & (n/0) & 0 \\
(\pi/0) & 0 & 0 & (n/0)\vee(u/0)\vee(\lambda/0) & (d/0) \\
(\pi/1) & 0 & 0 & (n/0)\vee(u/0)\vee(\lambda/0) & (d/0)
\end{bmatrix}
\end{array}$$

$$
[M] = \begin{array}{c} \\ \sigma_{i_1} \\ \sigma_{i_2} \\ \vdots \\ \sigma_{i_r} \\ \\ \end{array}
\begin{array}{c} \sigma_{i_1} \quad \sigma_{i_2} \quad \cdots \quad \sigma_{i_r} \\ \left[\begin{array}{c:c} [M_{11}] & [M_{12}] \\ \hline [M_{21}] & [M_{22}] \end{array}\right] \end{array} .
$$

A3:

$$
\begin{array}{c|ccc:ccc:ccc|}
 & 1 & 4 & 7 & 2 & 5 & 8 & 3 & 6 & 9 \\
1 & 0 & (\beta/1) & (\alpha/0) & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & (\beta/0) & (\alpha/0) & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
7 & 0 & (\alpha/1) \vee (\beta/0) & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hdashline
2 & (\alpha/0) & 0 & 0 & 0 & (\beta/1) & 0 & 0 & 0 & 0 \\
5 & 0 & (\beta/0) & (\alpha/0) & 0 & 0 & 0 & 0 & 0 & 0 \\
8 & 0 & 0 & 0 & (\beta/0) & (\alpha/1) & 0 & 0 & 0 & 0 \\
\hdashline
3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & (\beta/1) & (\alpha/1) \\
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & (\alpha/1) & (\beta/0) \\
9 & 0 & 0 & 0 & 0 & 0 & 0 & (\alpha/0) \vee (\beta/1) & 0 & 0
\end{array}
$$

Спасибо за внимание!

- Переходим к выполнению практической работы №4

Задание 4.

- **Для задач 1.2-1.6 постройте граф переходов. Для каждого случая рассмотрите число возможных начальных состояний и входных последовательностей.**
- **Задания 2.2, 2.3. - общие**
- **Вариант 1 - задачи 1.2, 1.4**
- **Вариант 2 – задачи 1.3., 1.5**

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).