В. Н. САЛИЙ

УНИВЕРСАЛЬНАЯ АЛГЕБРА И АВТОМАТЫ

Саратовский ордена Трудового Красного Знамени
государственный университет им. Н.Г. Чернышевского

В.Н.Салий

УНИВЕРСАЛЬНАЯ АЛГЕБРА И АВТОМАТЫ

Учебное пособие
для студентов механико-математического факультета

Издательство Саратовского университета
1988

УДК 519.95
С 16

В пособии излагаются основные понятия и результаты теории конечных автоматов без выхода, связанные с универсально-алгебраическими конструкциями.

Для студентов механико-математических факультетов университетов, а также для всех занимающихся или интересующихся алгебраической теорией автоматов.

Рекомендуют к печати:
кафедра математической кибернетики
Саратовского университета,
кандидат физико-математических наук В.А.Твердохлебов,
кандидат физико-математических наук В.И.Игошин

С $\frac{1402040000 - 521}{176(02) - 88}$ 90 -88

Вячеслав Николаевич Салий

УНИВЕРСАЛЬНАЯ АЛГЕБРА И АВТОМАТЫ

Учебное пособие
для студентов механико-математического факультета

Редактор Л.В. Аброськина
Технический редактор Л.В.Агальцова Корректор Л.В.Володина

Н/К

Подписано к печати 30.05.88. Формат 60x84 1/16.
Бумага типографская №3. Печать офсетная. Усл.печ.л.4,18(4,5).
Уч.-изд.л. 3,9. Тираж 300. Заказ 3169 Цена 10 к.

Издательство Саратовского университета. 410601, Саратов, Университетская, 42.
ООП Саратовмашинформ статуправления. 410830. Саратов, Сакко и Ванцетти, 54/60.
ISBN 5-292-00263-1

Предлагаемое пособие написано по материалам одноименного спецкурса, который автор читает на механико-математическом факультете Саратовского университета и который был прочтен также (весной 1986 г.) в университете Мартина Лютера в Галле (ГДР).

Представление об автомате без выхода как о конечной унарной алгебре позволяет применить в теории автоматов хорошо разработанные универсально-алгебраические средства, придать установленным с их помощью фактам естественную "автоматную" трактовку.

Все вводимые в тексте конструкции, разумеется, допускают аналоги и для автоматов самого общего вида, где возникает, кроме того, большое число специфических задач. Однако этот переход сопряжен со значительными техническими усложнениями (придется привлекать многоосновные алгебры), борясь с которыми, можно потерять основную идейную нить. Поэтому мы оставляем в стороне эту почти не исследованную область.

Пособие состоит из введения и трех глав, разбитых на параграфы. Каждый параграф имеет свою нумерацию пунктов, теорем и примеров. Список литературы в основном состоит из работ, имеющих непосредственное отношение к тексту. В виде задач поставлены вопросы (в духе обзора А.М.Богомолова и автора [2]), ответ на которые пока не известен. Размышления над ними могут дать толчок к самостоятельной творческой работе.

Введение. АБСТРАКТНЫЕ АВТОМАТЫ И СПОСОБЫ ИХ ЗАДАНИЯ

I. Автоматом называется тройка $\mathcal{A} = (S, X, \delta)$, где S, X - произвольные конечные непустые множества, а $\delta : S \times X \to S$ - функция, определенная на декартовом произведении $S \times X$ и принимающая значения в множестве S.

Элементы множества S называются состояниями автомата $\mathcal{A}$, элементы из X - входными сигналами этого автомата, а δ называется функцией переходов автомата $\mathcal{A}$.

Автомат $\mathcal{A}$ "работает" в дискретной временной шкале по следующему правилу: если s_1 - состояние автомата $\mathcal{A}$ в данный момент, а x - входной сигнал, то в следующий момент $\mathcal{A}$ перейдет в состояние $s_2 = \delta(s_1, x)$.

2. Рассмотрим способы наглядного представления автоматов.

Так как множество состояний S и входной алфавит X конечны, функцию переходов можно задать в виде таблицы с двумя входами.

Пусть $S = \{s_1, s_2, \dots, s_m\}$, $X = \{x_1, x_2, \dots, x_n\}$. Тогда табл. I описывает функцию переходов автомата $\mathcal{A} = (S, X, \delta)$.

Таблица I

δ	x_1	x_2	...	x_n
s_1	$\delta(s_1, x_1)$	$\delta(s_1, x_2)$	...	$\delta(s_1, x_n)$
s_2	$\delta(s_2, x_1)$	$\delta(s_2, x_2)$	...	$\delta(s_2, x_n)$
...	...	...	...	...
s_m	$\delta(s_m, x_1)$	$\delta(s_m, x_2)$	...	$\delta(s_m, x_n)$

Другую возможность представления автоматов дают графы. Состояния автомата изображаются вершинами графа. Если состояние s под действием входного сигнала x переходит в состояние s' (т.е. если $\delta(s, x) = s'$), то из вершины s в вершину s' проводим направленную дугу (стрелку), помеченную символом x.

Таким образом, из одной вершины (s в другую вершину(s' могут вести несколько дуг, но все они имеют различные метки. Число стрелок, выходящих из каждой вершины, в точности равно количеству входных сигналов автомата.

Стрелки, соответствующие различным входным сигналам, можно рисовать различными красками. Тогда метки опускают.

П р и м е р I. Пусть S - множество остатков при делении натуральных чисел на 6, $X=\{x_1,x_2\}$, $\delta(s,x_1)=s+1 \pmod 6$, $\delta(s,x_2)=2s \pmod 6$. Автомат $\mathcal{A}=(S,X,\delta)$ опишем таблицей переходов (табл. 2) и графом (рис. I).

Таблица 2

s	x_1	x_2
0	I	0
I	2	2
2	3	4
3	4	0
4	5	2
5	0	4

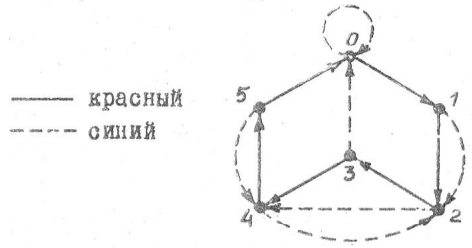


Рис. I

3. Автомат $\mathcal{A}$ называется автономным, если X является одноэлементным множеством: $X=\{x\}$.

В дальнейшем автономные автоматы будем записывать в виде $\mathcal{A}=(S,\delta)$ и рассматривать δ как отображение множества S в себя, т.е. $\delta: S \to S$.

Пусть $\mathcal{A}=(S,X,\delta)$ - некоторый автомат. Для фиксированного входного сигнала $x_i \in X$ определим функцию $\delta_i: s \mapsto \delta(s,x_i)$. Автономные автоматы $\mathcal{A}_i=(S,\delta_i)$, $i=1,2,\ldots,n$, назовем автономными компонентами автомата $\mathcal{A}$.

Произвольный автомат можно задать также и набором графов, представляющих его автономные компоненты.

П р и м е р 2. Автомат, который мы рассматривали в предыдущем примере, имеет две автономные компоненты: $\mathcal{A}_1=(S,\delta_1)$, где $\delta_1(s)=\delta(s,x_1)$, и $\mathcal{A}_2=(S,\delta_2)$, где $\delta_2(s)=\delta(s,x_2)$. Представим их таблицами переходов (табл. 3) и графами переходов (рис. 2).

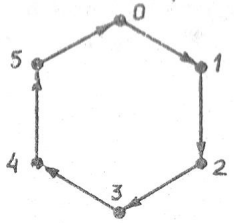
Таблица 3

s	0	I	2	3	4	5
$\delta_1(s)$	I	2	3	4	5	0
$\delta_2(s)$	0	2	4	0	2	4

4. Пусть $\mathcal{A}=(S, X, \delta_{\mathcal{A}})$ и $\mathcal{B}=(T, X, \delta_{\mathcal{B}})$ будут произвольными автоматами с одним и тем же входным алфавитом X. Говорят, что $\mathcal{A}$ и $\mathcal{B}$ изоморфны (и пишут $\mathcal{A} \cong \mathcal{B}$), если существует взаимно однозначное отображение $\varphi : S \xrightarrow{\text{на}} T$ такое, что

$$(\forall s \in S)(\forall x \in X)(\varphi(\delta_{\mathcal{A}}(s,x)) = \delta_{\mathcal{B}}(\varphi(s), x)).$$

Это отображение φ называется изоморфизмом.



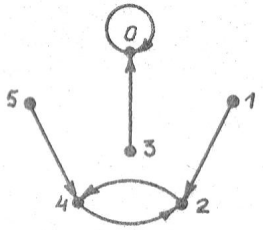


Рис. 2

Несложные рассуждения показывают, что отношение изоморфности является отношением эквивалентности в множестве всех автоматов.

Изоморфные автоматы с абстрактной точки зрения не различаются: они считаются различными реализациями одного и того же абстрактного автомата.

Когда хотят составить общее впечатление о структуре некоторого автомата, рисуют его граф, опуская обозначения вершин (но стрелки по-прежнему останутся раскрашенными (или помеченными)). Понятно, что два автомата тогда и только тогда могут быть представлены одним и тем же графом с "немыми" вершинами, когда эти автоматы изоморфны.

Пример 3. Пусть функция переходов автомата $\mathcal{B}$ задана таблицей 4, а). Покажем, что этот автомат изоморфен автомату $\mathcal{A}$ из примера I.

Таблица 4

а)

$\delta_{\mathcal{B}}$	x_1	x_2
t_1	t_4	t_1
t_2	t_5	t_3
t_3	t_6	t_2
t_4	t_2	t_2
t_5	t_3	t_1
t_6	t_1	t_3

б)

	x_1	x_2
t_1	t_4	t_1
t_2	t_2	t_2
t_3	t_6	t_3
t_4	t_3	t_1
t_5	t_6	t_2
t_6	t_1	t_3

Рассмотрим отображение $\varphi: S \to T$ со следующими значениями: $\varphi(0)=t_1, \varphi(1)=t_4, \varphi(2)=t_2, \varphi(3)=t_5, \varphi(4)=t_3$ и, наконец, $\varphi(5)=t_6$. Видно, что φ взаимно однозначно. Перепишем таблицу переходов автомата $\mathcal{A}$, проставляя вместо каждого состояния его φ-образ (табл. 4, б)). Легко заметить, что полученная таблица есть не что иное, как таблица переходов автомата $\mathcal{B}$ (нужно только расставить в одинаковом порядке строчки). Таким образом, имеем: $(\forall s \in S)(\forall x \in X)(\varphi(\delta_{\mathcal{A}}(s,x)) = \delta_{\mathcal{B}}(\varphi(s),x))$, т.е. φ является изоморфизмом.

Можно поступить и по-другому. Нарисуем (затратив некоторые усилия) граф переходов автомата $\mathcal{B}$ в виде, показанном на рис.3. Если отвлечься от названий вершин, получился граф автомата $\mathcal{A}$. Значит, автоматы $\mathcal{A}$ и $\mathcal{B}$ изоморфны. Изоморфизм задается отождествлением "одинаковых" вершин: $0 \leftrightarrow t_1$, $1 \leftrightarrow t_4$, $2 \leftrightarrow t_2$, $3 \leftrightarrow t_5$, $4 \leftrightarrow t_3$, $5 \leftrightarrow t_6$.

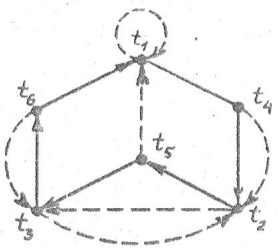


Рис. 3

Пример 4. Автономные компоненты упомянутого в примерах 1-3 автомата $\mathcal{A}$ не изоморфны между собой: у них "совсем разные" графы (см. рис. 2).

Пример 5. Пусть $S=\{s_1,s_2\}$, $T=\{t_1,t_2\}$, $X=\{x_1,x_2\}$. Автомат $\mathcal{A}=(S,X,\delta_{\mathcal{A}})$ с функцией переходов $\delta_{\mathcal{A}}$: $s_1 \xrightarrow{x_1} s_2 \xrightarrow{x_1} s_2$, $s_2 \xrightarrow{x_2} s_1 \xrightarrow{x_2} s_1$ и автомат $\mathcal{B}=(T,X,\delta_{\mathcal{B}})$ с функцией переходов $\delta_{\mathcal{B}}$: $t_1 \xrightarrow{x_1} t_2 \xrightarrow{x_1} t_2$, $t_1 \xrightarrow{x_2} t_2 \xrightarrow{x_2} t_2$ не являются изоморфными, хотя все четыре автономные компоненты: $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{B}_1$, $\mathcal{B}_2$ – попарно изоморфны. Если бы какое-нибудь отображение $\varphi: S \to T$ было изоморфизмом, мы получили бы следующую цепочку рассуждений, приводящую к противоречию:

$$s_1 \neq s_2 \Longrightarrow \delta_{\mathcal{A}}(s_1,x_2) \neq \delta_{\mathcal{A}}(s_1,x_1) \Longrightarrow \varphi(\delta_{\mathcal{A}}(s_1,x_2)) \neq \varphi(\delta_{\mathcal{A}}(s_1,x_1)) \Longrightarrow$$

$$\Longrightarrow \delta_{\mathcal{B}}(\varphi(s_1),x_2) \neq \delta_{\mathcal{B}}(\varphi(s_1),x_1) \Longrightarrow t_2 \neq t_2.$$

Пример 6. Заметим, что в силу принятого определения изоморфности автоматы $\mathcal{A}$ и $\mathcal{B}$, заданные таблицами 5, а) и б) соответственно, не изоморфны. Дело в том, что когда мы говорим об изоморфизме двух автоматов, их входные алфавиты ("внешняя среда") считаются одинаковыми, и следовательно, ка-

ждый входной сигнал имеет свой постоянный, фиксированный цвет, который должен сохраняться в обоих графах. Чтобы изобразить $\mathcal{A}$ и $\mathcal{B}$ одним и тем же графом с "немыми" вершинами, пришлось бы поменять цвета у входных сигналов x_1 и x_2, а это запрещено.

Таблица 5

а)

$\delta_{\mathcal{A}}$	x_1	x_2
s_1	s_1	s_2
s_2	s_2	s_1

б)

$\delta_{\mathcal{B}}$	x_1	x_2
t_1	t_2	t_1
t_2	t_1	t_2

5. Очевидно, что существует единственный абстрактный автономный автомат с одним состоянием. Графом его является "петля".

Переходя к построению абстрактных автономных автоматов с двумя состояниями, заметим, что имеется лишь три способа добавления нового состояния к уже имеющемуся автомату: 1) в качестве изолированного состояния, 2) в качестве "недостижимого" состояния (т.е. состояния, в которое автомат в принципе не может перейти), 3) в качестве "циклического" (т.е. входящего в неодноэлементный цикл) состояния.

Действуя таким образом, из одноэлементного автомата получаем три существенно различных (т.е. попарно не изоморфных) автономных автомата с двумя состояниями (рис. 4).

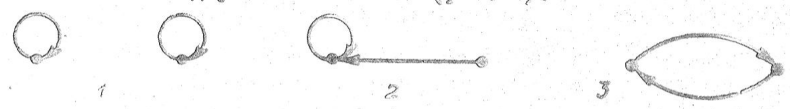


Рис. 4

Теперь перечислим все существенно различные автономные автоматы с тремя состояниями.

Добавляя к каждому из полученных автоматов с двумя состояниями третье состояние по способу 1, находим три автомата (рис. 5).

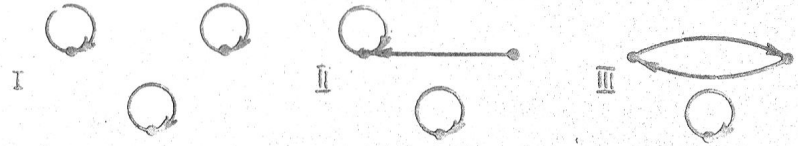


Рис. 5

Требуя, чтобы новое состояние было недостижимым (способ 2), строим еще три автомата (рис. 6).

Способ 3 дает лишь один новый автомат (три другие уже встречались). Его граф изображен последним на рис. 6.

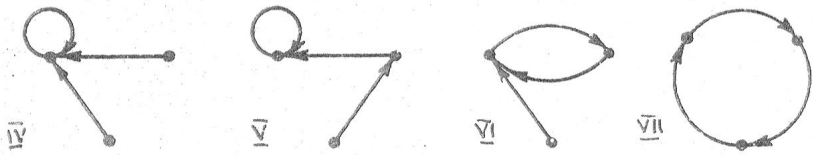


Рис. 6

Последовательным применением описанной процедуры можно для любого натурального числа n получить все попарно не изоморфные автономные автоматы с n состояниями. Через $i(n)$ обозначим количество таких автоматов. Как мы видели, $i(1)=1$, $i(2)=3$, $i(3)=7$. Чему равно $i(4)$?

ЗАДАЧА I. Чему равно $i(n)$ для произвольного n? (Указать точную или асимптотическую формулу).

6. Пусть S - непустое множество, n - натуральное число. Операцией арности n, или n-арной операцией, на множество S называется отображение $o: S^n \to S$, где S^n - декартова n-я степень множества S, т.е. совокупность всевозможных упорядоченных n-ок $(s_1, s_2, \ldots, s_n)$ составленных из элементов множества S. При $n=1,2,3$ получаем соответственно унарную, бинарную, тернарную операции. Если в множестве S фиксируется некоторый элемент, то говорят иногда, что на S задана нульарная операция, которую обозначают так же, как и упомянутый элемент.

Пусть $\mathcal{A}=(S, X, \delta)$ - некоторый автомат. Сопоставляя каждому входному сигналу $x_i \in X$ функцию $\delta_i: S \to S : s \mapsto \delta(s, x_i)$, определяем на множестве S унарную операцию. Это дает возможность рассматривать автомат $\mathcal{A}$ как унарную алгебру, т.е. как множество, на котором задана некоторая совокупность унарных операций: $(S, \delta_1, \delta_2, \ldots, \delta_m)$. В этом смысле всякая конечная (т.е. с конечным числом элементов) унарная алгебра $(S, \delta_1, \delta_2, \ldots, \delta_m)$ получается из некоторого автомата: в качестве множества его состояний берем S, входных сигналов будет столько, сколько в алгебре операций, и для $s \in S$, $x \in X$ полагаем $\delta(s, x_i) = \delta_i(s)$.

Алгебра с одной унарной операцией называется унаром. С нашей точки зрения автономные автоматы - это не что иное, как конечные унары.

Типом алгебры называется последовательность (в порядке убывания) арностей ее операций. Две алгебры, имеющие одинаковый

тип, называются однотипными. Автомат с m входными сигналами как алгебра имеет тип $(1, 1, \ldots, 1)$. Тип унара - (1).

Пусть $(S, o_1, o_2, \ldots, o_m)$ и $(T, o_1, o_2, \ldots, o_m)$ - две однотипные алгебры (соответствующие друг другу операции обозначены одним и тем же символом). Гомоморфизмом первой алгебры во вторую называют отображение $\varphi : S \to T$, согласованное со всеми операциями в том смысле, что для любой n-арной операции o и любого набора $x_1, x_2, \ldots, x_n \in S$ выполняется равенство

$$\varphi(o(x_1, x_2, \ldots, x_n)) = o(\varphi(x_1), \varphi(x_2), \ldots, \varphi(x_n)).$$

Изоморфизм алгебр - это взаимно однозначное соответствие между их элементами, являющееся гомоморфизмом. Сопоставляя это определение с понятием изоморфизма автоматов, видим, что два автомата изоморфны тогда и только тогда, когда изоморфны соответствующие им унарные алгебры.

Глава I. РЕШЕТКА ПОДАВТОМАТОВ АВТОМАТА

§1. Упорядоченные множества и решетки

1. Упорядоченным множеством (у-множеством) называется пара $(A, \leq)$, где A - непустое множество, а $\leq$ - бинарное отношение порядка на A, по определению удовлетворяющее следующим условиям:

1) $x \leq x$ (рефлексивность),

2) $x \leq y \;\&\; y \leq z \Longrightarrow x \leq z$ (транзитивность),

3) $x \leq y \;\&\; y \leq x \Longrightarrow x = y$ (антисимметричность).

Выражение $x \leq y$ читается по-разному: " x меньше (меньше или равен, не больше, содержится в, включается в) y " или соответственно " y больше (больше или равен, не меньше, содержит, включает) x ". Тот же смысл имеет и запись $y \geq x$. Наконец, в том случае, когда $x \leq y$ и $x \neq y$, пишут знак строгого неравенства: $x < y$ или $y > x$.

Заметим, что в каждом конкретном случае в у-множестве для обозначения порядка, как правило, имеется свой традиционный знак.

Пример 1. Множество $\mathbb{N}$ натуральных чисел упорядочивается обычным отношением $\leq$.

Пример 2. Пусть в множестве $\mathbb{N}$ запись $x|y$ означает, что число x является делителем числа y. Нетрудно проверить, что $(\mathbb{N}, |)$ - тоже у-множество.

Так как, например, $2 \leq 3$, но 2 не является делителем тройки, то $\leq$ и $|$ - разные порядки на $\mathbb{N}$: одно и то же множество можно упорядочивать разными способами.

П р и м е р 3. Для произвольного множества A через $P(A)$ обозначим множество всех его подмножеств. Теоретико-множественное включение $\subseteq$ упорядочивает множество $P(A)$.

2. Наименьшим элементом у-множества $(A, \leq)$ называется его элемент 0 (ноль), удовлетворяющий в $(A, \leq)$ тождественному неравенству $0 \leq x$. Очевидно, что каждое у-множество имеет разве лишь один наименьший элемент (если 0_1 и 0_2 - наименьшие элементы в $(A, \leq)$, то $0_1 \leq 0_2$ и $0_2 \leq 0_1$ одновременно, откуда $0_1 = 0_2$, вследствие антисимметричности).

Наибольший элемент 1 (единица) определяется в $(A, \leq)$ тождественным неравенством $x \leq 1$. Очевидно, что каждое у-множество имеет разве лишь один наибольший элемент.

П р и м е р 4. Число I является наименьшим элементом в у-множествах $(\mathbb{N}, \leq)$ и $(\mathbb{N}, |)$. Ни $(\mathbb{N}, \leq)$, ни $(\mathbb{N}, |)$ наибольшего элемента не имеют.

П р и м е р 5. Множество $\mathbb{R}$ действительных чисел, упорядоченное обычным отношением $\leq$, не имеет ни наименьшего, ни наибольшего элемента.

П р и м е р 6. В у-множестве $(P(A), \subseteq)$ пустое подмножество $\varnothing$ будет наименьшим, а само множество A - наибольшим элементом.

3. Элемент a у-множества $(A, \leq)$ назовем минимальным, если в A нет элементов, строго меньших, чем a . Аналогично элемент a называется максимальным в $(A, \leq)$, если в этом у-множестве нет элементов, строго больших, чем a .

ЛЕММА I. Конечное (т.е. с конечным числом элементов) у-множество имеет по крайней мере один минимальный и по крайней мере один максимальный элемент.

Доказательство. Пусть x - произвольный элемент конечного упорядоченного множества $(A, \leq)$. Если x не минимален, то найдется $x_1 \in A$ такой, что $x_1 < x$. Если x_1 не минимален, то можно найти $x_2 \in A$ такой, что $x_2 < x_1$. И так далее. Получаем убывающую цепь $x > x_1 > x_2 > \ldots$. Поскольку множество A конечно, эта цепь тоже конечна. Ее последний элемент и будет минимальным в A.

Для максимальных элементов рассуждения вполне аналогичны. ▨

В общем случае у-множество может иметь много минимальных и много максимальных элементов, а может не иметь их совсем.

Пример 7. Пусть множество A имеет не менее двух элементов и $P'(A)$ обозначает совокупность всех собственных (т.е. отличных от A) непустых подмножеств в A. Тогда одноэлементные подмножества $\{x\}$, $x \in A$, и только они, будут минимальными элементами в у-множестве $(P'(A), \subseteq)$. Максимальными же элементами будут, очевидно, дополнения одноэлементных подмножеств. Таким образом, $(P'(A), \subseteq)$ имеет много минимальных и много максимальных элементов, но в нем нет ни наименьшего, ни наибольшего элемента.

4. Если в у-множестве $(A, \leq)$ есть наименьший (наибольший) элемент, то он, разумеется, будет единственным минимальным (максимальным) элементом в A.

ЛЕММА 2. Если конечное у-множество имеет только один минимальный (максимальный) элемент, то этот элемент будет наименьшим (наибольшим) элементом.

Доказательство. Пусть a - единственный минимальный элемент конечного у-множества $(A, \leq)$. Для произвольного $x \in A$ рассмотрим начинающуюся с него убывающую цепь $x > x_1 > x_2 > \ldots$. Как было отмечено при доказательстве леммы I, последний элемент x_n этой цепи минимален в $(A, \leq)$. В силу единственности, $x_n = a$, и значит, $a \leq x$ вследствие транзитивности.

5. Пусть x и y - произвольные элементы у-множества $(A, \leq)$. Если $x \leq y$ или $y \leq x$, то x и y называются сравнимыми элементами, в противном случае x и y, по определению, не сравнимы. В случае, когда x и y несравнимые элементы, пишут $x \| y$.

Если любые два элемента у-множества $(A, \leq)$ сравнимы, это у-множество называется линейно упорядоченным, или цепью. Под длиной n-элементной цепи понимают число $n-1$.

Теперь определим высоту $h(x)$ элемента x как наибольшую из длин убывающих цепей, начинающихся с x. Например, для минимального элемента x имеем $h(x) = 0$.

6. Пусть x и y - два элемента у-множества $(A, \leq)$, причем $x < y$. Если в A нет такого элемента z, чтобы было $x < z < y$, то говорят, что y является верхним соседом для x (другая терминология: "y покрывает x") или что x является нижним соседом для y.

Верхние соседи наименьшего элемента 0 называются атомами у-множества, а нижние соседи наибольшего элемента 1 - дуальными атомами.

7. Каждому конечному у-множеству $(A, \leq)$ следующим образом со-

поставляется его диаграмма. Пусть n – максимальная из высот элементов в $(A, \leq)$. На $n+1$ горизонталях, которые пронумерованы снизу вверх числами $0, 1, 2, \ldots, n$, разместим (изображая их кружками) элементы множества A таким образом, чтобы при $h(x)=k$ элемент x лежал на прямой с номером k. Если y является верхним соседом для x, соединим эти элементы отрезком (точнее, двигаясь снизу вверх, соединяем каждый элемент с его нижними соседями).

Полученная фигура (горизонтали не изображаются) и есть диаграмма у-множества $(A, \leq)$.

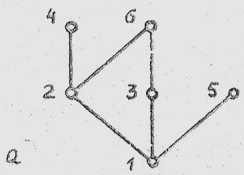
Нетрудно убедиться, что $x < y$ в $(A, \leq)$ в точности тогда, когда на диаграмме у-множества $(A, \leq)$ из x в y ведет восходящая ломаная.

Пример 8. Первые шесть натуральных чисел с обычным порядком $\leq$. Очевидно, что в этом случае $h(x)=x-1$ и диаграмма имеет вид, показанный на рис. 7.

Рис. 7

Пример 9. То же множество, но упорядоченное делимостью. Выписывая убывающие цепи, начинающиеся с каждого элемента (например, для числа 6 это будут 6, 6:1, 6:2, 6:3, 6:2:1, 6:3:1), найдем высоты $h(1)=0$, $h(2)=h(3)=h(5)=1$, $h(4)=h(6)=2$. После чего нетрудно построить диаграмму (рис. 8,а). На диаграмме сразу видны максимальные элементы 4, 5, 6 (наибольшего нет) и наименьший (единственный минимальный) элемент 1.

Пример 10. Множество $P(A)$ всех подмножеств трехэлементного множества $S=\{1, 2, 3\}$, упорядоченное включением. Здесь высота подмножества равна числу его элементов. Диаграмма изображена на рис. 8, б. Одноэлементные множества являются атомами, а их дополнения, т.е. двухэлементные множества, – дуальными атомами.



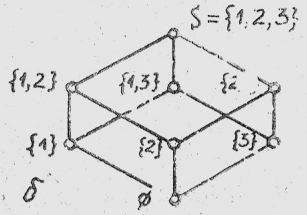


Рис. 8

Пример II. Делители числа 30, упорядоченные делимостью. Очевидно, что $h(1)=0$, для простых делителей 2, 3, 5 высота равна 1, числа 6, 10, 15 имеют высоту 2 (соответствующими максимальными убывающими цепями будут, например, 6:2:1, 10:2:1, 15:3:1), наконец, 30 имеет высоту 3. На рис. 9 приведены два варианта диаграммы для рассматриваемого у-множества (у нас есть произвол в расположении элементов на горизонталях). Если стереть названия элементов, вторая диаграмма совпадет с диаграммой у-множества из примера 10 (рис. 8, б).

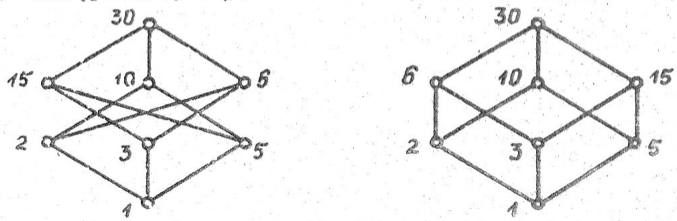


Рис. 9

8. Пусть $(A,\leqslant)$ и $(B,\leqslant)$ - некоторые у-множества. Отображение $\varphi: A \to B$ называется изотонным, если

$$(\forall x,y\in A)(x\leqslant y \Longrightarrow \varphi(x)\leqslant\varphi(y)).$$

Под порядковым изоморфизмом у-множества A на у-множество B понимается взаимно однозначное отображение $\varphi: A \xrightarrow{\text{на}} B$ такое, что

$$(\forall x,y\in A)(x\leqslant y \Longleftrightarrow \varphi(x)\leqslant\varphi(y)).$$

В этом случае говорят, что $(A,\leqslant)$ и $(B,\leqslant)$ изоморфны. Отношение изоморфности является эквивалентностью на множестве всех множеств с отношением порядка.

У-множества, рассматривавшиеся в примерах 10 и 11, изоморфны: порядковым изоморфизмом между ними является, например, соответствие $\varnothing \longleftrightarrow 1$, $\{1\}\longleftrightarrow 2$, $\{2\}\longleftrightarrow 3$, $\{3\}\longleftrightarrow 5$, $\{1,2\}\longleftrightarrow 6$, $\{1,3\}\longleftrightarrow 10$, $\{2,3\}\longleftrightarrow 15$, $S \longleftrightarrow 30$.

Нетрудно понять, что два конечных у-множества тогда и только тогда можно представить одной и той же диаграммой (без обозначения кружков), когда эти у-множества изоморфны.

Пример 12. Диаграммы всех существенно различных (т.е. попарно не изоморфных) трехэлементных у-множеств приведены на рис. 10.

9. Отображение $\varphi: A \xrightarrow{\text{на}} B$ называется антиизоморфизмом, или дуальным изоморфизмом, у-множеств $(A, \leq)$ и $(B, \leq)$, если оно взаимно однозначно и выполняется условие

$$(\forall x, y \in A)(x \leq y \iff \varphi(x) \geqslant \varphi(y)).$$

Например, у-множества, представленные на рис. 10, г и д, антиизоморфны.

10. Пусть A^* - некоторое подмножество у-множества $(A, \leq)$. Элемент $a \in A$ называется нижней гранью для A^*, если $a \leq x$ при любом $x \in A^*$, и называется верхней гранью для A^*, если $x \leq a$ при любом $x \in A^*$.

Под наибольшей нижней (наименьшей верхней) гранью подмножества A^* в $(A, \leq)$ понимается наибольший (наименьший) элемент в множестве всех нижних (верхних) граней для A^* при условии, что такой элемент в $(A, \leq)$ существует.

Очевидно, что любое подмножество $A^* \subseteq A$ имеет разве лишь одну наибольшую нижнюю грань и разве лишь одну наименьшую верхнюю грань. Эти элементы обозначают соответственно $\operatorname{Inf} A^*$ (инфимум) и $\operatorname{Sup} A^*$ (супремум) и называют также точными гранями для A^*.

11. Говорят, что множество A образует относительно порядка $\leq$ решетку, если любое его двухэлементное подмножество имеет наибольшую нижнюю и наименьшую верхнюю грани. Вместо $\operatorname{Inf}\{x, y\}$ и $\operatorname{Sup}\{x, y\}$ будем писать соответственно $\inf(x, y)$ и $\sup(x, y)$.

Пример 13. Любое линейно упорядоченное множество (т.е. любая цепь) является решеткой, так как при $x \leq y$ будет, очевидно, $\inf(x, y) = x$ и $\sup(x, y) = y$. Таким образом, решетками будут $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{R}, \leq)$, причем в каждой из них $\inf(x, y) = \min(x, y)$, $\sup(x, y) = \max(x, y)$ (здесь и далее $\mathbb{Z}$ - множество целых чисел).

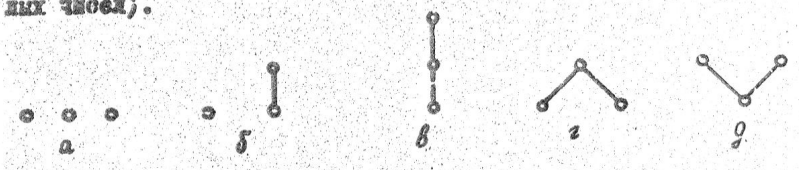


Рис. 10

Пример 14. У-множество $(\mathbb{N}, |)$ - решетка, поскольку для любых $x, y \in \mathbb{N}$ имеем: $\inf(x, y) = \text{НОД}(x, y)$ (наибольший общий делитель), $\sup(x, y) = \text{НОК}(x, y)$ (наименьшее общее кратное).

Пример 15. В $(P(A), \subseteq)$, очевидно, будет $\inf(X,Y)=X\cap Y$ и $\sup(X,Y)=X\cup Y$. Так что и это у-множество является решеткой.

Пример 16. У-множества, изображенные на рис. II, решетками не будут. В первом у-множестве пара $\{x,y\}$ вообще не имеет верхних граней, во втором у $\{x,y\}$ нет нижних граней, в третьем среди нижних граней подмножества $\{x,y\}$ нет наибольшей (а среди верхних граней подмножества $\{u,v\}$ – наименьшей).

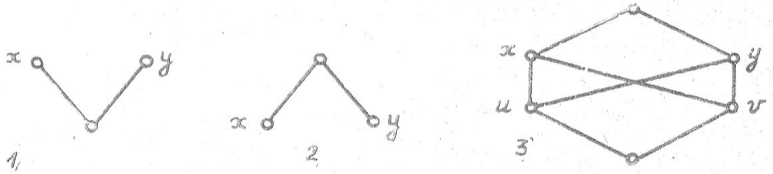


Рис. II

12. Пусть $(A,\leqslant)$ – решетка. Отображение $A\times A\to A:(x,y)\mapsto\inf(x,y)$ представляет собой бинарную операцию на множестве A. Эта операция называется пересечением и обозначается знаком $\wedge$. Так что $x\wedge y \underset{def}{=} \inf(x,y)$ (символ $\underset{def}{=}$ означает равенство по определению).

Отображение $A\times A\to A:(x,y)\mapsto \sup(x,y)$ тоже является бинарной операцией, которая называется объединением и обозначается знаком $\vee$. Так что $x\vee y \underset{def}{=} \sup(x,y)$.

Теперь решетку $(A,\leqslant)$ можно рассматривать как алгебру с двумя бинарными операциями.

Пример 17.

у-множество	Решетка как алгебра
$(\mathbb{N},\leqslant)$	$(\mathbb{N},\min,\max)$
$(\mathbb{N},\mid)$	$(\mathbb{N},\text{НОД},\text{НОК})$
$(P(A),\subseteq)$	$(P(A),\cap,\cup)$

13. Пусть $(A,\wedge,\vee)$ – решетка, рассматриваемая как алгебра. Без труда проверяются следующие свойства пересечения и объединения:

I.1) $x\wedge x=x$, 2) $x\vee x=x$ (идемпотентность);

II.1) $x\wedge y=y\wedge x$, 2) $x\vee y=y\vee x$ (коммутативность);

III.1) $x\wedge(y\wedge z)=(x\wedge y)\wedge z$, 2) $x\vee(y\vee z)=(x\vee y)\vee z$ (ассоциативность);

(Например, полагая $u = x \wedge (y \wedge z)$, $v = (x \wedge y) \wedge z$, имеем: $u \leq x \;\&\; u \leq y \wedge z \Longrightarrow u \leq x \;\&\; u \leq y \;\&\; v \leq z \Longrightarrow u \leq x \wedge y \;\&\; u \leq z \Longrightarrow$ $\Longrightarrow u \leq (x \wedge y) \wedge z = v$, так что $u \leq v$. Аналогично $v \leq u$, и в силу антисимметрии $u = v$);

IУ. I) $x \wedge (x \vee y) = x$, 2) $x \vee (x \wedge y) = x$ (поглощение);

(Например, с одной стороны, $x \leq x \vee (x \wedge y)$, а с другой, так как $x \leq x$ и $x \wedge y \leq x$, то x будет верхней гранью для пары $\{x, x \wedge y\}$, а $x \vee (x \wedge y)$ - это наименьшая верхняя грань этой пары, и значит, $x \vee (x \wedge y) \leq x$. В силу антисимметрии $x \vee (x \wedge y) = x$).

Между алгебраическими операциями и порядком в каждой решетке выполняются следующие вполне понятные соотношения:

$$x \wedge y = x \Longleftrightarrow x \leq y \Longleftrightarrow x \vee y = y.$$

I4. Итак, решетку можно рассматривать и как у-множество, и как алгебру с двумя бинарными операциями. В связи с этим особое значение приобретает

ТЕОРЕМА I. Две решетки тогда и только тогда изоморфны как алгебры, когда они изоморфны как у-мьожества.

Доказательство. I) Пусть $(\mathcal{L}_1, \wedge, \vee)$ и $(\mathcal{L}_2, \wedge, \vee)$ - изоморфные решетки. Это означает, что существует взаимно однозначное отображение φ: $\mathcal{L}_1 \xrightarrow{\text{на}} \mathcal{L}_2$, удовлетворяющее условиям

$$\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y), \quad \varphi(x \vee y) = \varphi(x) \vee \varphi(y).$$

Тогда для любых $x, y \in \mathcal{L}_1$ имеем: $x \leq y \Longleftrightarrow x \wedge y = x \Longleftrightarrow$

$\Longleftrightarrow \varphi(x \wedge y) = \varphi(x) \Longleftrightarrow \varphi(x) \wedge \varphi(y) = \varphi(x) \Longleftrightarrow \varphi(x) \leq \varphi(y)$,

и значит, $\mathcal{L}_1$ и $\mathcal{L}_2$ порядково изоморфны.

2) Пусть теперь $(\mathcal{L}_1, \leq)$ и $(\mathcal{L}_2, \leq)$ будут две порядково изоморфные решетки. Это означает, что существует взаимно однозначное отображение φ : $\mathcal{L}_1 \xrightarrow{\text{на}} \mathcal{L}_2$, удовлетворяющее тождественному соотношению $x \leq y \Longleftrightarrow \varphi(x) \leq \varphi(y)$.

Тогда для любых $x, y \in \mathcal{L}_1$ имеем:

$x \wedge y \leq x \;\&\; x \wedge y \leq y \Longrightarrow \varphi(x \wedge y) \leq \varphi(x) \;\&\; \varphi(x \wedge y) \leq \varphi(y)$,

т.е. $\varphi(x \wedge y)$ является нижней гранью для подмножества $\{\varphi(x), \varphi(y)\}$. Если $\varphi(z)$ - тоже нижняя грань этого подмножества, то

$\varphi(x) \geq \varphi(z) \;\&\; \varphi(y) \geq \varphi(z) \Longrightarrow x \geq z \;\&\; y \geq z \Longrightarrow x \wedge y \geq z \Longrightarrow \varphi(x \wedge y) \geq \varphi(z)$,

так что $\varphi(x \wedge y)$ - наибольшая нижняя грань для $\{\varphi(x), \varphi(y)\}$. Значит,

$\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$. Аналогично доказывается тождественное равенство $\varphi(x \vee y) = \varphi(x) \vee \varphi(y)$.

I5. Следующая теорема имеет бесчисленные приложения.

ТЕОРЕМА 2. Конечное у-множество тогда и только тогда является решеткой, когда I) оно имеет наибольший элемент, 2) для любых двух элементов этого у-множества существует наибольшая нижняя грань.

Доказательство. Пусть $(A, \leq)$ - конечная решетка. Тогда второе условие выполняется по определению решетки, а что касается наибольшего элемента, то им будет очевидно элемент $\sup A$.

Обратно, пусть в конечном у-множестве $(A, \leq)$ имеется наибольший элемент 1 и любая пара элементов имеет наибольшую нижнюю грань. Нужно доказать, что любые два элемента имеют и наименьшую верхнюю грань.

Пусть $a, b \in A$ - произвольные элементы. Через $U(a,b)$ обозначим множество всех верхних граней для подмножества $\{a, b\}$, т.е. $U(a,b) = \{x \in A : x \geq a \;\&\; x \geq b\}$. Очевидно, что $1 \in U(a,b)$, так что $U(a,b)$ не пусто.

У-множество $U(a,b)$ (порядок в нем тот же, что и в $(A, \leq)$) конечно и по лемме I имеет минимальные элементы. Пусть α и β минимальны в $(U(a,b), \leq)$. Согласно второму условию, в $(A, \leq)$ существует $\gamma = \inf(\alpha, \beta)$. Так как α и β лежат в $U(a,b)$, то $a \leq \alpha$, $a \leq \beta$, $b \leq \alpha$, $b \leq \beta$, и следовательно, $a \leq \alpha \wedge \beta = \gamma$ (элемент a - нижняя грань для α и β, а γ - наибольшая нижняя грань для этих элементов) и $b \leq \gamma$. Значит, $\gamma \in U(a,b)$. Так как α и β минимальны в $(U(a,b), \leq)$, то $\alpha = \gamma = \beta$.

Таким образом, у-множество $U(a,b)$ содержит единственный минимальный элемент, который, согласно лемме 2, будет его наименьшим элементом. Следовательно, $\sup(a,b)$ существует.

I6. Подмножество $\mathcal{L}^*$ решетки $(\mathcal{L}, \wedge, \vee)$ называется ее подрешеткой, если $\mathcal{L}^*$ замкнуто относительно обеих операций, т.е. если $x \wedge y$ и $x \vee y$ принадлежат $\mathcal{L}^*$ для любых $x, y \in \mathcal{L}^*$. Заметим, что, согласно этому определению, пустое подмножество будет подрешеткой.

П р и м е р I8. В решетке $\mathcal{L}$ с диаграммой, изображенной на рис. I2, подмножество $\{0, a, b, 1\}$ образует относительно имеющегося в $\mathcal{L}$ порядка решетку. Но это подмножество не будет подрешеткой в $\mathcal{L}$: в нем объединение элементов a и b равно 1, что не согласуется с объединением в решетке $\mathcal{L}$, где $a \vee b = c$.

I7. Решетка $(\mathcal{L}, \wedge, \vee)$ называется дистрибутивной, если в ней выполняется тождество

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$$

называемое дистрибутивным законом.

Важнейший пример дистрибутивной решетки – решетка $(P(A), \cap, \cup)$ всех подмножеств произвольного множества A.

Очевидно, что подрешетка дистрибутивной решетки сама дистрибутивна.

Через M_3 обозначим решетку, изображенную на рис. I3, а, а через N_5 – решетку с диаграммой, представленной на рис. I3, б.

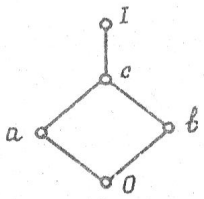
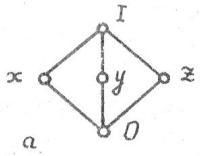


Рис. I2



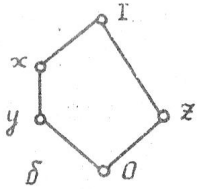


Рис. I3

Простые рассуждения показывают, что решетки M_3 и N_5 не дистрибутивны. В самом деле, в M_3 будет $x \wedge (y \vee z) = x \wedge 1 = x$, но $(x \wedge y) \vee (x \wedge z) = 0 \vee 0 = 0$. Что касается N_5, то там получаем $x \wedge (y \vee z) = x \wedge 1 = x$, но $(x \wedge y) \vee (x \wedge z) = y \vee 0 = y$.

Можно доказать, что решетка тогда и только тогда дистрибутивна, когда в ней нет подрешеток, изоморфных решеткам M_3 и N_5.

Отсюда следует, в частности, что каждая цепь является дистрибутивной решеткой.

§2. Некоторые свойства решетки подавтоматов

I. Пусть $\mathcal{A} = (S, X, \delta)$ – некоторый автомат. Подмножество $S^* \subseteq S$ называется устойчивым в $\mathcal{A}$, если

$$(\forall s \in S)(s \in S^* \longrightarrow (\forall x \in X)(\delta(s,x) \in S^*)).$$

В любом автомате множество состояний S и его пустое подмножество $\varnothing$ устойчивы.

Принципиальное значение имеет следующая простая

ТЕОРЕМА I. Устойчивые подмножества автомата $\mathcal{A} = (S, X, \delta)$ образуют подрешетку решетки $(P(S), \cap, \cup)$ всех подмножеств множества S.

Доказательство. Достаточно показать, что теоретико-множественные

пересечение и объединение любых двух устойчивых подмножеств устойчивы. Пусть S_1 и S_2 – произвольные устойчивые подмножества в автомате $\mathcal{A}$ и $x \in X$ – любой входной сигнал. Тогда имеем:

$$s \in S_1 \cap S_2 \Rightarrow s \in S_1 \,\&\, s \in S_2 \Rightarrow \delta(s,x) \in S_1 \,\&\, \delta(s,x) \in S_2 \Rightarrow \delta(s,x) \in S_1 \cap S_2.$$

Таким образом, $S_1 \cap S_2$ устойчиво. Устойчивость подмножества $S_1 \cup S_2$ доказывается вполне аналогично.

2. Пусть S^* – устойчивое подмножество в автомате $\mathcal{A} = (S, X, \delta)$. Автомат $\mathcal{A}^* = (S^*, X, \delta^*)$ называется подавтоматом автомата $\mathcal{A}$, если δ^* является ограничением функции δ на множестве $S^* \times X$. В дальнейшем будем писать $\mathcal{A}^* = (S^*, X, \delta)$.

Каждый автомат $\mathcal{A}$ имеет, по крайней мере, два подавтомата. Во-первых, сам $\mathcal{A}$ является своим подавтоматом, а во-вторых, им будет и так называемый нулевой подавтомат $\mathbb{0} = (\varnothing, X, \varnothing)$.

Совокупность всех подавтоматов автомата $\mathcal{A}$ обозначается символом $Sub\,\mathcal{A}$.

Если $\mathcal{A}_1 = (S_1, X, \delta)$ и $\mathcal{A}_2 = (S_2, X, \delta)$ – подавтоматы автомата $\mathcal{A}$, то положим $\mathcal{A}_1 \leq \mathcal{A}_2 \underset{def}{\Longleftrightarrow} S_1 \subseteq S_2$ (символ $\underset{def}{\Longleftrightarrow}$ обозначает эквивалентность по определению).

Очевидно, что введенное отношение упорядочивает множество $Sub\,\mathcal{A}$.

Из определения сразу вытекает, что у-множество $(Sub\,\mathcal{A}, \leq)$ порядково изоморфно у-множеству всевозможных устойчивых подмножеств автомата $\mathcal{A}$.

Из сказанного, теорем I,I(§I) и рассуждений, проведенных в пункте I5 (§1), легко получается

ТЕОРЕМА 2. Упорядоченное множество $(Sub\,\mathcal{A}, \leq)$ является дистрибутивной решеткой.

Доказательство. I) Решетка $(P(S), \cap, \cup)$ дистрибутивна (§I, п. I5); 2) устойчивые подмножества образуют подрешетку в решетке $P(S)$ (теорема I); 3) решетка устойчивых подмножеств дистрибутивна (п. I из §I); 4) у-множество $(Sub\,\mathcal{A}, \leq)$ порядково изоморфно решетке устойчивых подмножеств (определение порядка в $Sub\,\mathcal{A}$); 5) $(Sub\,\mathcal{A}, \leq)$ – дистрибутивная решетка (теорема I из §I).

Пример I. Нарисуем диаграмму решетки подавтоматов для каждого типа автономных автоматов с тремя состояниями (рис. I5, I6). В каждом случае будем строить решетку устойчивых подмножеств, а эта решетка, согласно теореме I из §I, является подрешеткой решетки всех подмножеств трехэлементного множества (рис. I4).

В пункте 5 введения были перечислены все семь типов интересующих нас автоматов (мы сохраним нумерацию), а на рис.5 и 6 приведены их графы.

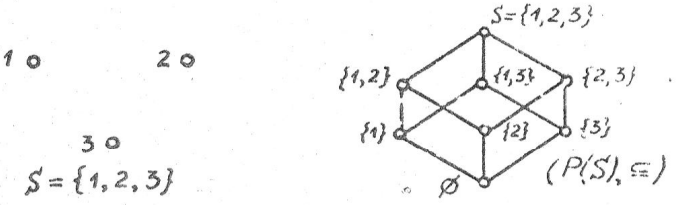


Рис. I4. Трехэлементное множество и решетка его подмножеств

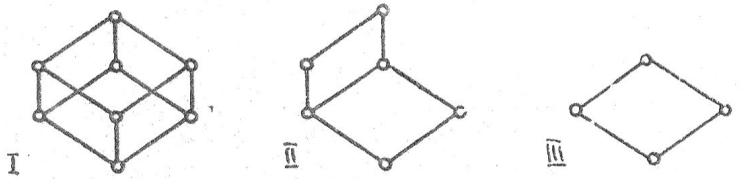


Рис. I5. Решетка $Sub\mathcal{A}$ для автомата $\mathcal{A}$ типов I (устойчивы все подмножества множества S), II (устойчивы $\emptyset, \{1\}, \{3\}, \{1,2\}, \{1,3\}, S$), III (устойчивы $\emptyset, \{3\}, \{1,2\}, S$)

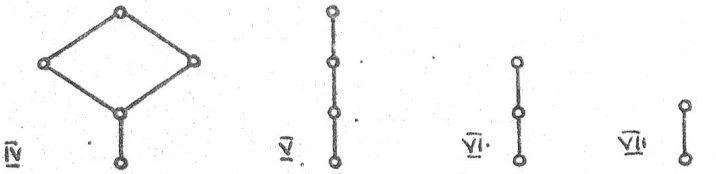


Рис. I6. Решетка $Sub\mathcal{A}$ для автомата $\mathcal{A}$ типов IV (устойчивы подмножества $\emptyset, \{1\}, \{1,2\}, \{1,3\}, S$), V (устойчивы $\emptyset, \{1\}, \{1,2\}, S$), VI (устойчивы $\emptyset, \{1,2\}, S$), VII (нет нетривиальных устойчивых подмножеств)

3. Очевидно, что подмножество $S^* \subseteq S$ тогда и только тогда устойчиво в автомате $\mathcal{A}$, когда оно устойчиво в каждой его автономной компоненте.

П р и м е р 2. Рассмотрим автомат $\mathcal{A}$, с которым мы имели дело в примерах I, 2 из введения. В x_2-компоненте этого автомата имеется много устойчивых подмножеств: $\emptyset, \{0\}, \{0,3\}, \{2,4\}, \{0,2,4\}, \{1,2,4\}, \{2,4,5\}, \{0,2,3,4\}, \{0,1,2,4\}, \{0,2,4,5\}, \{0,1,2,3,4\}, \{0,2,3,4,5\}, S$. Но только два из них: $\emptyset$ и S – будут устойчивыми относительно второго входного сигнала x_1. Таким образом, решетка $Sub\mathcal{A}$ двухэлементна.

4. Автомат $\mathcal{A}$ называется примитивным, если он имеет только тривиальные подавтоматы: $Sub\,\mathcal{A} = \{0, \mathcal{A}\}$.

Чтобы получить описание примитивных автоматов, введем ряд новых понятий.

Пусть $X = \{x_1, x_2, \ldots, x_n\}$ - некоторый алфавит. Через X^* обозначим множество всевозможных конечных последовательностей вида $x_{i_1} x_{i_2} \ldots x_{i_k}$, которые естественно называть словами в алфавите X. Пустое слово e, т.е. слово, не содержащее ни одной буквы, тоже включим в X^*.

Если $\mathcal{A} = (S, X, \delta)$ - автомат с входным алфавитом X, то положим

$$\delta(s, e) = s, \quad \delta(s, px) = \delta(\delta(s, p), x)$$

для произвольных $s \in S$, $p \in X^*$, $x \in X$.

Говорят, что состояние s_2 достижимо в автомате $\mathcal{A}$ из состояния s_1, если существует слово $p \in X^*$ такое, что $\delta(s_1, p) = s_2$.

Множество всех состояний, достижимых из данного состояния s, обозначим через $S(s)$. Например, $s \in S(s)$, поскольку $s = \delta(s, e)$.

Очевидно, что множество $S(s)$ устойчиво при любом $s \in S$. Подавтомат $\mathcal{A}(s) = (S(s), X, \delta)$ называется главным подавтоматом автомата $\mathcal{A}$, порожденным состоянием s.

Ненулевой автомат $\mathcal{A}$ называется сильно связным, если любые два его состояния достижимы друг из друга.

ТЕОРЕМА 3. Автомат примитивен тогда и только тогда, когда он является сильно связным.

Доказательство. I) Пусть s_1, s_2 - произвольные состояния примитивного автомата $\mathcal{A} = (S, X, \delta)$. Вследствие примитивности, будет $\mathcal{A}(s_1) = \mathcal{A}$, и значит, $s_2 \in S(s_1)$. Следовательно, состояние s_2 достижимо из s_1. Точно так же доказывается достижимость состояния s_1 из состояния s_2. Автомат $\mathcal{A}$ сильно связен.

2) Пусть $\mathcal{A}$ - сильно связный автомат и $\mathcal{A}^* = (S^*, X, \delta)$ - его ненулевой подавтомат. Если $s \in S^*$, то, конечно, $S(s) \subseteq S^*$ в силу устойчивости подмножества S^*. С другой стороны, сильная связность автомата $\mathcal{A}$ обеспечивает равенство $S(s) = S$. Итак, $S^* = S$, откуда $\mathcal{A}^* = \mathcal{A}$. Автомат $\mathcal{A}$ примитивен.

СЛЕДСТВИЕ I. Автономный автомат примитивен тогда и только тогда, когда его граф представляет собой цикл.

СЛЕДСТВИЕ 2. Атомами решетки подавтоматов автомата являются его сильно связные подавтоматы, и только они.

СЛЕДСТВИЕ 3. Атомами решетки подавтоматов автономного автомата будут в точности его циклы.

(Последнее утверждение сформулировано весьма свободно, но смысл его, конечно, понятен).

5. Ненулевой автомат называется связным, если пересечение любых двух его ненулевых подавтоматов отлично от 0.

ТЕОРЕМА 4. Для ненулевого автомата $\mathcal{A}$ следующие условия равносильны:

1) $\mathcal{A}$ – связный автомат,

2) решетка подавтоматов $Sub\,\mathcal{A}$ содержит в точности один атом,

3) автомат $\mathcal{A}$ имеет точно один сильно связный подавтомат.

Доказательство. I $\Longrightarrow$ 2, поскольку пересечение двух различных атомов любой решетки равно 0.

2 $\Longrightarrow$ I, так как в случае, когда конечная решетка содержит точно один атом, пересечение любых двух ее ненулевых элементов отлично от 0. Условия 2 и 3 равносильны ввиду следствия 2 из теоремы 3.

СЛЕДСТВИЕ. Автономный автомат тогда и только тогда связен, когда его граф содержит точно один цикл.

6. Состояние s автомата $\mathcal{A}=(S, X, \delta)$ называется недостижимым, если s не достижимо из других состояний этого автомата.

Максимальные собственные подавтоматы автономного автомата описывает

ТЕОРЕМА 5. Подавтомат $\mathcal{A}^*=(S^*, \delta)$ автономного автомата $\mathcal{A}=(S, \delta)$ тогда и только тогда является дуальным атомом решетки подавтоматов $Sub\,\mathcal{A}$, когда дополнение $\overline{S^*}$ подмножества S^* в S представляет собой цикл или недостижимое состояние.

Доказательство. I) Пусть $\mathcal{A}^*$ будет дуальным атомом решетки $Sub\,\mathcal{A}$. Если подмножество $\overline{S^*}$ одноэлементно, то образующее его состояние, конечно, недостижимо. Допустим, что $\overline{S^*}$ имеет по крайней мере два элемента. Если $\overline{S^*}$ не цикл, то в нем найдутся s_1, s_2 такие, что s_1 не достижимо из s_2. Поскольку $\mathcal{A}^*$ – максимальный собственный подавтомат в $\mathcal{A}$, будет $S^* \cup S(s_2) = S$. Но $s_1 \notin S^*$ и $s_1 \notin S(s_2)$. Следовательно, $s_1 \notin S$, что невозможно. Полученное противоречие показывает, что $\overline{S^*}$ – цикл.

2) Пусть $\mathcal{A}^*=(S^*, \delta)$ – подавтомат автомата $\mathcal{A}$, причем S^* удовлетворяет условиям теоремы. Нетрудно заметить, что в этом случае S будет единственным отличным от S^* устойчивым подмножеством, содержащим S^*. Значит, $\mathcal{A}^*$ – дуальный атом решетки $Sub\,\mathcal{A}$ подавтоматов автомата $\mathcal{A}$.

ЗАДАЧА 2. Описать дуальные атомы решетки подавтоматов произвольного автомата.

7. Каждая цепь является дистрибутивной решеткой. Естественный интерес вызывают автоматы с линейно упорядоченной решеткой подавтоматов.

ТЕОРЕМА 6. Решетка подавтоматов автомата $\mathcal{A}$ линейно упорядочена тогда и только тогда, когда, каковы бы ни были два различные состояния автомата $\mathcal{A}$, одно из них достижимо из другого.

Доказательство. Необходимость. Пусть $Sub\mathcal{A}$ – цепь. Предположим, что в $\mathcal{A}$ существуют различные состояния s_1, s_2, не достижимые друг из друга. Тогда главные подавтоматы $\mathcal{A}(s_1)$ и $\mathcal{A}(s_2)$ будут не равнимыми элементами решетки $Sub\mathcal{A}$, – противоречие.

Достаточность. Если состояние s_1 достижимо из состояния s_2, то, конечно, $\mathcal{A}(s_1) \leq \mathcal{A}(s_2)$, так что в автомате $\mathcal{A}$, удовлетворяющем условию теоремы, главные подавтоматы образуют цепь. Но поскольку любой подавтомат представляет собой объединение всех содержащихся в нем главных подавтоматов, получаем, что все подавтоматы автомата $\mathcal{A}$ – главные.

СЛЕДСТВИЕ. Решетка подавтоматов автономного автомата линейно упорядочена тогда и только тогда, когда граф этого автомата является циклом или циклом с одним простым (т.е. без разветвлений) хвостом.

ЗАДАЧА 3. Упростить способ распознавания линейности решетки подавтоматов неавтономного автомата.

8. Элемент a решетки $\mathcal{L}$ называется неразложимым, если для любых $x, y \in \mathcal{L}$ из $a = x \vee y$ следует $a = x$ или $a = y$. Например, наименьший элемент 0 не разложим в любой решетке.

П р и м е р 3. На диаграммах рис. I7 неразложимые элементы изображены черными кружками.

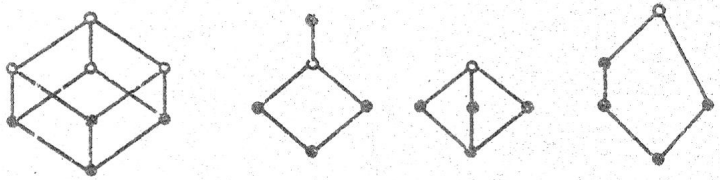


Рис. I7

П р и м е р 4. Каждый элемент цепи не разложим.

ТЕОРЕМА 7. Ненулевой подавтомат $\mathcal{A}^*$ автомата $\mathcal{A}$ тогда и только тогда является неразложимым элементом решетки подавтоматов $Sub\mathcal{A}$, когда $\mathcal{A}^*$ – главный подавтомат.

Доказательство. I) Пусть $\mathcal{A}^*$ - ненулевой неразложимый элемент решетки подавтоматов $Sub\mathcal{A}$ автомата $\mathcal{A}$. Если S^* состоит из элементов $s_1, s_2, \ldots, s_k$, то в решетке $Sub\mathcal{A}$ будет
$\mathcal{A}^* = \mathcal{A}(s_1) \vee \mathcal{A}(s_2) \vee \ldots \vee \mathcal{A}(s_k) = \mathcal{A}(s_1) \vee [\mathcal{A}(s_2) \vee \ldots \vee \mathcal{A}(s_k)]$.

В силу неразложимости, $\mathcal{A}^* = \mathcal{A}(s_1)$ (и тогда все доказано) или $\mathcal{A}^* = \mathcal{A}(s_2) \vee \ldots \vee \mathcal{A}(s_k)$. После нескольких шагов получаем, что $\mathcal{A}^* = \mathcal{A}(s_i)$ для некоторого состояния $s_i \in S^*$. Так что $\mathcal{A}^*$ - главный подавтомат.

2) Пусть $\mathcal{A}(s)$ - главный подавтомат автомата $\mathcal{A}$, порожденный состоянием $s \in S$. Тогда для любых $\mathcal{A}_1, \mathcal{A}_2 \in Sub\mathcal{A}$ имеем:
$\mathcal{A}(s) = \mathcal{A}_1 \vee \mathcal{A}_2 \Longrightarrow S(s) = S_1 \cup S_2 \Longrightarrow s \in S_1 \cup S_2 \Longrightarrow s \in S_1$ или $s \in S_2 \Longrightarrow$
$\Longrightarrow S(s) \subseteq S_1$ или $S(s) \subseteq S_2 \Longrightarrow \mathcal{A}(s) \leq \mathcal{A}_1$ или $\mathcal{A}(s) \leq \mathcal{A}_2$.

С другой стороны,
$\mathcal{A}(s) = \mathcal{A}_1 \vee \mathcal{A}_2 \Longrightarrow \mathcal{A}_1 \leq \mathcal{A}(s)$ & $\mathcal{A}_2 \leq \mathcal{A}(s)$.

Следовательно, $\mathcal{A}(s) = \mathcal{A}_1$ или $\mathcal{A}(s) = \mathcal{A}_2$, - подавтомат $\mathcal{A}(s)$ является неразложимым элементом решетки $Sub\mathcal{A}$.

§3. Конечные дистрибутивные решетки как решетки подавтоматов

I. Пусть $(A, \leq)$ - некоторое у-множество. Подмножество $\mathcal{J} \subseteq A$ называется идеалом в $(A, \leq)$, если
$$(\forall a \in \mathcal{J})(\forall x \in A)(x \leq a \Longrightarrow x \in \mathcal{J}).$$

ЛЕММА. Идеалы любого у-множества $(A, \leq)$ образуют подрешетку решетки $(P(A), \cap, \cup)$.

Доказательство. Достаточно показать, что теоретико-множественное пересечение и теоретико-множественное объединение любых двух идеалов снова будут идеалами.

Пусть $\mathcal{J}_1$ и $\mathcal{J}_2$ - произвольные идеалы у-множества $(A, \leq)$. Для любых $a, x \in A$ имеем:
$x \leq a$ & $a \in \mathcal{J}_1 \cap \mathcal{J}_2 \Longrightarrow x \leq a$ & $(a \in \mathcal{J}_1$ & $a \in \mathcal{J}_2) \Longrightarrow$
$\Longrightarrow (x \leq a$ & $a \in \mathcal{J}_1)$ & $(x \leq a$ & $a \in \mathcal{J}_2) \Rightarrow x \in \mathcal{J}_1$ & $x \in \mathcal{J}_2 \Rightarrow x \in \mathcal{J}_1 \cap \mathcal{J}_2$.

Следовательно, $\mathcal{J}_1 \cap \mathcal{J}_2$ - идеал. Далее,
$x \leq a$ & $a \in \mathcal{J}_1 \cup \mathcal{J}_2 \Longrightarrow x \leq a$ & $(a \in \mathcal{J}_1$ или $a \in \mathcal{J}_2) \Longrightarrow$

$\Rightarrow (x \leq a \;\&\; a \in \mathfrak{J}_1)$ или $(x \leq a \;\&\; a \in \mathfrak{J}_2) \Rightarrow x \in \mathfrak{J}_1$ или $x \in \mathfrak{J}_2 \Rightarrow x \in \mathfrak{J}_1 \cup \mathfrak{J}_2$.

Значит, $\mathfrak{J}_1 \cup \mathfrak{J}_2$ – идеал.

СЛЕДСТВИЕ. Идеалы любого у-множества образуют относительно теоретико-множественного включения дистрибутивную решетку.

ТЕОРЕМА I. Каждая конечная дистрибутивная решетка $\mathfrak{L}$ изоморфна решетке идеалов у-множества, которое образуют в $\mathfrak{L}$ неразложимые элементы.

Доказательство. Пусть $\mathfrak{L}$ – конечная дистрибутивная решетка. Множество неразложимых в $\mathfrak{L}$ элементов обозначим через $I(\mathfrak{L})$. Это множество упорядочено отношением $\leq$, заданным в $\mathfrak{L}$.

Пусть $\mathfrak{J}(\mathfrak{L})$ – решетка идеалов у-множества $(I(\mathfrak{L}), \leq)$.

Очевидно, что для любого $a \in \mathfrak{L}$ множество $I(a) = \{x \in I(\mathfrak{L}) : x \leq a\}$, состоящее из неразложимых в $\mathfrak{L}$ элементов, не превосходящих a, является идеалом в $(I(\mathfrak{L}), \leq)$.

Покажем, что отображение $\varphi : \mathfrak{L} \to \mathfrak{J}(\mathfrak{L}) : a \mapsto I(a)$ будет порядковым изоморфизмом у-множеств $(\mathfrak{L}, \leq)$ и $(\mathfrak{J}(\mathfrak{L}), \subseteq)$.

Сперва заметим, что для любого $a \in \mathfrak{L}$ имеет место представление $a = \bigvee I(a)$ (т.е. что a совпадает с объединением всех элементов, входящих в $I(a)$). Действительно, если элемент a неразложим в $\mathfrak{L}$, то $a \in I(a)$ и, следовательно, a будет наибольшим элементом в $I(a)$, откуда $\bigvee I(a) = a$. Если же a разложим, то $a = a_1 \vee a_2$ для некоторых $a_1 < a$, $a_2 < a$. Каждый из элементов a_1 и a_2 может быть разложимым или неразложимым. После некоторого числа шагов ($\mathfrak{L}$ – конечная решетка!) получим равенство $a = a_1^* \vee a_2^* \vee \ldots \vee a_\kappa^*$, где $a_i^* \in I(a)$, $1 \leq i \leq \kappa$. Отсюда $\bigvee I(a) = a$.

Теперь проверим, что для φ выполняются все свойства порядкового изоморфизма.

I) φ взаимно однозначно.

В самом деле,

$$\varphi(a) = \varphi(b) \Longrightarrow I(a) = I(b) \Longrightarrow a = \bigvee I(a) = \bigvee I(b) = b.$$

2) φ отображает $\mathfrak{L}$ на $\mathfrak{J}(\mathfrak{L})$.

Действительно, пусть $\mathfrak{J}$ – произвольный идеал у-множества $(I(\mathfrak{L}), \leq)$. Положим $a = \bigvee \mathfrak{J}$. Тогда $x \leq a$ для любого $x \in \mathfrak{J}$, так что $x \in I(a)$, и значит, $\mathfrak{J} \subseteq I(a)$. Обратно, пусть x – неразложимый элемент решетки $\mathfrak{L}$, содержащийся в a (т.е. пусть $x \in I(a)$). Если $\mathfrak{J} = \{a_1, a_2, \ldots, a_\kappa\}$, то

$$x = x \wedge a = x \wedge \bigvee_{i=1}^{\kappa} a_i = \bigvee_{i=1}^{\kappa} (x \wedge a_i) = (x \wedge a_1) \vee (x \wedge a_2) \vee \ldots \vee (x \wedge a_\kappa).$$

Но элемент x не разложим в $\mathcal{L}$. Следовательно, $x = x \wedge a_i$ для подходящего i. Значит, $x \le a_i \in \mathcal{J}$. Поскольку $\mathcal{J}$ – идеал в у-множестве $(I(\mathcal{L}), \le)$, получаем, что $x \in \mathcal{J}$. Таким образом, $I(a) \subseteq \mathcal{J}$.

Мы показали, что для любого идеала $\mathcal{J} \in \mathfrak{J}(\mathcal{L})$ будет $\mathcal{J} = \varphi(\vee\mathcal{J})$.

3) φ сохраняет порядок.

В самом деле, для любых $a, b \in \mathcal{L}$ имеем:

$$a \le b \Longrightarrow I(a) \subseteq I(b) \Longrightarrow \vee I(a) \le \vee I(b),$$
$$\varphi(a) \qquad \varphi(b) \qquad a \qquad b$$

откуда $a \le b \Longleftrightarrow \varphi(a) \subseteq \varphi(b)$.

Решетки $(\mathcal{L}, \le)$ и $(\mathfrak{J}(\mathcal{L}), \subseteq)$ изоморфны. ▨

Из доказанного и теоремы I (§ I) вытекает

СЛЕДСТВИЕ. Две конечные дистрибутивные решетки $\mathcal{L}_1$ и $\mathcal{L}_2$ тогда и только тогда изоморфны, когда изоморфны у-множества $I(\mathcal{L}_1)$ и $I(\mathcal{L}_2)$ их неразложимых элементов.

2. Теперь все готово для доказательства основного результата главы I.

ТЕОРЕМА 2. Любая конечная дистрибутивная решетка изоморфна решетке подавтоматов автомата с двумя входными сигналами.

Доказательство. Пусть $\mathcal{L}$ – конечная дистрибутивная решетка. Через $I^*(\mathcal{L})$ обозначим множество, состоящее из неразложимых элементов решетки $\mathcal{L}$, отличных от 0.

Следующим образом построим множество S.

Каждому минимальному элементу l у-множества $(I^*(\mathcal{L}), \le)$ сопоставим элемент $s_0(l)$ так, чтобы было $s_0(l_1) \ne s_0(l_2)$ при $l_1 \ne l_2$.

Пусть l – не минимальный элемент в $(I^*(\mathcal{L}), \le)$. Тогда l имеет в $(I^*(\mathcal{L}), \le)$ нижних соседей: $l_0, l_1, \ldots, l_{k-1}$, $k \ge 1$. Сопоставим элементу l точно k различных элементов: $s_0(l)$, $s_1(l), \ldots, s_{k-1}(l)$.

Проделав указанные действия для каждого элемента $l \in \mathcal{L}$, закончим построение множества S.

Автомат $\mathcal{A}(\mathcal{L}) = (S, X, \delta)$ с двумя входными сигналами x_1, x_2 будет работать по следующим правилам:

1) если l – минимальный элемент у-множества $I^*(\mathcal{L})$, то $\delta(s_0(l), x_1) = s_0(l) = \delta(s_0(l), x_2)$;

2) если l – не минимальный элемент в $I^*(\mathcal{L})$, то состояния $s_0(l), s_1(l), \ldots, s_{k-1}(l)$ относительно входного сигнала x_1 образуют цикл: $s_0(l) \mapsto s_1(l) \mapsto \ldots \mapsto s_{k-1}(l) \mapsto s_0(l)$;

5) если l – не минимальный элемент в $\Gamma^*(\mathcal{L})$ и $l_0, l_1, \ldots, l_{k-1}$ – его нижние соседи, то $\delta(s_i(l), x_2) = s_0(l_i)$, $0 \le i \le k-1$.

По построению, все главные подавтоматы автомата $\mathcal{A}(\mathcal{L})$ имеют вид $\mathcal{A}(s_0(l))$, $l \in \Gamma^*(\mathcal{L})$. Напомним, что главные подавтоматы – это в точности ненулевые неразложимые элементы решетки подавтоматов (теорема 7 из §2).

Отображение $\varphi : \mathcal{A}(s_0(l)) \longmapsto l$ является порядковым изоморфизмом у-множеств $(\{\mathcal{A}(s_0(l)) : l \in \Gamma^*(\mathcal{L})\}, \le)$ и $(\Gamma^*(\mathcal{L}), \le)$. Полагая еще $\varphi(\mathcal{O}) = 0$, получаем, что у-множества $\Gamma(Sub\,\mathcal{A}(\mathcal{L}))$ и $\Gamma(\mathcal{L})$ порядково изоморфны. В силу следствия из теоремы I решетки $\mathcal{L}$ и $Sub\,\mathcal{A}(\mathcal{L})$ изоморфны. ▨

Теорему 2 получили Джонсон и Сейферт (см. Йонссон [35, теорема 3.8.8]).

Пример I. На рис. I8 последовательно изображены: конечная дистрибутивная решетка $\mathcal{L}$ (ненулевые неразложимые элементы выделены черными кружками), у-множество $\Gamma^*(\mathcal{L})$ ее ненулевых неразложимых элементов, граф автомата $\mathcal{A}(\mathcal{L})$, получающегося из $\mathcal{L}$ применением конструкции, описанной в теореме 2.

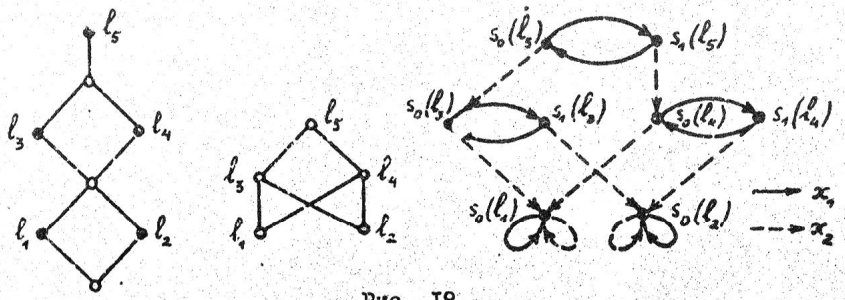


Рис. I8

3. Теорема 2 не дает ответа на вопрос о том, какими свойствами характеризуются решетки подавтоматов автономных автоматов.

Пример 2. Покажем, что решетка $\mathcal{L}$ с диаграммой, изображенной на рис. I2, не может быть реализована как решетка подавтоматов автономного автомата. Действительно, если бы такой автомат существовал, то, согласно следствию 3 из теоремы 3 (§2), его граф имел бы в точности два цикла (в решетке $\mathcal{L}$ два атома). Тогда элемент c представляет объединение этих циклов. Согласно теореме 5(§2), описывающей дуальные атомы решетки подавтоматов автономного автомата, наш гипотетический автомат имеет единственное нециклическое состояние. Но тогда у него получаются две максималь-

ных собственных подавтомата, что невозможно, так как в $\mathcal{L}$ только один дуальный атом.

ТЕОРЕМА 3. Конечная дистрибутивная решетка тогда и только тогда изоморфна решетке подавтоматов автономного автомата, когда нижние грани любого неразложимого в ней элемента образуют цепь.

Доказательство. I) Пусть $\mathcal{A}^*$ – ненулевой неразложимый элемент решетки подавтоматов $Sub\,\mathcal{A}$ автономного автомата $\mathcal{A}$. По теореме 7(§2) $\mathcal{A}^*$ является главным подавтоматом, т.е. $\mathcal{A}^* = \mathcal{A}(s)$ для некоторого $s \in S$. Ясно, что $\mathcal{A}(s)$ имеет в точности один цикл и не более чем одно недостижимое состояние. По теореме 6(§2) подавтоматы автомата $\mathcal{A}(s)$ образуют цепь.

2) Обратно, пусть $\mathcal{L}$ – конечная дистрибутивная решетка, в которой выполнено условие теоремы.

В соответствии с конструкцией теоремы 2 представим $\mathcal{L}$ как решетку подавтоматов автомата $\mathcal{A}(\mathcal{L})$ с двумя входными сигналами.

Поскольку каждый элемент у-множества $(\Gamma^*(\mathcal{L}), \leq)$ имеет не более одного нижнего соседа, входной сигнал x_1 будет каждое состояние переводить в себя. Следовательно, любое подмножество множества S состояний автомата $\mathcal{A}(\mathcal{L})$ будет устойчивым в автономной x_1-компоненте этого автомата. Это означает, что устойчивыми подмножествами автомата $\mathcal{A}(\mathcal{L})$ являются в точности устойчивые подмножества его x_2-компоненты. Таким образом, решетка $Sub\,\mathcal{A}(\mathcal{L})$ (а значит, и $\mathcal{L}$) изоморфна решетке подавтоматов автономного автомата $\mathcal{A}_2(\mathcal{L}) = (S, \delta_2)$. ▨

Теорему 3 также получили Джонсон и Сейферт (см. Йонссон [35, теорема 3.8.9]).

4. Пусть $\mathcal{A} = (S, \delta)$ – автономный автомат. Заменим каждый его цикл петлей, т.е. одноэлементным циклом. Полученный так автомат $\mathcal{A}^\circ = (S^\circ, \delta)$ назовем скелетом автомата $\mathcal{A}$.

ТЕОРЕМА 4. Для любых двух автономных автоматов $\mathcal{A}$ и $\mathcal{B}$ будет $Sub\,\mathcal{A} \cong Sub\,\mathcal{B}$ тогда и только тогда, когда $\mathcal{A}^\circ \cong \mathcal{B}^\circ$.

Доказательство. I) Из определения скелета непосредственно следует, что $Sub\,\mathcal{A} \cong Sub\,\mathcal{A}^\circ$ для каждого автономного автомата $\mathcal{A}$. Поэтому

$$\mathcal{A}^\circ \cong \mathcal{B}^\circ \Longrightarrow Sub\,\mathcal{A}^\circ \cong Sub\,\mathcal{B}^\circ \Longrightarrow Sub\,\mathcal{A} \cong Sub\,\mathcal{B}.$$

2) Пусть $\mathcal{A} = (S, \delta)$ и $\mathcal{B} = (T, \delta)$ – автономные автоматы с изоморфными решетками подавтоматов: $Sub\,\mathcal{A} \cong Sub\,\mathcal{B}$. Тогда будет $Sub\,\mathcal{A}^\circ \cong Sub\,\mathcal{B}^\circ$ и $\Gamma^*(Sub\,\mathcal{B}^\circ) \cong \Gamma^*(Sub\,\mathcal{A}^\circ)$.

Для $s_1, s_2 \in S^\circ$ положим $s_1 \trianglelefteq s_2 \overset{def}{\Longleftrightarrow} s_1 \in S(s_2)$. Очевидно, что отношение $\trianglelefteq$ рефлексивно и транзитивно. Если $s_1 \trianglelefteq s_2$ и одновременно $s_2 \trianglelefteq s_1$, то $s_1 \in S(s_2)$ и одновременно $s_2 \in S(s_1)$. Это означает, что s_1 и s_2 взаимно достижимы в $\mathcal{A}^\circ$, откуда $s_1 = s_2$.

Итак, отношение $\trianglelefteq$ упорядочивает множество S°.

Покажем, что у-множество $(S^\circ, \trianglelefteq)$ изоморфно у-множеству $(\Gamma^*(Sub\mathcal{A}^\circ), \leqslant)$, установив, что отображение $S^\circ \to Sub\mathcal{A}: s \mapsto \mathcal{A}(s)$ является порядковым изоморфизмом.

В самом деле, при этом отображении каждый главный подавтомат автомата $\mathcal{A}^\circ$ имеет прообраз. Далее, наше отображение взаимно однозначно:

$$\mathcal{A}(s_1) = \mathcal{A}(s_2) \Longrightarrow s_1 \in S(s_2) \;\&\; s_2 \in S(s_1) \Longrightarrow s_1 = s_2.$$

Наконец, для любых $s_1, s_2 \in S^\circ$ будет

$$s_1 \trianglelefteq s_2 \Longleftrightarrow s_1 \in S(s_2) \Longleftrightarrow S(s_1) \subseteq S(s_2) \Longleftrightarrow \mathcal{A}(s_1) \leqslant \mathcal{A}(s_2).$$

Так как у-множества $\Gamma^*(Sub\mathcal{A}^\circ)$ и $\Gamma^*(Sub\mathcal{B}^\circ)$ изоморфны, то теперь мы получаем, что $(S^\circ, \trianglelefteq)$ и $(T^\circ, \trianglelefteq)$ также изоморфны. Пусть отображение $\varphi: S \xrightarrow{\text{на}} T$ будет порядковым изоморфизмом между $(S^\circ, \trianglelefteq)$ и $(T^\circ, \trianglelefteq)$. Заметим, что для любого $s \in S^\circ$ состояние $\delta(s)$ является единственным нижним соседом для элемента s в у-множестве $(S^\circ, \trianglelefteq)$. Тогда для любого $s \in S^\circ$ получаем:

$$\varphi(\delta(s)) = \varphi(\text{нижний сосед элемента } s) = \text{нижний сосед элемента } \varphi(s) = \delta(\varphi(s)).$$

Значит, φ - изоморфизм автономных автоматов $\mathcal{A}^\circ$ и $\mathcal{B}^\circ$.

5. С помощью теорем 2 и 4 можно восстановить автономный автомат по решетке его подавтоматов - с точностью до длин циклов. Сначала в решетке подавтоматов $Sub\mathcal{A}$ выделяется у-множество $\Gamma^*(Sub\mathcal{A})$ ненулевых неразложимых элементов. Затем в каждом минимальном элементе этого у-множества рисуем петлю, а из каждого неминимального элемента проводим стрелку к его единственному нижнему соседу. Полученный таким образом граф представляет собой граф переходов скелета $\mathcal{A}^\circ$ автомата $\mathcal{A}$.

ЗАДАЧА 4. **Обобщить построения, проделанные в п.п.4 и 5, на случай произвольных автоматов.**

Глава II. РЕШЕТКА КОНГРУЭНЦИЙ АВТОМАТА

§1. Эквивалентности и разбиения

1. Отношением эквивалентности (коротко: эквивалентностью) на множестве A называется бинарное отношение ε на A, которое тождественно удовлетворяет следующим условиям:

1) $(x,x)\in\varepsilon$ (рефлексивность);

2) $(x,y)\in\varepsilon \;\&\; (y,z)\in\varepsilon \Rightarrow (x,z)\in\varepsilon$ (транзитивность);

3) $(x,y)\in\varepsilon \Rightarrow (y,x)\in\varepsilon$ (симметричность).

Примеры эквивалентностей: отношение равенства $x=y$ на произвольном множестве, изоморфность автоматов $\mathcal{A}\cong\mathcal{B}$, сравнимость натуральных чисел $i\equiv j\,(\mathrm{mod}\,k)$. Конечно, в каждом конкретном случае для обозначения эквивалентности элементов, как правило, имеется свой традиционный знак.

2. Совокупность π непустых подмножеств множества A называется разбиением этого множества, если 1) $A_i\cap A_j=\varnothing$ для любых различных $A_i, A_j\in\pi$; 2) $\bigcup\pi=A$. Подмножества, составляющие данное разбиение, называют его блоками.

Пусть ε - эквивалентность на множестве A. Обозначим через $\varepsilon(x)$ совокупность всех элементов множества A, состоящих с x в отношении ε, т.е. эквивалентных в смысле ε элементу x. Будем называть $\varepsilon(x)$ классом эквивалентности (или ε-классом) элемента x. Понятно, что равенство $\varepsilon(x)=\varepsilon(y)$ равносильно тому, что $(x,y)\in\varepsilon$.

ЛЕММА 1. Всевозможные классы эквивалентности ε образуют разбиение множества A.

Доказательство. 1) Пусть $\varepsilon(x)\cap\varepsilon(y)\neq\varnothing$, т.е. найдется $z\in\varepsilon(x)\cap\varepsilon(y)$. Тогда $(x,z)\in\varepsilon$, $(z,y)\in\varepsilon$, и значит, $(x,y)\in\varepsilon$, откуда $\varepsilon(x)=\varepsilon(y)$. Следовательно, различные классы эквивалентности не пересекаются.

2) Так как каждый элемент x находится в ε-классе $\varepsilon(x)$, то $\bigcup_{x\in A}\varepsilon(x)=A$. ▨

Таким образом, каждой эквивалентности ε на множестве A соответствует разбиение $\pi(\varepsilon)$ этого множества, блоками которого являются ε-классы. Почти очевидна

ЛЕММА 2. Пусть π - разбиение множества A. Отношение "быть в одном π-блоке" является эквивалентностью на множестве A. ▨

Таким образом, каждому разбиению π множества A соответству-

ет эквивалентность $\varepsilon(\pi)$ на этом множестве, классами которой являются π-блоки.

ТЕОРЕМА I. Отображения $\varepsilon \longmapsto \pi(\varepsilon)$ и $\pi \longmapsto \varepsilon(\pi)$ устанавливают взаимно однозначное соответствие между эквивалентностями и разбиениями на данном множестве. При этом $\varepsilon(\pi(\varepsilon)) = \varepsilon$ и $\pi(\varepsilon(\pi)) = \pi$.

3. Множество всех эквивалентностей на множестве A упорядочивается теоретико-множественным включением. Если $\varepsilon_1 \subseteq \varepsilon_2$, то каждый ε_1-класс является частью подходящего ε_2-класса. Так что включение эквивалентностей трансформируется в следующее упорядочение разбиений: $\pi_1 \leqslant \pi_2$ означает, что каждый π_1-блок содержится в подходящем π_2-блоке. У-множества $(E(A), \subseteq)$ всех эквивалентностей на множестве A и $(\Pi(A), \leqslant)$ всех разбиений этого множества изоморфны.

П р и м е р. На трехэлементном множестве $A = \{1, 2, 3\}$ имеется пять разбиений: π_1 с блоками $[1]$, $[2]$, $[3]$; π_2 с блоками $[1,2]$, $[3]$; $\pi_3 = [1,3]$, $[2]$; $\pi_4 = [1],[2,3]$; $\pi_5 = [1,2,3]$. Упорядоченные указанным выше отношением $\leqslant$, эти разбиения образуют недистрибутивную решетку - ромб M_3 (рис. I3, а).

4. Понятно, что точной нижней гранью для двух эквивалентностей ε_1 и ε_2 будет их теоретико-множественное пересечение $\varepsilon_1 \cap \varepsilon_2$ (нужно просто проверить, что это тоже эквивалентность).

Покажем, что отношение

$$\varepsilon = \{(x,y) \in A \times A : (\exists k \in \mathbb{N})(\exists t_1, \ldots, t_k \in A)((x,t_1) \in \varepsilon_1 \& (t_1,t_2) \in \varepsilon_2 \& (t_2,t_3) \in \varepsilon_1 \& \ldots \& (t_k,y) \in \varepsilon_2)\}$$

является точной верхней гранью для ε_1 и ε_2. Действительно, из его определения, свойств ε_1 и ε_2 и соотношений

I) $(x,x) \in \varepsilon_1$;

2) $(x,u_1) \in \varepsilon_1 \& \ldots \& (u_m,y) \in \varepsilon_2 \& (y,v_1) \in \varepsilon_1 \& \ldots \& (v_n,z) \in \varepsilon_2 \Longrightarrow (x,z) \in \varepsilon$;

3) $(x,t_1) \in \varepsilon_1 \& \ldots \& (t_k,y) \in \varepsilon_2 \Longrightarrow (y,y) \in \varepsilon_1 \& (y,t_k) \in \varepsilon_2 \& \ldots \& (t_1,x) \in \varepsilon_1 \& (x,x) \in \varepsilon_2$

для ε вытекают соответственно рефлексивность, транзитивность и симметричность. Кроме того, если некоторая эквивалентность содержит ε_1 и ε_2, то она, конечно, содержит и ε. Таким образом, доказана

ТЕОРЕМА 2. У-множество $E(A)$ всех эквивалентностей на множестве A является решеткой. ▨

Вследствие теоремы I из §I главы I решеткой будет и у-множество $\Pi(A)$ всех разбиений множества A.

Известно, что любая конечная решетка изоморфна подходящей подрешетке решетки разбиений конечного множества (Пудлак и Тума [36]).

§2. Конгруэнции автомата. Алгоритм построения решетки конгруэнций автомата

I. Пусть $\mathcal{A}=(S,X,\delta)$ – некоторый автомат. Эквивалентность θ на множестве S называется конгруэнцией автомата $\mathcal{A}$, если она устойчива относительно функции переходов δ в том смысле, что

$$(\forall s_1,s_2\in S)(\forall x\in X)((s_1,s_2)\in\theta\Longrightarrow(\delta(s_1,x),\delta(s_2,x))\in\theta)$$

(т.е. если s_1 и s_2 находятся в одном θ-классе, то состояния, получаемые из них действием любого входного сигнала, тоже будут в одном θ-классе).

В любом автомате конгруэнциями будут тождественное отношение Δ и универсальное отношение $S\times S$.

Пример I. Состояния s_1, s_2 называются неразличимыми в автомате $\mathcal{A}=(S,X,\delta)$, если $\delta(s_1,x)=\delta(s_2,x)$ для любого входного сигнала $x\in X$. Отношение неразличимости очевидным образом является конгруэнцией автомата $\mathcal{A}$

Пример 2. Отношение $\theta=\{(s_1,s_2):\mathcal{A}(s_1)=\mathcal{A}(s_2)\}$ – всегда эквивалентность. Конгруэнцией оно будет в любом автономном автомате (отождествляются элементы каждого цикла), в общем случае устойчивости относительно функции переходов нет. Например, в автомате с тремя состояниями I, 2, 3 и двумя входными сигналами x_1, x_2 такими, что δ_1: $1\mapsto2\mapsto1$, $3\mapsto3$ и δ_2: $1\mapsto3\mapsto3$, $2\mapsto2$, будет $\mathcal{A}(1)=\mathcal{A}(2)$, но $\mathcal{A}(\delta(1,x_2))=\mathcal{A}(3)\neq\mathcal{A}(2)=\mathcal{A}(\delta(2,x_2))$.

2. Совокупность всех конгруэнций автомата $\mathcal{A}$ обозначим $\mathrm{Con}\mathcal{A}$. Так как теоретико-множественное пересечение $\theta_1\cap\theta_2$ двух конгруэнций снова является конгруэнцией и $S\times S$ – тоже конгруэнция, то, по теореме 2 (из §2 главы I), у-множество $(\mathrm{Con}\mathcal{A},\subseteq)$ – решетка.

ТЕОРЕМА. $(\mathrm{Con}\mathcal{A},\subseteq)$ является подрешеткой решетки $(E(S),\subseteq)$ всех эквивалентностей на множестве состояний автомата $\mathcal{A}$.

Доказательство. Так как $\mathrm{Con}\mathcal{A}\subseteq E(S)$ и операция пересечения в этих решетках одна и та же, остается проверить, что наименьшая эквивалентность θ, содержащая две данные конгруэнции θ_1, θ_2, сама будет конгруэнцией, т.е. что θ устойчива относительно функции переходов.

Пусть $\bar{s},\bar{\bar{s}}\in S$, $x\in X$. Тогда

$$(\bar{s},\bar{\bar{s}})\in\theta\Longrightarrow(\exists k\in\mathbb{N})(\exists t_1,\dots,t_k\in S)((\bar{s},t_1)\in\theta_1\,\&\,(t_1,t_2)\in\theta_2\,\&\dots\&\,(t_k,\bar{\bar{s}})\in\theta_2)\Longrightarrow$$

$$\Longrightarrow(\exists t_1,\dots,t_k\in S)((\delta(\bar{s},x),\delta(t_1,x))\in\theta_1\,\&\,(\delta(t_1,x),\delta(t_2,x))\in\theta_2\,\&\dots\&$$

$$\&\,((\delta(t_k,x),\delta(\bar{\bar{s}},x))\in\theta_2)\Longrightarrow(\delta(\bar{s},x),\delta(\bar{\bar{s}},x))\in\theta.$$ ▨

Для автономного автомата $\mathcal{A}$, в котором входной сигнал каждое состояние переводит в себя, будет $\mathrm{Con}\,\mathcal{A} = E(S)$. Но решетка $E(S)$ на трехэлементном множестве S не будет дистрибутивной (пример I, §I). Следовательно, решетка конгруэнций автомата не обязательно дистрибутивна.

3. Пусть s_1, s_2 – какие-нибудь различные состояния автомата $\mathcal{A}$. Через $\theta(s_1, s_2)$ обозначим наименьшую из конгруэнций, отождествляющих s_1 и s_2, т.е. $\theta(s_1,s_2) = \bigcap\{\theta : (s_1,s_2) \in \theta\}$. Конгруэнции вида $\theta(s_1,s_2)$ будем называть главными конгруэнциями автомата $\mathcal{A}$.

Любая конгруэнция θ автомата является объединением подходящего набора главных конгруэнций: $\theta = \bigvee\{\theta(s_1,s_2) : (s_1,s_2) \in \theta\}$.

Не все главные конгруэнции будут неразложимыми элементами решетки $\mathrm{Con}\,\mathcal{A}$. Например, в шестиэлементном цикле $1 \to 2 \to 3 \to 4 \to 5 \to 6 \to 1$ имеем: $\theta(1,2) = [1,2,3,4,5,6]$, $\theta(1,3) = [1,3,5][2,4,6]$, $\theta(1,4) = [1,4][2,5][3,6]$ и $\theta(1,2) = \theta(1,3) \vee \theta(1,4)$ (мы отождествляем конгруэнции и соответствующие им разбиения).

С другой стороны, всякая неразложимая конгруэнция, как нетрудно заметить, будет главной.

Полагая

$$\theta^*(s_1,s_2) = \begin{cases} \theta(s_1,s_2), & \text{если } \theta(s_1,s_2) \text{ является неразложимой;} \\ \Delta, & \text{в противном случае;} \end{cases}$$

получаем, что для любой $\theta \in \mathrm{Con}\,\mathcal{A}$ имеет место представление $\theta = \bigvee\{\theta^*(s_1,s_2) : (s_1,s_2) \in \theta\}$. Оно и лежит в основе алгоритма построения решетки конгруэнций автомата (Фарр [27]).

Диаграмма решетки $\mathrm{Con}\,\mathcal{A}$ строится снизу. Найдя все ее элементы, имеющие данную высоту h, берем их попарные объединения и затем определяем элементы высоты $h+1$. Следующее предложение гарантирует, что таким образом будут получены все элементы решетки $\mathrm{Con}\,\mathcal{A}$.

ЛЕММА. Всякий разложимый элемент конечной решетки $\mathcal{L}$ может быть представлен в виде объединения двух элементов одинаковой высоты.

Доказательство. Пусть $a = a_1 \vee a_2$, $a_1 \neq a \neq a_2$, $h(a_1) \neq h(a_2)$. В интервалах $[a_1, a)$ и $[a_2, a)$ выберем по одному максимальному элементу – соответственно a_1^* и a_2^*. Если $h(a_1^*) = h(a_2^*)$, то все в порядке, так как, конечно, $a_1^* \vee a_2^* = a$ и $a_1^* \neq a \neq a_2^*$. Пусть будет $h(a_1^*) < h(a_2^*)$. В интервале $[0, a_2^*)$ возьмем любой элемент a_2° такой, что $h(a_2^\circ) = h(a_1^*)$. Тогда $a = a_1^* \vee a_2^* \geqslant a_1^* \vee a_2^\circ > a_1^*$. Так как a является верхним соседом для a_1^*, должно быть $a_1^* \vee a_2^\circ = a$. ▨

Алгоритм построения решетки конгруэнций автомата состоит из следующих этапов.

Шаг I. На уровень $h=0$ записать элементы множества $R(0)=\{\Delta\}$.

Шаг 2. Найти множество $S(0)$ всех главных конгруэнций автомата.

Шаг 3. Положить $h=1$.

Шаг 4. Построить множество

$$\mathcal{Y}(h)=\begin{cases}\varnothing, & \text{если } R(h-1) \text{ одноэлементно;}\\ \text{попарное объединение элементов из } R(h-1) & \text{иначе.}\end{cases}$$

Шаг 5. Построить множество $S(h)=(S(h-1)\setminus R(h-1))\cup\mathcal{Y}(h)$.

Шаг 6. Выделить в $S(h)$ множество $R(h)$ минимальных элементов.

Шаг 7. Если $R(h)$ не пусто, записать элементы этого множества на уровень h и перейти в 4, полагая $h=h+1$.

Шаг 8. Если $R(h)$ пусто, работа алгоритма заканчивается.

После выполнения алгоритма все конгруэнции автомата (их удобно представлять в виде разбиений) распределятся в соответствии с их высотой в у-множестве $(Con\,\mathcal{A},\subseteq)$. Двигаясь снизу вверх, соединяем отрезком каждый элемент этого у-множества с его нижними соседями.

Эффективная программа построения решетки конгруэнций автомата была составлена (на языке Фортран) С.В.Камановым.

4. Очевидно, что эквивалентность θ на множестве S тогда и только тогда будет конгруэнцией автомата $\mathcal{A}=(S,X,\delta)$, когда она устойчива в каждой автономной компоненте автомата $\mathcal{A}$.

Пример 3. Пусть автомат $\mathcal{A}$ с множеством состояний $\{1,2,3,4\}$ и входным алфавитом $\{x_1,x_2\}$ задан таблицей переходов (табл. 6) и графами автономных компонент, изображенными на рис. I9, а, б.

Таблица 6

δ	x_1	x_2
I	2	I
2	3	2
3	3	2
4	4	3

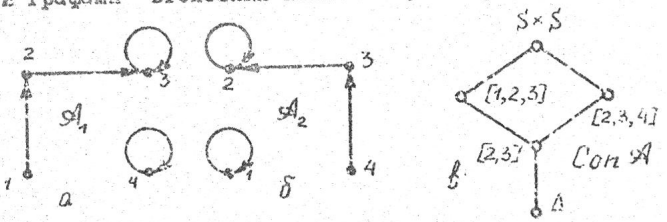


Рис. I9

Нетождественные конгруэнции $\mathcal{A}_1$-компоненты автомата $\mathcal{A}$ задаются следующими разбиениями (указываем только неодноэлементные блоки): $\theta_1=[2,3]$, $\theta_2=[3,4]$, $\theta_3=[1,2,3]$, $\theta_4=[2,3,4]$, $\theta_5=[1,2,3,4]$.

Аналогичный список для x_2-компоненты: θ_1, $\theta_2^*=[1,2]$, θ_3, θ_4, θ_5. Диаграмма решетки $Con\mathcal{A}$ представлена на рис. 19, в.

5. Пусть $\mathcal{A}=(S,X,\delta)$ – некоторый автомат и θ – конгруэнция на нем. Фактор-автоматом автомата $\mathcal{A}$ по конгруэнции θ называется автомат $\mathcal{A}/\theta=(S/\theta, X, \delta)$, где S/θ – множество классов конгруэнции θ, а $\delta: S/\theta\times X\to S/\theta$ определяется формулой $\delta(\theta(s),x)=\theta(\delta(s,x))$ для всех $s\in S$, $x\in X$. Поскольку все элементы θ-класса под действием входного сигнала переходят в один и тот же θ-класс, определение функции переходов автомата $\mathcal{A}/\theta$ не зависит от выбора конкретного s в соответствующем θ-классе.

Очевидно, что фактор-автомат $\mathcal{A}/\Delta$ изоморфен автомату $\mathcal{A}$, а фактор-автомат $\mathcal{A}/S\times S$ – одноэлементен.

ЗАДАЧА 5. Описать автоматы, у которых каждый фактор-автомат изоморфен подходящему подавтомату.

§3. Автоматы со специальными типами решетки конгруэнций

1. Следующее предложение неоднократно будет использоваться в дальнейшем. Оно представляет и самостоятельный интерес.

ТЕОРЕМА 1. Если граф автономного автомата $\mathcal{A}$ представляет собой цикл длины n, то решетка $Con\mathcal{A}$ антиизоморфна решетке делителей числа n.

Доказательство. Пусть $S=\{1,2,\dots,n\}$ и $\delta: 1\mapsto 2\mapsto\dots\mapsto n\mapsto 1$. Решетку делителей числа n обозначим через $\mathcal{L}(n)$ (в примере II из §1 главы I рассматривалась решетка $\mathcal{L}(30)$).

Определим отображение $\varphi: \mathcal{L}(n)\to Con\mathcal{A}: d\mapsto\theta_d$, где при $n=du$ конгруэнция θ_d имеет классы $[1,1+d,\dots,1+d(u-1)]$, $[2,2+d,\dots,2+d(u-1)]$, $\dots$, $[d,d+1,\dots,d+d(u-1)]$. Покажем, что θ_d в самом деле будет конгруэнцией автомата $\mathcal{A}$ для любого делителя d числа n.

Общий вид элементов в классе, содержащем состояние i, где $1\le i\le d$, есть $i+dk$, причем $0\le k\le u-1$. Если $i+dk=j+dl$, где $1\le j\le d$, $0\le l\le u-1$, то $i-j=(l-k)d$. Но $|i-j|<d$, так что $l=k$, откуда $i=j$, – различные классы не пересекаются.

Кроме того, каждое состояние содержится в некотором θ_d-классе: если $1\le s\le n$, то $s=i+dk$, где $1\le i\le d-1$, $0\le k\le u-1$, когда s делится с остатком i на d, и $s=d+dk$, где $1\le k\le u-1$, когда s делится без остатка на d, – так что s имеет вид $i+dk$ при подходящих i и k, где $1\le i\le d$, $0\le k\le u-1$.

Это означает, что состояние s находится в классе $\theta_d(i)$.

Таким образом, θ_d – эквивалентность. Ее устойчивость относительно функции переходов очевидна: при $i<d$ состояния класса $\theta_d(i)$ переходят в класс $\theta_d(i+1)$, а при $i=d$ – из класса $\theta_d(d)$ – в класс $\theta_d(1)$.

Отображение φ взаимно однозначно. Действительно, пусть будет $n=du$, $n=tv$. Конгруэнция θ_d имеет d классов, а конгруэнция θ_t имеет t классов. Если $\theta_d=\varphi(d)=\varphi(t)=\theta_t$, то сразу $d=t$.

Будет ли φ отображением на, т.е. любая ли конгруэнция автомата $\mathcal{A}$ имеет вид θ_d для подходящего делителя d числа n? Пусть $\theta\in Con\mathcal{A}$. Понятно, что $\Delta=\theta_n$, $S\times S=\theta_1$, так что θ будем считать собственной нетождественной конгруэнцией. Расположим состояния, входящие в некоторый неодноэлементный θ-класс, в соответствии с их естественной нумерацией: $i_1<i_2<\dots$. Положим $d=i_2-i_1$. Тогда i_1+1, i_1+2, $\dots$, $i_1+(d-1)$ не лежат в классе $\theta(i_1)$, а значит, и i_2+1, i_2+2, $\dots$, $i_2+(d-1)$ не лежат в этом классе. Но $(i_2,i_3)\in\theta$, откуда $i_3=i_2+d$. Теперь видим, что наш θ-класс состоит из состояний i_1, i_1+d, i_1+2d, $\dots$, последнее из которых $i_1+d\bar{u}$ таково, что $(i_1+d\bar{u})+d=n+i_1$, откуда $n=d(\bar{u}+1)=du$. Итак, $n=du$ и рассматриваемый θ-класс имеет вид $[i_1, i_1+d, \dots, i_1+d(u-1)]$. Действуя на содержащиеся в нем состояния входным сигналом, получим и остальные θ-классы: все они содержат по d элементов, и значит, $\theta=\theta_d$.

Теперь нужно проверить справедливость соотношения $d\mid t\Leftrightarrow\varphi(d)\supseteq\varphi(t)$ для любых различных делителей d, t числа n.

Пусть $n=du=tv$, $t=dw$. Тогда $n=tv=d(vw)$, откуда получаем $vw=u$. Общий вид элементов θ_t-класса таков: $i+tk$, где $1\le i\le t$, $0\le k\le v-1$. Представим $i=j+dl$, где $1\le j\le d$, $0\le l\le w-1$. Тогда $i+tk=j+dl+(dw)k=j+d(l+wk)$, где $1\le j\le d$ и $0\le l+wk\le w-1+w(v-1)=wv-1=u-1$. Следовательно, состояние $i+tk$ находится в θ_d-классе, содержащем состояние j. Таким образом, при $d\mid t$ будет $\varphi(t)=\theta_t\subset\theta_d=\varphi(d)$.

С другой стороны, пусть $\varphi(t)\subset\varphi(d)$, т.е. $\theta_t\subset\theta_d$. Каждый θ_d-класс имеет u элементов и разбивается на θ_t-классы, каждый из которых содержит v элементов. Следовательно, u делится на v. Если $u=vw$, то $tv=n=du=d(vw)=(dw)v$, откуда $t=dw$, т.е. $d\mid t$. Решетки $\mathcal{L}(n)$ и $Con\mathcal{A}$ антиизоморфны. ☐

Представленное в теореме I описание решетки конгруэнций цикла получил Берман [22].

2. Автомат $\mathcal{A}$, имеющий больше одного состояния, называется простым, если у него нет конгруэнций, отличных от тождественной и универсальной, т.е. если решетка $Con\,\mathcal{A}$ двухэлементна.

ТЕОРЕМА 2. Простой автомат с не менее чем тремя состояниями содержит самое большее один собственный подавтомат, причем этот подавтомат имеет точно одно состояние.

Доказательство. Пусть $\mathcal{A}=(S, X, \delta)$ – простой автомат, $|S| \geqslant 3$ и $\mathcal{A}^*$ – собственный подавтомат в $\mathcal{A}$. Если множество состояний S^* подавтомата $\mathcal{A}^*$ содержит более одного элемента, то отношение $\theta^* = (S^* \times S^*) \cup \Delta_S$ будет, как нетрудно заметить, отличной от Δ и $S \times S$ конгруэнцией автомата $\mathcal{A}$. Следовательно, каждый собственный подавтомат в $\mathcal{A}$ имеет точно одно состояние.

Пусть $\mathcal{A}_1$ и $\mathcal{A}_2$ – различные подавтоматы в $\mathcal{A}$. Так как по доказанному $|S_1|=|S_2|=1$, то $|S_1 \cup S_2| < S$, так что подавтомат $\mathcal{A}^* = \mathcal{A}_1 \vee \mathcal{A}_2$ будет собственным подавтоматом автомата $\mathcal{A}$, содержащим два состояния, что, как мы видели, невозможно.

СЛЕДСТВИЕ. Автономный автомат тогда и только тогда является простым, когда I) он имеет два состояния или 2) граф его переходов представляет собой цикл простой длины.

Доказательство. Необходимость. Из теоремы 2 получается, что простой автономный автомат с $\geqslant 3$ состояниями может быть только циклом. По теореме I длина этого цикла должна быть простым числом.

Достаточность. Понятно, что любой автомат с двумя состояниями будет простым. Если граф автономного автомата $\mathcal{A}$ – цикл простой длины, то по теореме I решетка $Con\,\mathcal{A}$ двухэлементна.

ЗАДАЧА 6. Описать простые автоматы.

3. Как мы увидим впоследствии (§4), важную роль играют автоматы, у которых решетка конгруэнций имеет единственный атом.

Следующий результат получил Йоели [38].

ТЕОРЕМА 3. Следующие графы, и только они, представляют автономные автоматы с одноатомной решеткой конгруэнций:

1) петля с одним простым хвостом;

2) цикл, длина которого равна степени простого числа;

3) две петли;

4) цикл, длина которого равна степени простого числа, с присоединенной петлей.

Доказательство. Необходимость. Пусть решетка $Con\mathcal{A}$ конгруэнций автономного автомата $\mathcal{A}$ имеет единственный атом. Тогда пересечение любых двух нетождественных конгруэнций автомата $\mathcal{A}$ тоже будет нетождественной конгруэнцией.

I. Пусть граф переходов автомата $\mathcal{A}$ связен. Могут представиться два случая.

1) Единственный цикл графа одноэлементен (петля). Предположим, что существуют различные нециклические состояния s_1, s_2 такие, что $\delta(s_1)=s_0=\delta(s_2)$. Если s_0 – циклическое состояние, то главные конгруэнции $\theta(s_0,s_1)$ и $\theta(s_0,s_2)$ имеют тождественное пересечение. Если s_0 – нециклическое состояние, то тождественное пересечение имеют главные конгруэнции $\theta(s_1,s_2)$ и $\theta(s_0,\delta(s_0))$. Следовательно, для любых двух различных нециклических состояний s_1, s_2 будет $\delta(s_1)\neq\delta(s_2)$, – граф представляет собой петлю с одним простым хвостом.

2) Цикл графа переходов автомата $\mathcal{A}$ неодноэлементен. Если s_1 – нециклическое состояние, а s_2 – циклическое и при этом $\delta(s_1)=s_0=\delta(s_2)$, то главные конгруэнции $\theta(s_1,s_2)$ и $\theta(s_0,s_2)$ имеют тождественное пересечение. Следовательно, автомат $\mathcal{A}$ имеет пустое множество нециклических состояний, и его граф представляет собой цикл. Предположим, что длина цикла n не является степенью простого числа. Тогда n можно представить в виде произведения двух взаимно простых чисел: $n=pq$, причем $p\neq 1\neq q$. В решетке $\mathcal{L}(n)$ делителей числа n будет $p\vee q=HOK(p,q)=n$, и значит, в дуально изоморфной ей решетке $Con\mathcal{A}$ получим $\theta_p\cap\theta_q=\Delta$. Следовательно, длина цикла не разложима в произведение двух взаимно простых чисел, т.е. является степенью простого числа.

II. Пусть граф автомата $\mathcal{A}$ не связен.

Предположим, что в графе больше двух циклов. Если среди них есть два неодноэлементных, то для конгруэнций θ_1 и θ_2, первая из которых имеет единственным неодноэлементным классом один цикл, а вторая – другой, имеем: $\theta_1\cap\theta_2=\Delta$. Если неодноэлементный цикл только один, то конгруэнции θ_1 и θ_2, первая из которых отождествляет элементы этого цикла, а вторая – два одноэлементных цикла, имеют тождественное пересечение. Если, наконец, все циклы одноэлементны, то, выбрав три из них, построим конгруэнции θ_{12} и θ_{23}: первая отождествляет элементы первого и второго, а вторая – второго и третьего циклов. Понятно, что $\theta_{12}\cap\theta_{23}=\Delta$.

Итак, граф переходов автомата $\mathcal{A}$ имеет в точности два цикла причем один из них обязательно одноэлементен.

3) Пусть и второй цикл одноэлементен. Тогда и одна из двух компонент связности графа не может иметь больше одного элемента: если s_1 и s_2 циклические состояния, а $\delta(s_3)=s_1$, $s_3 \neq s_1$, то $\theta(s_1,s_2)\cap\theta(s_1,s_3)=\Delta$. Следовательно, граф состоит из двух петель.

4) Один из циклов содержит не менее двух элементов. Тогда, согласно 2), он должен иметь длину p^α, где p – простое число.

Достаточность. Пусть автономный автомат $\mathcal{A}$ принадлежит одному из типов I)–4). Покажем, что решетка $Con\mathcal{A}$ имеет только один атом. В случае 3) это очевидно, случай 4) сводится к случаю 2): неуниверсальные конгруэнции автомата типа 4) выделяют петлю в отдельный класс.

I) Допустим, что автомат $\mathcal{A}$ имеет состояния $0, I, \ldots, n$ и его функция переходов действует следующим образом: $n \mapsto n-1 \mapsto \ldots$ $\ldots \mapsto I \mapsto 0 \mapsto 0$. Если $n=1$, т.е. $\mathcal{A}$ имеет всего два состояния, то $Con\mathcal{A}$ двухэлементна.

Пусть $n>1$. Так как в автомате $\mathcal{A}$ имеется собственный двухэлементный подавтомат (с состояниями 0 и I), согласно теореме 2, $\mathcal{A}$ имеет и собственные нетождественные конгруэнции. Пусть θ – любая из них. Если $(i,j)\in\theta$, $i<j$, то $(\delta^i(i),0)\in\theta$, и значит, состояние 0 входит в неодноэлементный θ-класс. Пусть K – наибольшее (как число) состояние в классе $\theta(0)$. Тогда $K-1=\delta(K)\in\theta(0)$, $K-2=\delta(K-1)\in\theta(0)$ и т.д. – в классе $\theta(0)$ находятся все состояния $0, I, \ldots, K$.

Таким образом, каждая нетождественная конгруэнция автомата $\mathcal{A}$ имеет единственный неодноэлементный класс, и этот класс будет устойчивым подмножеством в $\mathcal{A}$. Устойчивые подмножества автомата $\mathcal{A}$ согласно теореме 6 (из §2 главы I) образуют цепь. В таком случае и решетка $Con\mathcal{A}$ будет цепью.

2) Пусть граф переходов автомата $\mathcal{A}$ является циклом длины $n=p^\alpha$, где p – простое число. Тогда решетка $\mathcal{L}(n)$ делителей числа n представляет собой цепь $1|p|p^2|\ldots|p^\alpha$. По теореме I цепью будет и решетка $Con\mathcal{A}$.

СЛЕДСТВИЕ. Решетка конгруэнций автономного автомата тогда и только тогда будет одноатомной, когда она – цепь. ▨

Что в общем случае это не так, показывает автомат, рассмотренный в примере 3 (§2).

ЗАДАЧА 7. Описать автоматы, у которых решетка конгруэнций является цепью.

(Автоматы можно классифицировать по свойствам решетки конгруэн-

ций. Автономные автоматы $\mathcal{A}$, у которых решетка $Con\mathcal{A}$ обладает дополнениями, описали Л.А.Скорняков и Д.П.Егорова [6], а свойства, равносильные модулярности или дистрибутивности решетки $Con\mathcal{A}$, для них нашла Д.П.Егорова [5]).

4. Пусть $\mathcal{A}=(S,X,\delta)$ – некоторый автомат. Рассмотрим отображение $Sub\mathcal{A}\to Con\mathcal{A}$: $\mathcal{A}^*\mapsto\theta^*=(S^*\times S^*)\cup\Delta$, где S^* – множество состояний подавтомата $\mathcal{A}^*$.

ТЕОРЕМА 4. Соответствие $\mathcal{A}^*\mapsto\theta^*$

1) взаимно однозначно тогда и только тогда, когда в $\mathcal{A}$ нет подавтоматов с одним состоянием;

2) является $\wedge$-гомоморфизмом решетки $Sub\mathcal{A}$ в решетку $Con\mathcal{A}$;

3) будет $\vee$-гомоморфизмом решетки $Sub\mathcal{A}$ в решетку $Con\mathcal{A}$ тогда и только тогда, когда $\mathcal{A}$ – связный автомат.

Доказательство. 1) Понятно, что если $\mathcal{A}_1$ и $\mathcal{A}_2$ – подавтоматы, имеющие более одного состояния, то $\theta_1^*\neq\theta_2^*$. В то же время для любого подавтомата $\mathcal{A}^*$ с одним состоянием $\theta^*=\Delta$, так же как и для нулевого подавтомата $\mathcal{O}$.

2) Это утверждение следует из очевидного равенства

$$(S_1\cap S_2)\times(S_1\cap S_2)=(S_1\times S_1)\cap(S_2\times S_2).$$

3) Необходимость. Пусть соответствие $\mathcal{A}^*\mapsto\theta^*$ сохраняет операцию объединения, но автомат $\mathcal{A}$ не является связным. Согласно теореме 4§I.2,в решетке $Sub\mathcal{A}$ найдутся два различных атома: $\mathcal{A}_1$ и $\mathcal{A}_2$. Тогда для $\mathcal{A}^*=\mathcal{A}_1\vee\mathcal{A}_2$ будет $\theta^*=((S_1\cup S_2)^2)\cup\Delta$. С другой стороны, поскольку $S_1\cap S_2=\varnothing$, получаем, что $\theta^*=\theta_1^*\cup\theta_2^*=(S_1\times S_1)\cup(S_2\times S_2)\cup\Delta$. Но при $S_1\cap S_2=\varnothing$, как нетрудно заметить, $(S_1\cup S_2)\times(S_1\cup S_2)\neq(S_1\times S_1)\cup(S_2\times S_2)$. Противоречие.

Достаточность. Если автомат $\mathcal{A}$ связен, то любые два его непустые устойчивые подмножества S_1 и S_2 имеют непустое пересечение. Тогда $\theta_1^*\vee\theta_2^*=((S_1\times S_1)\cup\Delta)\vee((S_2\times S_2)\cup\Delta)=((S_1\cup S_2)\times(S_1\cup S_2))\cup\Delta$, – в силу транзитивности. Отсюда получаем, что соответствие $\mathcal{A}^*\mapsto\theta^*$ является $\vee$-гомоморфизмом решетки $Sub\mathcal{A}$ в решетку $Con\mathcal{A}$.

ЗАДАЧА 8. Описать автоматы $\mathcal{A}$, для которых соответствие $\mathcal{A}^*\mapsto\theta^*$ отображает $Sub\mathcal{A}$ на $Con\mathcal{A}$ (т.е. все конгруэнции автомата $\mathcal{A}$ определяются его подавтоматами).

§4. Конечные решетки как решетки конгруэнций автоматов

I. Через Θ_n обозначим класс решеток, изоморфных решеткам конгруэнций автоматов с n входными сигналами. Очевидно, что

если $m \le n$, то $\Theta_m \subseteq \Theta_n$ (решетка конгруэнций автомата $\mathcal{A}$ с m входными сигналами $x_1, x_2, \ldots, x_m$ изоморфна решетке конгруэнций автомата с тем же множеством состояний и n входными сигналами $x_1, x_2, \ldots, x_m, x_{m+1}, \ldots, x_n$, если $x_m, x_{m+1}, \ldots, x_n$ все действуют одинаково).

Пусть Θ и Λ соответственно будут класс решеток, изоморфных решеткам конгруэнций произвольных автоматов, и класс всех конечных решеток. Понятно, что $\Theta = \bigcup_{i=1}^{\infty} \Theta_i$.

Непосредственно из определений получаем:

$$\Theta_1 \subseteq \Theta_2 \subseteq \Theta_3 \subseteq \Theta_4 \subseteq \ldots \subseteq \Theta \subseteq \Lambda.$$

2. Пример 3§2) и следствие из теоремы 3§3) показывают, что на самом деле имеет место строгое включение $\Theta_1 \subset \Theta_2$ (в указанном примере представлен автомат с двумя входными сигналами, решетка конгруэнций которого не может быть реализована как решетка конгруэнций автономного автомата).

Следующий замечательный результат устанавливает равенство $\Theta = \Theta_4$.

ТЕОРЕМА. Для всякого автомата существует автомат с четырьмя входными сигналами, имеющий такую же решетку конгруэнций.

Доказательство. Пусть $\mathcal{A} = (S, X, \delta)$, где $S = \{s_1, s_2, \ldots, s_n\}$ и $X = \{x_1, x_2, \ldots, x_m\}$, $m > 4$.

Построим автомат $\mathcal{B} = (\Gamma, \{y_1, y_2, y_3, y_4\}, \delta)$ следующим образом. Положим $\Gamma = S^{m+n+1}$ и для $t = (s^1, s^2, \ldots, s^{m+n+1})$ определим:

$$\delta(t, y_1) = (s_1, s_2, \ldots, s_n, \delta(s^1, x_1), \ldots, \delta(s^1, x_m), s^1),$$

$$\delta(t, y_2) = (s^2, s^3, s^4, \ldots, s^{m+n+1}),$$

$$\delta(t, y_3) = (s^{m+n+1}, s^1, s^2, \ldots, s^{m+n}),$$

$$\delta(t, y_4) = (s^2, s^1, s^3, s^4, \ldots, s^{m+n+1}).$$

Далее, для $\theta \in \mathrm{Con}\,\mathcal{A}$ введем в множестве Γ отношение $\bar{\theta} = \{(t, {}^*t) : (s^i, {}^*s^i) \in \theta, 1 \le i \le m+n+1\}$, где ${}^*t = ({}^*s^1, {}^*s^2, \ldots, {}^*s^{m+n+1})$.

Из этого определения сразу следует, что $\theta \subseteq \psi \Leftrightarrow \bar{\theta} \subseteq \bar{\psi}$. В частности, $\theta = \bar{\psi}$ тогда и только тогда, когда $\theta = \psi$.

I) Докажем, что $\bar{\theta}$ является конгруэнцией автомата $\mathcal{B}$.

Нужно проверить, что при $j = 1, 2, 3, 4$ из $(t, {}^*t) \in \bar{\theta}$ следует $(\delta(t, y_j), \delta({}^*t, y_j)) \in \bar{\theta}$.

Для $j = 2, 3, 4$ это вполне очевидно. Рассмотрим случай $j = 1$.

Пусть $(t,{}^*t)\in\bar\theta$. Тогда $(s^i,{}^*s^i)\in\theta$, $1\le i\le m+n+1$. В автомате $\mathcal{B}$ будет:

$$\delta(t,y_1)=(s_1,s_2,\dots,s_n,\delta(s^1,x_1),\dots,\delta(s^1,x_m),s^1),$$

$$\delta({}^*t,y_1)=(s_1,s_2,\dots,s_n,\delta({}^*s^1,x_1),\dots,\delta({}^*s^1,x_m),{}^*s^1).$$

Так как $\theta\in\operatorname{Con}\mathcal{A}$, то $(\delta(s^1,x_j),\delta({}^*s^1,x_j))\in\theta$, $1\le j\le m$, откуда $(\delta(t,y_1),\delta({}^*t,y_1))\in\bar\theta$.

Таким образом, соответствие $\theta\mapsto\bar\theta$ отображает решетку $\operatorname{Con}\mathcal{A}$ в решетку $\operatorname{Con}\mathcal{B}$.

2) Покажем, что $\theta\mapsto\bar\theta$ отображает $\operatorname{Con}\mathcal{A}$ на $\operatorname{Con}\mathcal{B}$.

Для $\Psi\in\operatorname{Con}\mathcal{B}$ положим

$$\theta_\Psi=\{(s,{}^*s)\in S\times S:(\underbrace{s,s_2\dots,s}_{m+n+1},\underbrace{{}^*s,{}^*s\dots,{}^*s}_{m+n+1})\in\Psi\}.$$

а) Отношение θ_Ψ будет конгруэнцией автомата $\mathcal{A}$. Действительно, если $(s,{}^*s)\in\theta_\Psi$, то $((s,s,\dots,s),({}^*s,{}^*s,\dots,{}^*s))\in\Psi$. Подавая на вход автомата $\mathcal{B}$ сигнал y_1 и учитывая, что $\Psi\in\operatorname{Con}\mathcal{B}$, получаем, что $((s_1,\dots,s_n,\delta(s,x_1),\dots,\delta(s,x_m),s),(s_1,\dots,s_n,\delta({}^*s,x_1),\dots,\delta({}^*s,x_m),{}^*s))\in\Psi$.

Используя входное слово $\underbrace{y_3\,y_3\dots y_3}_{m+2}$, приходим к соотношению

$$((s_1,\delta(s,x_1),\dots,\delta(s,x_m),s,s_1,\dots,s_{n-1}),(s_1,\delta({}^*s,x_1),\dots,\delta({}^*s,x_m),{}^*s,s_1,\dots,s_{n-1}))\in\Psi.$$

Наконец, входное слово $\underbrace{y_2(y_3y_2)\dots(y_3y_2)}_{n}$ дает

$$((\underbrace{\delta(s,x_1),\dots,\delta(s,x_1)}_{m+n+1}),(\underbrace{\delta({}^*s,x_1),\dots,\delta({}^*s,x_1)}_{m+n+1}))\in\Psi,$$

откуда $(\delta(s,x_1),\delta({}^*s,x_1))\in\theta_\Psi$. Аналогично доказывается, что для всех $k\ge2$ выполняется $(\delta(s,x_k),\delta({}^*s,x_k))\in\theta_\Psi$.

б) $\Psi\subseteq\bar\theta_\Psi$. В самом деле, если $(t,{}^*t)\in\Psi$, то, подавая на вход автомата $\mathcal{B}$ слово $\underbrace{(y_3y_2)\dots(y_3y_2)}_{m+n}$, получаем $((s^1,s^1,\dots,s^1),({}^*s^1,{}^*s^1,\dots,{}^*s^1))\in\Psi$, откуда $(s^1,{}^*s^1)\in\theta_\Psi$. Входная последовательность $\underbrace{y_4(y_3y_2)\dots(y_3y_2)}_{m+n}$ приведет к установлению того, что $(s^2,{}^*s^2)\in\theta_\Psi$. И так для любого $i\le m+n+1$ можно подобрать входную последовательность, приводящую t в состояние $(s^i,s^i,\dots,s^i)\in T$. Следовательно, $(s^i,{}^*s^i)\in\theta_\Psi$ для всех i. Значит, $(s,{}^*s)\in\bar\theta_\Psi$.

в) Для доказательства включения $\bar\theta_\Psi\subseteq\Psi$ потребуется

ЛЕММА. Пусть τ, ${}^*\tau$ – два состояния автомата $\mathcal{B}$, причем $\sigma^i=s^i$, ${}^*\sigma^i={}^*s^i$ для некоторого фиксированного i и $\sigma^j={}^*\sigma^j$ для всех $j\ne i$. Тогда из $(t,{}^*t)\in\Psi$ вытекает, что $(\tau,{}^*\tau)\in\Psi$.

(Рассмотрим случай $i=1$. Тогда $\tau=(s^1,\sigma^2,\dots,\sigma^{m+n+1})$ и ${}^*\tau=({}^*s^1,\sigma^2,\dots,\sigma^{m+n+1})$. Так как $(t,{}^*t)\in\Psi$, то отношение Ψ будет

содержать и пару

$$(\delta(t,y_3),\delta(^*t,y_4))=((s_1,\dots,s_n,\delta(s^1,x_1),\dots,\delta(s^1,x_m),s^1),(s_1,\dots,s_n,\delta(^*s^1,x_1),\dots,\delta(^*s^1,x_m),{}^*s^1).$$

Поскольку каждая из двух этих $(m+n+1)$-систем содержит все состояния автомата $\mathcal{A}$, с помощью входных сигналов y_2, y_3, y_4 из пары $(\delta(t,y_3),\delta(^*t,y_4))$ можно получить пару $(\tau,{}^*\tau)$. При этом получающиеся на каждом шаге состояния автомата $\mathcal{B}$ будут Ψ-конгруэнтными. Значит, $(\tau,{}^*\tau)\in\Psi$.

Если $i=2$, будем подавать на вход автомата $\mathcal{B}$ сигнал y_3 до тех пор, пока из $(t,{}^*t)\in\Psi$ не получим, что $((s^2,s^3,\dots,s^{m+n+1},s^1),({}^*s^2,{}^*s^3,\dots,{}^*s^{m+n+1},{}^*s^2))\in\Psi$, после чего повторим проведенные для $i=1$ рассуждения.)

Пусть теперь $(t,{}^*t)\in\overline{\theta}_\Psi$. Тогда $(s^i,{}^*s^i)\in\theta_\Psi$ для любого i, и значит, $((s^i,\dots,s^i),({}^*s^i,\dots,{}^*s^i))\in\Psi$. Полагая $i=1$ и пользуясь леммой, получим, что $((s^1,s^2,\dots,s^{m+n+1}),({}^*s^1,s^2,\dots,s^{m+n+1}))\in\Psi$. При $i=2$ лемма дает соотношение $((^*s^1,s^2,s^3,\dots,s^{m+n+1}),({}^*s^1,{}^*s^2,s^3,\dots,s^{m+n+1}))\in\Psi$. Вследствие транзитивности $((s^1,s^2,s^3,\dots,s^{m+n+1}),({}^*s^1,{}^*s^2,s^3,\dots,s^{m+n+1}))\in\Psi$. Полагая $i=3$ и применяя лемму, ставим во второй $(m+n+1)$-систе ме третью звездочку и т.д. Следовательно, $(t,{}^*t)\in\Psi$.

Из б) и в) получаем равенство $\overline{\theta}_\Psi=\Psi$.

Таким образом, соответствие $\theta\mapsto\overline{\theta}$ является изоморфизмом упорядоченных множеств $(Con\,\mathcal{A},\subseteq)$ и $(Con\,\mathcal{B},\subseteq)$. ▨

Доказанная теорема принадлежит Маккензи (см. Йонссон [35, теорема 4.7.2]).

3. Учитывая полученные результаты, имеем:

$$\Theta_1\subset\Theta_2\subseteq\Theta_3\subseteq\Theta_4=\Theta\subseteq\Lambda.$$

ЗАДАЧА 9. Верно ли, что $\Theta=\Lambda$, т.е. что каждая конечная решетка изоморфна решетке конгруэнций подходящего автомата?

ЗАДАЧА 10. Верно ли, что $\Theta=\Theta_2$, т.е. что для любого автомата существует автомат с двумя входными сигналами, имеющий такую же решетку конгруэнций?

(С.Р.Когаловский и В.В.Солдатова [10] показали, что для любого автомата $\mathcal{A}$ существует автомат $\mathcal{B}$ с двумя входными сигналами такой, что решетка $Con\,\mathcal{B}$ получается из $Con\,\mathcal{A}$ добавлением сверху одного элемента.)

§5. Конгруэнции и разложение автоматов

1. Прямым произведением автоматов $\mathcal{A}=(S,X,\delta)$ и $\mathcal{B}=(T,X,\delta)$ называется автомат $\mathcal{A}\times\mathcal{B}=(S\times T,X,\delta)$, функция переходов которого

$\delta : (S\times T)\times X \to S\times T$ действует следующим образом: $\delta((s,t),x) = (\delta(s,x),\delta(t,x))$ для любых $s\in S$, $t\in T$, $x\in X$ (три буквы δ в этой формуле обозначают функции переходов трех разных автоматов!).

ЗАДАЧА II. Каким условиям должны удовлетворять автоматы $\mathcal{A}$ и $\mathcal{B}$, чтобы прямое произведение $\mathcal{A}\times\mathcal{B}$ было сильно связным?

Будем говорить, что автомат $\mathcal{C}$ разложим в прямое произведение, если существует изоморфизм $\mathcal{C}\cong\mathcal{A}\times\mathcal{B}$ при подходящих автоматах $\mathcal{A}$ и $\mathcal{B}$, ни один из которых не изоморфен автомату $\mathcal{C}$.

Две конгруэнции θ_1, θ_2 автомата $\mathcal{A}$ называются перестановочными, если $\theta_2\circ\theta_1 = \theta_1\circ\theta_2$, где, по определению,

$$\psi\circ\theta = \{(s_1,s_2): (\exists s)((s_1,s)\in\theta \;\&\; (s,s_2)\in\psi)\}$$

(обычное умножение отношений, сомножители пишутся справа налево).

ТЕОРЕМА I. Автомат тогда и только тогда разлагается в прямое произведение, когда в нем существуют две перестановочные конгруэнции, пересечение которых совпадает с тождественной, а объединение – с универсальной конгруэнцией.

Доказательство. Необходимость. Покажем, что в автомате $\mathcal{A}\times\mathcal{B}$ конгруэнции $\theta_1 = \{((s_1,t_1),(s_2,t_2)): s_1 = s_2\}$ и $\theta_2 = \{((s_1,t_1),(s_2,t_2)): t_1 = t_2\}$ удовлетворяют условиям теоремы.

Действительно,

$$\theta_1\cap\theta_2 = \{((s_1,t_1),(s_2,t_2)): s_1 = s_2 \;\&\; t_1 = t_2\} = \Delta.$$

Пусть (s_1,t_1), (s_2,t_2) – произвольные состояния автомата $\mathcal{A}\times\mathcal{B}$. Тогда $((s_1,t_1),(s_1,t_2))\in\theta_1$ и $((s_1,t_2),(s_2,t_2))\in\theta_2$, и значит, вследствие транзитивности объединения конгруэнций, $((s_1,t_1),(s_2,t_2))\in\theta_1\vee\theta_2$. Следовательно, $\theta_1\vee\theta_2$ – универсальная конгруэнция.

Добавляя еще соотношения $((s_1,t_1),(s_2,t_1))\in\theta_2$ и $((s_2,t_1),(s_2,t_2))\in\theta_1$ получаем, что произведения $\theta_2\circ\theta_1$ и $\theta_1\circ\theta_2$ оба совпадают с объединением $\theta_1\vee\theta_2$, т.е. θ_1 и θ_2 перестановочны.

Достаточность. Пусть в автомате $\mathcal{C} = (U,X,\delta)$ существуют перестановочные конгруэнции θ_1 и θ_2 такие, что $\theta_1\cap\theta_2 = \Delta$ и одновременно $\theta_1\vee\theta_2 = U\times U$. Построим факторавтоматы $\mathcal{C}/\theta_1 = (S,X,\delta) = \mathcal{A}$ и $\mathcal{C}/\theta_2 = (T,X,\delta) = \mathcal{B}$, где $S = U/\theta_1$, $T = U/\theta_2$, причем для всех $u\in U$, $x\in X$ имеют место равенства $\delta(\theta_1(u),x) = \theta_1(\delta(u,x))$ и $\delta(\theta_2(u),x) = \theta_2(\delta(u,x))$.

Покажем, что автомат $\mathcal{C}$ изоморфен прямому произведению автоматов $\mathcal{A}$ и $\mathcal{B}$.

Рассмотрим отображение $\varphi : U \to S\times T$, определяемое формулой $\varphi(u) = (\theta_1(u),\theta_2(u))$.

Если $\varphi(\bar{u}) = \varphi(\bar{\bar{u}})$, то $\theta_1(\bar{u}) = \theta_1(\bar{\bar{u}})$ и $\theta_2(\bar{u}) = \theta_2(\bar{\bar{u}})$, т.е. $(\bar{u}, \bar{\bar{u}}) \in \theta_1 \cap \theta_2 = \Delta$, и значит, $\bar{u} = \bar{\bar{u}}$, - отображение φ взаимно однозначно.

Пусть $\theta_1(\bar{u})$, $\theta_2(\bar{\bar{u}})$ - произвольные классы соответствующих конгруэнций. Так как $\theta_1 \vee \theta_2$ - универсальная конгруэнция, то найдутся $u_1, u_2, \ldots, u_k \in U$ такие, что $(\bar{u}, u_1) \in \theta_1, (u_1, u_2) \in \theta_2, \ldots, (u_k, \bar{\bar{u}}) \in \theta_2$. В силу перестановочности θ_1 и θ_2 можно построить цепочку той же длины, имеющую вид $(\bar{u}, \tilde{u}_1) \in \theta_1, (\tilde{u}_1, \tilde{u}_2) \in \theta_2, \ldots, (\tilde{u}_{\ell-1}, \tilde{u}_\ell) \in \theta_1, (\tilde{u}_\ell, \tilde{u}_{\ell+1}) \in \theta_2, \ldots, (\tilde{u}_k, \bar{\bar{u}}) \in \theta_2$. Но тогда $(\bar{u}, \tilde{u}_\ell) \in \theta_1$ и $(\tilde{u}_\ell, \bar{\bar{u}}) \in \theta_2$, т.е. $\theta_1(\bar{u}) = \theta_1(\tilde{u}_\ell)$ и $\theta_2(\bar{\bar{u}}) = \theta_2(\tilde{u}_\ell)$. По определению, $(\theta_1(\bar{u}), \theta_2(\bar{\bar{u}})) = \varphi(\tilde{u}_\ell)$. Таким образом, φ отображает U на $S \times T$.

Наконец, если $u \in U$ и $x \in X$ - произвольные состояние и входной сигнал автомата $\mathcal{C}$, то $\varphi(\delta(u,x)) = (\theta_1(\delta(u,x)), \theta_2(\delta(u,x))) = (\delta'(\theta_1(u), x), \delta(\theta_2(u), x)) = \delta((\theta_1(u), \theta_2(u)), x) = \delta(\varphi(u), x)$.

Автоматы $\mathcal{C}$ и $\mathcal{A} \times \mathcal{B}$ изоморфны.

2. Свойство перестановочности конгруэнций и, следовательно, разложимость автомата в прямое произведение не выражается в терминах решетки $\mathrm{Con}\,\mathcal{A}$. Это показывает следующий

Пример 1. Пусть $S = \{1, 2, 3, 4, 5, 6\}$. Полагая δ_1: $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 1$, $6 \mapsto 1$, получаем автономный автомат $\mathcal{A}_1 = (S, \delta_1)$, у которого две конгруэнции: $\theta_{11} = [5,6]$ и $\theta_{12} = [1,2,3,4,5]$. При этом $\theta_{12} \cap \theta_{11} = \Delta$ и $\theta_{12} \vee \theta_{11} = S \times S$. Однако $\theta_{12} \circ \theta_{11} \neq \theta_{11} \circ \theta_{12}$, поскольку, например, $(6,1) \in \theta_{12} \circ \theta_{11}$, так как $(6,5) \in \theta_{11}$ и $(5,1) \in \theta_{12}$, но $(6,1) \notin \theta_{11} \circ \theta_{12}$ (если $(6,s) \in \theta_{12}$ и $(s,1) \in \theta_{11}$, то $s = 1$, откуда $(6,1) \in \theta_{12}$ - противоречие). Значит, автомат $\mathcal{A}_1$ не разложим в прямое произведение.

Определим теперь δ_2: $1 \mapsto \_ \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 6 \mapsto 1$. Граф автомата $\mathcal{A}_2 = (S, \delta_2)$ представляет собой шестиэлементный цикл, так что $\mathrm{Con}\,\mathcal{A}_2 = \{\Delta, S \times S, \theta_{21}, \theta_{22}\}$, где $\theta_{21} = [1,3,5]$, $[2,4,6]$ и $\theta_{22} = [1,4]$, $[2,5]$, $[3,6]$. Таким образом, $\mathrm{Con}\,\mathcal{A}_1 \cong \mathrm{Con}\,\mathcal{A}_2$. Но автомат $\mathcal{A}_2$ можно разложить в прямое произведение циклов $s_1 \mapsto s_2 \mapsto s_1$ и $t_1 \mapsto t_2 \mapsto t_3 \mapsto t_1$: разложение осуществляется соответствием $1 \leftrightarrow (s_1, t_1)$, $2 \leftrightarrow (s_2, t_2)$, $3 \leftrightarrow (s_1, t_3)$, $4 \leftrightarrow (s_2, t_1)$, $5 \leftrightarrow (s_1, t_2)$, $6 \leftrightarrow (s_2, t_3)$.

3. Следующая конструкция, как увидим, имеет уже чисто решеточный характер.

Подпрямым произведением автоматов $\mathcal{A} = (S, X, \delta)$ и $\mathcal{B} = (T, X, \delta)$ называется собственный подавтомат $\mathcal{C}^* = (U, X, \delta)$ прямого произве-

дения $\mathcal{A}\times\mathcal{B}$ такой, что

$$\pi_1(U)=\{s\in S:(\exists t\in T)((s,t)\in U)\}=S,$$

$$\pi_2(U)=\{t\in T:(\exists s\in S)((s,t)\in U)\}=T.$$

Подпрямое произведение двух данных автоматов определяется не однозначно: в автомате $\mathcal{A}\times\mathcal{B}$ может быть несколько подавтоматов, удовлетворяющих вышеуказанным условиям.

Будем говорить, что автомат $\mathcal{C}$ разложим в подпрямое произведение автоматов $\mathcal{A}$ и $\mathcal{B}$, если существует изоморфизм между автоматом $\mathcal{C}$ и подходящим подпрямым произведением автоматов $\mathcal{A}$ и $\mathcal{B}$.

Пример 2. Пусть автономный автомат $\mathcal{A}$ имеет пять состояний: s_1, s_2, s_3, s_4, s_5, которые образуют в этом порядке цикл, а автономный автомат $\mathcal{B}$ содержит два состояния – t_1, t_2, и при этом $t_1 \longmapsto t_2 \longmapsto t_2$. В прямом произведении $\mathcal{A}\times\mathcal{B}$ выделим состояния $(s_1,t_2), (s_2,t_2), (s_3,t_2), (s_4,t_2), (s_5,t_2), (s_5,t_1)$. Они образуют устойчивое подмножество:

$$(s_1,t_2)\longmapsto(s_2,t_2)\longmapsto(s_3,t_2)\longmapsto(s_4,t_2)\longmapsto(s_5,t_2)\longmapsto(s_1,t_2),\ (s_5,t_1)\longmapsto(s_1,t_2).$$

Очевидно, что определяемый этим подмножеством автомат $\mathcal{A}^*$ является подпрямым произведением автоматов $\mathcal{A}$ и $\mathcal{B}$. Соответствие $(s_i,t_2)\leftrightarrow i$, $i=\overline{1,5}$, $(s_5,t_1)\leftrightarrow 6$ является изоморфизмом автомата $\mathcal{A}^*$ на автомат $\mathcal{A}_1$ из примера I. Следовательно, автомат $\mathcal{A}_1$ разложим в подпрямое произведение автоматов $\mathcal{A}$ и $\mathcal{B}$.

ТЕОРЕМА 2. Автомат тогда и только тогда разлагается в подпрямое произведение, когда он имеет нетождественные конгруэнции θ_1 и θ_2 такие, что $\theta_1\cap\theta_2=\Delta$.

Доказательство. Необходимость. Пусть $\mathcal{C}=(U,X,\delta)$ – подпрямое произведение автоматов $\mathcal{A}=(S,X,\delta)$ и $\mathcal{B}=(T,X,\delta)$. На множестве $U\subseteq S\times T$ рассмотрим отношения

$$\theta_1=\{((s_1,t_1),(s_2,t_2)):s_1=s_2\},$$

$$\theta_2=\{((s_1,t_1),(s_2,t_2)):t_1=t_2\}.$$

Очевидно, что θ_1 и θ_2 – конгруэнции автомата $\mathcal{C}$. При этом если $((s_1,t_1),(s_2,t_2))\in\theta_1\cap\theta_2$, то $s_1=s_2$ и $t_1=t_2$, и значит, $\theta_1\cap\theta_2=\Delta$.

Достаточность. Пусть автомат $\mathcal{C}=(U,X,\delta)$ имеет нетождественные конгруэнции θ_1 и θ_2 такие, что $\theta_1\cap\theta_2=\Delta$. Построим фактор-

автоматы $\mathcal{A}=\mathcal{C}/\theta_1=(U/\theta_1, X, \delta)$ и $\mathcal{B}=\mathcal{C}/\theta_2=(U/\theta_2, X, \delta)$ и рассмотрим их прямое произведение $\mathcal{A}\times\mathcal{B}$. Состояниями автомата $\mathcal{A}\times\mathcal{B}$ будут всевозможные пары $(\theta_1(\bar{u}), \theta_2(\bar{\bar{u}}))$, где $\bar{u}, \bar{\bar{u}} \in U$, а функция переходов определяется правилом

$$\delta((\theta_1(\bar{u}), \theta_2(\bar{\bar{u}})), x) = (\delta(\theta_1(\bar{u}), x), \delta(\theta_2(\bar{\bar{u}}), x)) = (\theta_1(\delta(\bar{u}, x)), \theta_2(\delta(\bar{\bar{u}}, x))).$$

Так как θ_1 и θ_2 – конгруэнции на $\mathcal{C}$, то написанные соотношения не зависят от выбора конкретных представителей $\bar{u}$, $\bar{\bar{u}}$ в соответствующих классах эквивалентности.

Подмножество

$$V = \{(\theta_1(\bar{u}), \theta_2(\bar{\bar{u}})) : \bar{u} = \bar{\bar{u}}\},$$

как нетрудно понять, устойчиво в автомате $\mathcal{A}\times\mathcal{B}$ и, следовательно, определяет в $\mathcal{A}\times\mathcal{B}$ некоторый подавтомат $\mathcal{D}$. При этом, конечно, $\pi_1(V) = U/\theta_1$ и $\pi_2(V) = U/\theta_2$. Так что $\mathcal{D}$ – подпрямое произведение автоматов $\mathcal{A}$ и $\mathcal{B}$.

Покажем, что автоматы $\mathcal{C}$ и $\mathcal{D}$ изоморфны. Пусть $\varphi : U \to V$: $u \mapsto (\theta_1(u), \theta_2(u))$. Понятно, что φ отображает U на V. Далее, если $\varphi(\bar{u}) = \varphi(\bar{\bar{u}})$, то $\theta_1(\bar{u}) = \theta_1(\bar{\bar{u}})$ и $\theta_2(\bar{u}) = \theta_2(\bar{\bar{u}})$, откуда $(\bar{u}, \bar{\bar{u}}) \in \theta_1 \cap \theta_2 = \Delta$, и значит, $\bar{u} = \bar{\bar{u}}$. Следовательно, φ – взаимно однозначное соответствие.

Если, наконец, $u \in U$ и $x \in X$ – произвольные состояние и входной сигнал автомата $\mathcal{C}$, то

$$\varphi(\delta(u, x)) = (\theta_1(\delta(u, x)), \theta_2(\delta(u, x))) = (\delta(\theta_1(u), x), \delta(\theta_2(u), x)) =$$

$$= \delta((\theta_1(u), \theta_2(u)), x) = \delta(\varphi(u), x).$$

Мы доказали, что φ – изоморфизм автоматов $\mathcal{C}$ и $\mathcal{D}$.

4. Автомат, не разложимый в подпрямое произведение, называется подпрямо неразложимым. Из теоремы 2 вытекает

СЛЕДСТВИЕ. Автомат подпрямо неразложим тогда и только тогда, когда решетка его конгруэнций является одноатомной. ▨

Таким образом, теорема 3(§3) характеризует подпрямо неразложимые автономные автоматы.

ЗАДАЧА I2. Описать подпрямо неразложимые автоматы.

В связи с этой задачей отметим один интересный частный результат (Имрэх [34]). Автомат $\mathcal{A}=(S, X, \delta)$ называется определенным, если существует натуральное число n такое, что любое входное слово, имеющее длину $\geqslant n$, все состояния автомата переводит в некоторое определенное (для данного слова) состояние.

ТЕОРЕМА 3. Определенный автомат $\mathcal{A}=(S,X,\delta)$ подпрямо неразложим тогда и только тогда, когда он имеет два различных состояния s_0 и s_0^* такие, что 1) $\delta(s_0,x)=\delta(s_0^*,x)$ для любого $x\in X$; 2) если s_1 и s_2 – различные состояния и $\{s_1,s_2\}\neq\{s_0,s_0^*\}$, то $\delta(s_1,x)\neq\delta(s_2,x)$ для некоторого $x\in X$.

Доказательство. Необходимость. Пусть $\mathcal{A}=(S,X,\delta)$ – подпрямо неразложимый определенный автомат. Через $P_2(S)$ обозначим множество всех двухэлементных подмножеств в S. Положим $\{s_1,s_2\}\leqslant\{s_3,s_4\}$, если существует входное слово p такое, что выполняется равенство $\{\delta(s_1,p),\delta(s_2,p)\}=\{s_3,s_4\}$. Это отношение рефлексивно (p – пустое слово) и транзитивно (если p_1 переводит $\{s_1,s_2\}$ в $\{s_3,s_4\}$, а p_2 переводит $\{s_3,s_4\}$ в $\{s_5,s_6\}$, то p_1p_2 переведет $\{s_1,s_2\}$ в $\{s_5,s_6\}$). Докажем, что $\leqslant$ – антисимметричное отношение. В самом деле, если для $\{s_1,s_2\}$, $\{s_3,s_4\}\in P_2(S)$ найдутся непустые слова p_1 и p_2 такие, что p_1 переводит $\{s_1,s_2\}$ в $\{s_3,s_4\}$, а p_2 переводит $\{s_3,s_4\}$ в $\{s_1,s_2\}$, то $\{\delta(s_1,p_1p_2),\delta(s_2,p_1p_2)\}=\{s_1,s_2\}$. Следовательно, существуют слова сколь угодно большой длины, переводящие $\{s_1,s_2\}$ в себя. Вследствие определенности автомата $\mathcal{A}$ это невозможно ($s_1\neq s_2$), и значит, $\{s_1,s_2\}=\{s_3,s_4\}$.

Итак, $\leqslant$ является отношением порядка на множестве $P_2(S)$. Покажем, что в у-множестве $(P_2(S),\leqslant)$ есть наибольший элемент. Так как $P_2(S)$ конечно, оно имеет максимальные элементы. Пусть $\{s_1,s_2\}$, $\{s_3,s_4\}$ – различные максимальные элементы в этом у-множестве. Тогда $\delta(s_1,x)=\delta(s_2,x)$ и $\delta(s_3,x)=\delta(s_4,x)$ для любого $x\in X$. В самом деле, допустив, например, что $\delta(s_1,x)\neq\delta(s_2,x)$ для некоторого $x\in X$, мы получили бы в силу максимальности элемента $\{s_1,s_2\}$ в у-множестве $(P_2,\leqslant)$ равенство $\{\delta(s_1,x),\delta(s_2,x)\}=\{s_1,s_2\}$, которое сохранялось бы при повторной подаче на вход сигнала x. В силу определенности автомата это невозможно.

Теперь рассмотрим на $\mathcal{A}$ две конгруэнции: $\theta(s_1,s_2)$ и $\theta(s_3,s_4)$. Очевидно, что их пересечение совпадает с Δ, а это противоречит подпрямой неразложимости автомата $\mathcal{A}$ (теорема 2).

Мы доказали, что в у-множестве $(P_2,\leqslant)$ есть наибольший элемент. Обозначив его через $\{s_0,s_0^*\}$, и получаем выполнимость условий 1) и 2) в автомате $\mathcal{A}$.

Достаточность. Пусть в определенном автомате $\mathcal{A}$ выполняются условия 1) и 2). Так же, как при доказательстве необходимости, введем порядок на множестве $P_2(S)$ всех двухэлементных подмножеств множества S. Тогда $\{s_0,s_0^*\}$ будет наибольшим элементом в этом у-множестве. Покажем, что конгруэнция $\theta(s_0,s_0^*)$

будет наименьшей из нетождественных конгруэнций автомата $\mathcal{A}$. В самом деле, пусть θ – произвольная нетождественная конгруэнция на $\mathcal{A}$. Возьмем какие-нибудь различные θ-конгруэнтные состояния $s_1, s_2 \in S$. Так как $\{s_0, s_0^*\}$ – наибольший элемент в упорядоченном множестве $(P_2(S), \leq)$, то $\{s_1, s_2\} < \{s_0, s_0^*\}$, и значит, найдется непустое слово p такое, что $\{\delta(s_1, p), \delta(s_2, p)\} = \{s_0, s_0^*\}$. Но тогда $(s_0, s_0^*) \in \theta$, откуда $\theta(s_0, s_0^*) \leq \theta$.

Таким образом, решетка $\mathrm{Con}\,\mathcal{A}$ имеет единственный атом,– по теореме 2 автомат $\mathcal{A}$ подпрямо неразложим. ▨

Автомат $\mathcal{A} = (S, X, \delta)$ называется коммутативным, если для любых $s \in S$, $x_1, x_2 \in X$ выполняется равенство $\delta(s, x_1 x_2) = \delta(s, x_2 x_1)$. Эшби и Имрех [26] описали подпрямо неразложимые коммутативные автоматы.

Глава III. МОНОИД ЭНДОМОРФИЗМОВ И ГРУППА АВТОМОРФИЗМОВ АВТОМАТА

§1. Гомоморфизмы и конгруэнции автомата

1. Отображение $\varphi : S \to T$ называется гомоморфизмом автомата $\mathcal{A} = (S, X, \delta)$ в автомат $\mathcal{B} = (T, X, \delta)$ с тем же множеством входных сигналов X, если

$$(\forall s \in S)(\forall x \in X)(\varphi(\delta(s, x)) = \delta(\varphi(s), x)).$$

Будем писать также $\varphi : \mathcal{A} \to \mathcal{B}$.

Если упомянутое отображение φ взаимно однозначно, оно называется вложением автомата $\mathcal{A}$ в автомат $\mathcal{B}$.

Понятно, что взаимно однозначный гомоморфизм автомата $\mathcal{A}$ на автомат $\mathcal{B}$ будет изоморфизмом.

Если автомат $\mathcal{A}$ допускает гомоморфизм на автомат $\mathcal{B}$, то $\mathcal{B}$ называют гомоморфным образом автомата $\mathcal{A}$.

Ядром отображения $\varphi : S \to T$, по определению, является отношение $\mathrm{Ker}\,\varphi = \{(s_1, s_2) \in S \times S : \varphi(s_1) = \varphi(s_2)\}$.

Очевидно, что ядро любого отображения будет эквивалентностью на множестве S.

Пусть θ – эквивалентность на множестве S. Отображение $\mathrm{nat}\,\theta : S \to S/\theta : s \mapsto \theta(s)$ множества S на фактор-множество S/θ называется естественным отображением для θ.

ТЕОРЕМА 1. Ядро всякого гомоморфизма автоматов является конгруэнцией. Обратно, всякая конгруэнция автомата представляет собой ядро некоторого его гомоморфизма.

Доказательство. I) Пусть $\varphi : \mathcal{A} \to \mathcal{B}$ – гомоморфизм, $s_1, s_2 \in S$, $x \in X$. Тогда $(s_1, s_2) \in \operatorname{Ker}\varphi \Longrightarrow \varphi(s_1) = \varphi(s_2) \Longrightarrow \varphi(\delta(s_1, x)) = \delta(\varphi(s_1), x) =$
$= \delta(\varphi(s_2), x) = \varphi(\delta(s_2, x)) \Longrightarrow (\delta(s_1, x), \delta(s_2, x)) \in \operatorname{Ker}\varphi$.

Итак, $\operatorname{Ker}\varphi \in \operatorname{Con}\mathcal{A}$.

2) Пусть θ – конгруэнция автомата $\mathcal{A}$. Нужно найти автомат $\mathcal{B}$ и гомоморфизм $\varphi : \mathcal{A} \to \mathcal{B}$ так, чтобы было $\operatorname{Ker}\varphi = \theta$.

Возьмем в качестве $\mathcal{B}$ фактор-автомат $\mathcal{A}/\theta$, а в качестве φ – естественное отображение $\operatorname{nat}\theta : S \to S/\theta$. Для любых $s \in S$, $x \in X$ имеем (звездочка отмечает действие в автомате $\mathcal{A}/\theta$ – см. пункт 4 из §2 главы II):

$$(\operatorname{nat}\theta)(\delta(s,x)) = \theta(\delta(s,x)) \overset{*}{=} \delta(\theta(s), x) = \delta((\operatorname{nat}\theta)(s), x),$$

так что $\operatorname{nat}\theta$ – гомоморфизм.

Далее, $\operatorname{Ker}\operatorname{nat}\theta = \{(s_1, s_2) \in S \times S : (\operatorname{nat}\theta)(s_1) = (\operatorname{nat}\theta)(s_2)\} =$
$= \{(s_1, s_2) \in S \times S : \theta(s_1) = \theta(s_2)\} = \{(s_1, s_2) \in S \times S : (s_1, s_2) \in \theta\} = \theta$.

▨

2. Следующая вариация алгебраической теоремы о гомоморфизмах показывает, что гомоморфные образы автомата с точностью до изоморфизма совпадают с его фактор-автоматами.

ТЕОРЕМА 2. Если φ – гомоморфизм автомата $\mathcal{A}$ на автомат $\mathcal{B}$, то автоматы $\mathcal{B}$ и $\mathcal{A}/\operatorname{Ker}\varphi$ изоморфны.

Доказательство. По теореме I $\operatorname{Ker}\varphi$ – конгруэнция автомата $\mathcal{A}$. Состояниями фактор-автомата $\mathcal{A}/\theta$ будут $\operatorname{Ker}\varphi$-классы $(\operatorname{Ker}\varphi)(s)$. Изоморфизмом автомата $\mathcal{A}/\operatorname{Ker}\varphi$ на автомат $\mathcal{B}$ является отображение $\psi : S/\operatorname{Ker}\varphi \xrightarrow{\text{на}} T : (\operatorname{Ker}\varphi)(s) \mapsto \varphi(s)$. Действительно, это отображение взаимно однозначно:

$$\psi((\operatorname{Ker}\varphi)(s_1)) = \psi((\operatorname{Ker}\varphi)(s_2)) \Longrightarrow \varphi(s_1) = \varphi(s_2) \Longrightarrow (s_1, s_2) \in \operatorname{Ker}\varphi \Longrightarrow$$
$$\Longrightarrow (\operatorname{Ker}\varphi)(s_1) = (\operatorname{Ker}\varphi)(s_2).$$

Далее, ψ сохраняет функцию переходов:

$$\psi(\delta((\operatorname{Ker}\varphi)(s), x)) = \psi((\operatorname{Ker}\varphi)(\delta(s, x))) = \varphi(\delta(s, x)) = \delta(\varphi(s), x) =$$
$$= \delta(\psi((\operatorname{Ker}\varphi)(s)), x).$$

Теорема доказана.

§2. Моноиды и преобразования

I. Алгебра $(A, \cdot, e)$ с одной бинарной и одной нульарной операциями называется моноидом, если эти операции удовлетворяют следую-

щим тождествам: I) $(xy)z = x(yz)$ (ассоциативность), 2) $xe = ex = x$ (нейтральность элемента e).

Бинарная операция называется в общем случае умножением, а элемент e – нейтральным элементом моноида.

Пример I. $(\mathbb{N}, \cdot, 1)$ – натуральные числа с обычным умножением и числом 1 в качестве нейтрального элемента.

Пример 2. $(\mathbb{Z}, +, 0)$ – целые числа со сложением и числом 0 в качестве нейтрального элемента.

Пример 3. $(\mathbb{M}_n, \cdot, E)$ – множество всех $(n \times n)$– матриц с умножением и единичной $(n \times n)$–матрицей E.

Пример 4. $(P(S), \cup, \varnothing)$ – множество всех подмножеств множества S с объединением и пустым подмножеством.

2. Преобразованием непустого множества S называется отображение $\varphi : S \to S$ множества S в себя. Множество всех преобразований множества S обозначим через $\mathcal{F}(S)$.

ТЕОРЕМА I. Множество $\mathcal{F}(S)$ всех преобразований множества S образует относительно суперпозиции преобразований моноид, нейтральным элементом которого является тождественное преобразование Δ.

Доказательство. Пусть φ, ψ, χ – преобразования множества S. Для любого $s \in S$ имеем:

$$(\chi \circ (\psi \circ \varphi))(s) = \chi((\psi \circ \varphi)(s)) = \chi(\psi(\varphi(s))) = (\chi \circ \psi)(\varphi(s)) = ((\chi \circ \psi) \circ \varphi)(s).$$

Отсюда получаем равенство $\chi \circ (\psi \circ \varphi) = (\chi \circ \psi) \circ \varphi$, – суперпозиция преобразований ассоциативна.

Совсем просто доказывается нейтральность тождественного преобразования Δ:

$$(\forall s \in S)((\Delta \circ \varphi)(s) = \Delta(\varphi(s)) = \varphi(s)) \Longrightarrow \Delta \circ \varphi = \varphi$$

и аналогично $\varphi \circ \Delta = \varphi$. ▨

Моноид $(\mathcal{F}(S), \circ, \Delta)$ называется симметрическим моноидом на множестве S.

3. Пусть $A = (A, \cdot, e)$ и $B = (B, *, \epsilon)$ – два моноида. Отображение $f : A \to B$ называется гомоморфизмом моноида A в моноид B, если I) $f(xy) = f(x) * f(y)$ для любых $x, y \in A$; 2) $f(e) = \epsilon$.

Взаимно однозначный гомоморфизм называется вложением, а взаимно однозначный гомоморфизм моноида A на моноид B – изоморфизмом.

ТЕОРЕМА 2. Каждый моноид вкладывается в подходящий симметрический моноид.

Доказательство. Пусть $\mathbb{A}=(A,\cdot,e)$ – некоторый моноид. Определим отображение $f: A \to \mathcal{F}(A): a \mapsto \lambda_a$, где $\lambda_a(x)=xa$ для любого $x \in A$. Преобразования вида λ_a, $a \in A$, называются правыми сдвигами моноида $\mathbb{A}$.

1) Отображение f взаимно однозначно:

$$\lambda_a=\lambda_b \Rightarrow (\forall x\in A)(\lambda_a(x)=\lambda_b(x)) \overset{x=e}{\Longrightarrow} a=ea=\lambda_a(e)=\lambda_b(e)=eb=b.$$

Итак, из $a \neq b$ следует $\lambda_a \neq \lambda_b$.

2) f сохраняет умножение:

$$\lambda_{ab}(x)=x(ab)=(xa)b=\lambda_b(\lambda_a(x))=(\lambda_b\circ\lambda_a)(x),\ \forall x\in A,$$

так что $f(ab)=\lambda_{ab}=\lambda_b\circ\lambda_a=f(b)\circ f(a)$ (суперпозиция преобразований пишется справа налево!).

3) f-образом нейтрального элемента e является тождественное преобразование Δ:

$$\lambda_e(x)=xe=x=\Delta(x),\ \forall x\in A,$$

и значит, $f(e)=\lambda_e=\Delta$.

Таким образом, моноид $(A,\cdot,e)$ вложен в симметрический моноид $(\mathcal{F}(A),\circ,\Delta)$.

4. Алгебра $(A,\cdot,^{-},e)$ с одной бинарной, одной унарной и одной нульарной операциями называется группой, если эти операции удовлетворяют следующим тождествам: 1) $(xy)z=x(yz)$ (ассоциативность), 2) $xe=ex=x$ (нейтральность элемента e), 3) $x\bar{x}=\bar{x}x=e$ (обратимость).

Из этого определения следует, что группа – это моноид с дополнительной операцией $^{-}$, называемой обращением. Элемент $\bar{x}$ называется обратным для x.

Пример 5. $(\mathbb{R}^*,\cdot,^{-1},1)$ – множество отличных от нуля действительных чисел с обычными умножением и обращением и числом 1 в качестве нейтрального элемента.

Пример 6. $(\mathbb{Z},+,-,0)$ – целые числа с обычными сложением, противоположением и нулем.

Пример 7. $(\mathbb{M}_n^*,\cdot,^{-1},E)$ – невырожденные $(n\times n)$-матрицы с умножением, обращением и единичной $(n\times n)$-матрицей.

Пример 8. $(\mathbb{Z}_n,+_n,-_n,0)$ – остатки от деления целых чисел на натуральное число $n>1$ со сложением по модулю n, противоположением $-_n x=n-x$, нулем.

Пример 9. $(\mathcal{P}(S),+,\Delta,\varnothing)$ – множество всех подмножеств непустого множества S с симметрической разностью подмножеств

$X+Y=(X\cap\bar{Y})\cup(\bar{X}\cap Y)$, тождественной операцией $\Delta(X)=X$ и пустым подмножеством.

5. Множество всех взаимно однозначных отображений множества S на себя обозначим через $K(S)$.

Пусть $\varphi\in K(S)$. Каждому элементу $s\in S$ соотнесем единственный его φ-прообраз: $s\mapsto t$, где $\varphi(t)=s$. Тем самым определено преобразование множества S, которое называется обратным для φ преобразованием и обозначается φ^{-1}. Из этого определения сразу следует, что $\varphi^{-1}\in K(S)$ и что $(\varphi^{-1})^{-1}=\varphi$.

Элементы множества $K(S)$ называются обратимыми преобразованиями множества S.

ТЕОРЕМА 3. Пусть φ - преобразование конечного множества S. Следующие утверждения равносильны: 1) φ отображает S на S, 2) φ взаимно однозначно, 3) φ обратимо.

Доказательство. Каждому преобразованию φ n-элементного множества S можно сопоставить граф. Элементы множества S являются вершинами этого графа и, если элемент x имеет своим φ-образом элемент y (т.е. если $\varphi(x)=y$), из вершины x в вершину y рисуем стрелку. Полученный граф имеет точно n вершин и точно n стрелок. При этом из каждой вершины исходит ровно одна стрелка.

1 $\Longrightarrow$ 2. Пусть φ отображает S на S. Если φ не взаимно однозначно, то в графе, представляющем φ, имеется вершина, в которую приходят как минимум две стрелки. Но тогда можно отыскать вершину, из которой не выйдет ни одна стрелка,- противоречие.

2 $\Longrightarrow$ 1. Если φ взаимно однозначно, то в каждую вершину приходит самое большее одна стрелка. Это означает, что n стрелок графа имеют точно n различных концов. Следовательно, в каждую вершину графа приходит стрелка,- φ отображает S на S.

3 $\Longleftrightarrow$ 1 & 2. Обратимые преобразования множества S взаимно однозначны и отображают S на S.

ТЕОРЕМА 4. Множество $K(S)$ всех обратимых преобразований множества S образует относительно суперпозиции и обращения группу, нейтральным элементом которой является тождественное преобразование Δ.

Доказательство. Множество $K(S)$ замкнуто относительно суперпозиции, так как $(\psi\circ\varphi)^{-1}=\varphi^{-1}\circ\psi^{-1}$ для любых $\varphi,\psi\in K(S)$. Следовательно, по теореме 1 $(K(S),\circ,\Delta)$ - моноид. При этом для любого $s\in S$ будет $(\varphi^{-1}\circ\varphi)(s)=\varphi^{-1}(\varphi(s))=s=\varphi(\varphi^{-1}(s))=(\varphi\circ\varphi^{-1})(s)$,

откуда получаем равенства $\varphi^{-1}\circ\varphi = \varphi\circ\varphi^{-1} = \Delta$. Следовательно, все групповые тождества выполнены.

Группа $(K(S), \circ, ^{-1}, \Delta)$ называется симметрической группой на множестве S .

6. Теперь с помощью теоремы 2 устанавливается еще один важный факт.

ТЕОРЕМА 5. Каждая группа вкладывается в подходящую симметрическую группу.

Доказательство. Сначала напомним, что под вложением одной группы в другую понимается взаимно однозначное отображение, сохраняющее все три групповые операции.

Пусть $(A, \cdot, ^{-}, e)$ - группа. По теореме 2 моноид $(A, \cdot, e)$ вкладывается в моноид $(\mathcal{F}(A), \circ, \Delta)$ всех преобразований множества A . Это вложение осуществляется соответствием $a \mapsto \lambda_a$, где $\lambda_a : A \to A : x \mapsto xa$.

Однако, если наш моноид является группой, тогда все его правые сдвиги λ_a представляют собой обратимые преобразования множества A . Действительно, для любого $a \in A$ имеем:

$$\lambda_a(x) = \lambda_a(y) \Longrightarrow xa = ya \Longrightarrow x = xe = x(a\bar{a}) = (xa)\bar{a} =$$
$$= (ya)\bar{a} = y(a\bar{a}) = ye = y,$$

т.е. λ_a взаимно однозначно.

Далее,

$$x = xe = x(\bar{a}a) = (x\bar{a})a = \lambda_a(x\bar{a}),$$

и значит, λ_a отображает A на A .

Наконец,

$$(\lambda_{\bar{a}}\circ\lambda_a)(x) = (xa)\bar{a} = x = \Delta(x) = x = (x\bar{a})a = (\lambda_a\circ\lambda_{\bar{a}})(x),$$

так что $\lambda_{\bar{a}} = (\lambda_a)^{-1}$, - вложение моноида $(A, \cdot, e)$ в моноид $(\mathcal{F}(A), \circ, \Delta)$ сохраняет и обращение. Таким образом, группа $(A, \cdot, ^{-}, e)$ вложена в симметрическую группу $(K(A), \circ, ^{-1}, \Delta)$.

7. Пусть A - группа. Для произвольного элемента $a \in A$ определим $a^0 = e$, $a^n = \underbrace{a\cdot a\cdot\ldots\cdot a}_{n}$ (если $n > 0$). Очевидна справедливость следующих свойств возведения в степень: $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

Конечная группа называется циклической, если она состоит из различных степеней одного элемента. Говорят, что этот элемент порождает группу.

Число элементов конечной группы называется ее порядком.

ТЕОРЕМА 6. Конечная циклическая группа порядка n изоморфна аддитивной группе остатков от деления на n.

Доказательство. Аддитивная (т.е. когда бинарная операция обозначается знаком "+", унарная знаком "−", а нульарная символом "0") группа остатков от деления целых чисел на число n была введена в примере 8.

Пусть $A=\{e,a,a^2,\dots,a^{n-1}\}$. Рассмотрим соответствие $\varphi: a^i \mapsto i$. Это отображение множества A на множество $\mathbb{Z}_n$ взаимно однозначно. Кроме того, $\varphi(e)=\varphi(a^0)=0$.

Далее имеем:

$$a^i a^k = \left\{ \begin{array}{ll} a^{i+k}, & \text{если } i+k<n; \\ a^{(i+k)-n}, & \text{если } i+k \geq n \end{array} \right\} = a^{i+_n k},$$

так что $\varphi(a^i a^k)=\varphi(a^{i+_n k})=i+_n k=\varphi(a^i)+_n \varphi(a^k)$.

Наконец, $(a^i)^{-1}=a^{n-i}$, откуда $\varphi((a^i)^{-1})=\varphi(a^{n-i})=n-i=$ $=-_n i=-_n \varphi(a^i)$.

Отображение φ сохраняет все три групповые операции, и значит, является изоморфизмом. ▨

Пусть $A=\{e,a,a^2,\dots,a^{n-1}\}$ – циклическая группа порядка n. Если d – собственный делитель числа n, например, $n=md$, где $0<m<n$, то подмножество $A^*=\{e,a^d,a^{2d},\dots,a^{(m-1)d}\}$ оказывается замкнутым относительно всех трех операций группы A, и следовательно, само является группой – подгруппой группы A. Действительно, $a^{id}a^{kd}=a^{id+_n kd}=a^{(i+_m k)d}\in A^*$,

$(a^{id})^{-1}=a^{n-id}=a^{md-id}=a^{(m-i)d}\in A^*$, $e=a^0=a^{0d}\in A^*$.

§3. Некоторые свойства моноида эндоморфизмов автомата

1. Эндоморфизмами автомата называют его гомоморфизмы в себя. Множество всех эндоморфизмов автомата $\mathcal{A}$ обозначается $\mathrm{End}\,\mathcal{A}$.

ТЕОРЕМА 1. Множество $\mathrm{End}\,\mathcal{A}$ образует относительно суперпозиции моноид, нейтральным элементом которого является тождественное преобразование Δ.

Доказательство. На основании теоремы 1(§2) достаточно показать, что множество $\mathrm{End}\,\mathcal{A}$ замкнуто относительно суперпозиции преобразований и что $\Delta\in\mathrm{End}\,\mathcal{A}$. Пусть $\varphi,\psi\in\mathrm{End}\,\mathcal{A}$. Учитывая, что φ и ψ – эндоморфизмы автомата $\mathcal{A}$, получаем:

$$(\psi\circ\varphi)(\delta(s,x))=\psi(\varphi(\delta(s,x)))=\psi(\delta(\varphi(s),x))=\delta(\psi(\varphi(s)),x)=\delta((\psi\circ\varphi)(s),x),$$

так что $\psi\circ\varphi\in\mathrm{End}\,\mathcal{A}$.

Очевидные соотношения $\Delta(\delta(s,x)) = \delta(s,x) = \delta(\Delta(s),x)$ показывают, что $\Delta \in End\mathcal{A}$.

Моноид $End\mathcal{A}$ называется моноидом эндоморфизмов автомата $\mathcal{A}$.

2. Обращение доказанной теоремы является

ТЕОРЕМА 2. Каждый конечный моноид изоморфен моноиду эндоморфизмов подходящего автомата.

Доказательство. Пусть $\mathbb{M} = (S, \cdot, e)$ – конечный моноид. Рассмотрим автомат $\mathcal{A} = (S, S, \delta)$, где $\delta : S \times S \to S : (s,x) \mapsto xs$. Таким образом, носитель S моноида $\mathbb{M}$ является одновременно и множеством состояний и входным алфавитом автомата $\mathcal{A}$, а функция переходов такова, что входной сигнал $x \in S$ переводит состояние $s \in S$ в произведение xs, вычисляемое в моноиде $\mathbb{M}$. Докажем, что $\mathbb{M} \cong End\mathcal{A}$.

1) Каждый правый сдвиг λ_a моноида $\mathbb{M}$ является эндоморфизмом автомата $\mathcal{A}$.

Действительно, вспоминая, что соответствующий элементу $a \in S$ правый сдвиг есть отображение $\lambda_a : S \to S : x \mapsto xa$, для произвольных $s, x \in S$ получаем:

$$\lambda_a(\delta(s,x)) = \lambda_a(xs) = (xs)a = x(sa) = \delta(sa,x) = \delta(\lambda_a(s),x),$$

так что $\lambda_a \in End\mathcal{A}$.

2) Каждый эндоморфизм автомата $\mathcal{A}$ является правым сдвигом моноида $\mathbb{M}$.

В самом деле, если $\varphi \in End\mathcal{A}$, то для любого $x \in S$ получаем

$$\varphi(x) = \varphi(xe) = \varphi(\delta(e,x)) = \delta(\varphi(e),x) = x\varphi(e) = \lambda_{\varphi(e)}(x),$$

так что $\varphi = \lambda_{\varphi(e)}$.

3) Соответствие $s \mapsto \lambda_s$ является изоморфизмом моноидов $\mathbb{M}$ и $End\mathcal{A}$.

В теореме 2(§2) было доказано, что это соответствие представляет собой вложение моноида $\mathbb{M}$ в симметрический моноид $\mathcal{F}(S)$. Теперь мы видим, что область значений этого вложения совпадает с подмножеством $End\mathcal{A} \subseteq \mathcal{F}(S)$, которое в силу теоремы I замкнуто относительно суперпозиции и содержит тождественное преобразование Δ.

ЗАДАЧА I3. Какие конечные моноиды могут быть реализованы как моноиды эндоморфизмов автономных автоматов?

Пример I. Пусть $M=(S,\cdot,1)$ – четырехэлементный моноид: $S=\{1,2,3,4\}$, в котором умножение задается таблицей 7.

Таблица 7

·	1	2	3	4
1	1	2	3	4
2	2	2	3	3
3	3	2	3	2
4	4	2	3	1

Таблица 8

δ	1	2	3	4
1	1	2	3	4
2	2	2	2	2
3	3	3	3	3
4	4	3	2	1

В соответствии с теоремой 2 построим автомат $\mathcal{A}=(S,S,\delta)$ с функцией переходов, определенной таблицей 8. Таким образом, моноид M представлен как моноид эндоморфизмов автомата с четырьмя состояниями и четырьмя входными сигналами.

Рассмотрим теперь моноид всех преобразований двухэлементного множества, например, $A=\{\alpha,\beta\}$. Имеется в точности четыре преобразования этого множества. Мы запишем их в виде подстановок:

$$f_1=\begin{pmatrix}\alpha & \beta\\ \alpha & \beta\end{pmatrix},\quad f_2=\begin{pmatrix}\alpha & \beta\\ \alpha & \alpha\end{pmatrix},\quad f_3=\begin{pmatrix}\alpha & \beta\\ \beta & \beta\end{pmatrix},\quad f_4=\begin{pmatrix}\alpha & \beta\\ \beta & \alpha\end{pmatrix}.$$

Как нетрудно проверить, табл. 9 описывает операцию суперпозиции в моноиде $\mathcal{F}(A)$. Отображение $\varphi:\mathcal{F}(A)\to S: f_i\mapsto i$, где $1\le i\le 4$, является изоморфизмом моноидов $\mathcal{F}(A)$ и M. Но $\mathcal{F}(A)$ можно рассматривать как моноид эндоморфизмов $\mathrm{End}\,\mathcal{B}$ автономного автомата $\mathcal{B}$ с двумя состояниями и тождественной функцией переходов. Это означает, что моноид M можно представить как моноид эндоморфизмов автомата $\mathcal{B}$. При этом $\mathcal{A}$ содержит, как уже отмечалось, четыре состояния и четыре входных сигнала, а $\mathcal{B}$ – лишь два состояния и один входной сигнал. Этими рассмотрениями мотивируется

Таблица 9

∘	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_2	f_3	f_3
f_3	f_3	f_2	f_3	f_2
f_4	f_4	f_2	f_3	f_1

ЗАДАЧА I4. Реализовать заданный конечный моноид как моноид эндоморфизмов автомата с минимально возможным числом состояний.

3. Автомат $\mathcal{A}$ называется сильно жестким, если он не имеет нетождественных эндоморфизмов.

ТЕОРЕМА 3. Сильно жесткий автономный автомат тривиален (т.е. имеет одно состояние).

Доказательство. Пусть $\mathcal{A}=(S,\delta)$ – автономный автомат. Напомним, что δ мы рассматриваем как преобразование множества S. Эндоморфизмами автомата $\mathcal{A}$, по определению, будут преобразования, перестановочные в смысле суперпозиции с δ:

$$\varphi\in End\,\mathcal{A} \Longleftrightarrow (\forall s\in S)(\varphi(\delta(s))=\delta(\varphi(s))) \Longleftrightarrow \varphi\circ\delta=\delta\circ\varphi.$$

Если $\delta=\Delta$ (т.е. если δ каждое состояние переводит в себя), то любое преобразование множества S будет эндоморфизмом автомата $\mathcal{A}=(S,\delta)$, т.е. $End\,\mathcal{A}=\mathcal{T}(S)$. Понятно, что $\mathcal{T}(S)=\{\Delta\}$ лишь для одноэлементного S.

Если $\delta\neq\Delta$, то само преобразование δ является нетождественным эндоморфизмом автомата $\mathcal{A}$, и значит, $\mathcal{A}$ не может быть сильно жестким. ▨

Из доказанной теоремы следует, что понятие "сильно жесткий" для автономных автоматов лишено содержания. Что касается неавтономных автоматов, то здесь ситуация совсем другая.

ТЕОРЕМА 4. Для любого натурального числа n существует сильно жесткий автомат с двумя входными сигналами и n состояниями.

Доказательство. Пусть $\mathcal{A}=(S,X,\delta)$ – автомат с $S=\{1,2,\dots,n\}$, $X=\{x_1,x_2\}$ и с функцией переходов δ такой, что $\delta(s,x_1)=1$ для любого $s\in S$, а автономная x_2-компонента представляет собой цикл $1\longmapsto 2\longmapsto\dots\longmapsto n\longmapsto 1$.

Если φ – эндоморфизм автомата $\mathcal{A}$, то

$$\varphi(1)=\varphi(\delta(1,x_1))=\delta(\varphi(1),x_1)=1.$$

Следовательно, для любого $s\neq 2$ будет

$$\varphi(s)=\varphi(\delta(1,\underbrace{x_2x_2\dots x_2}_{s-1}))=\delta(\varphi(1),\underbrace{x_2x_2\dots x_2}_{s-1})=\delta(1,\underbrace{x_2x_2\dots x_2}_{s-1})=s.$$

Итак, $\varphi(s)=s$ для любого $s\in S$, т.е. $\varphi=\Delta$, и значит, автомат $\mathcal{A}$ – сильно жесткий.

ЗАДАЧА 15. Охарактеризовать сильно жесткие автоматы.

Автоматы можно классифицировать по свойствам их моноида эндоморфизмов. Например, автономные автоматы $\mathcal{A}$ с регулярными моноидами $End\,\mathcal{A}$ описал Л.А.Скорняков [17].

4. Посмотрим, какими свойствами обладают эндоморфизмы простейших по своей решеточной структуре автоматов. Начнем с примитивных

автоматов $\mathcal{A}$ – у которых двухэлементна решетка $Sub\,\mathcal{A}$, и следовательно, нет ненулевых собственных подавтоматов.

ЛЕММА. Если два эндоморфизма автомата одинаково действуют на некоторое состояние s_0, то они одинаково действуют и на любое состояние, достижимое из s_0.

Доказательство. Пусть $\mathcal{A}=(S,X,\delta)$ – автомат, φ_1,φ_2 – его эндоморфизмы и $\varphi_1(s_0)=\varphi_2(s_0)$ для некоторого состояния $s_0\in S$. Если состояние s достижимо из s_0, то существует слово $p(s)\in X^*$ такое, что $\delta(s_0,p(s))=s$. Тогда

$$\varphi_1(s)=\varphi_1\big(\delta(s_0,p(s))\big)=\delta\big(\varphi_1(s_0),p(s)\big)=\delta\big(\varphi_2(s_0),p(s)\big)=\varphi_2\big(\delta(s_0,p(s))\big)=\varphi_2(s).$$

Итак, $\varphi_1(s)=\varphi_2(s)$.

ТЕОРЕМА 5. Примитивный автомат с n состояниями имеет не более чем n различных эндоморфизмов.

Доказательство. Допустим, что моноид эндоморфизмов $End\,\mathcal{A}$ автомата $\mathcal{A}=(S,X,\delta)$ с n состояниями имеет больше, чем n, различных элементов. Пусть $s_0\in S$ – некоторое фиксированное состояние. Рассмотрим подмножество $S_0=\{\varphi(s_0):\varphi\in End\,\mathcal{A}\}$. Так как S_0 содержит не более, чем n, элементов, то для некоторых различных $\varphi_1,\varphi_2\in End\,\mathcal{A}$ должно выполняться равенство $\varphi_1(s_0)=\varphi_2(s_0)$. По теореме 3(§I 2) автомат сильно связен, т.е. любые два его состояния взаимно достижимы. Тогда в силу леммы сразу получаем $\varphi_1=\varphi_2$, что невозможно (φ_1 и φ_2, по предположению, не равны).

ТЕОРЕМА 6. Эндоморфизмы примитивного автомата являются обратимыми преобразованиями множества его состояний.

Доказательство. Согласно теореме 3(§2) достаточно установить, что каждый эндоморфизм φ примитивного автомата $\mathcal{A}=(S,X,\delta)$ отображает множество S на себя. Пусть s – произвольное фиксированное состояние автомата $\mathcal{A}$. Так как $\mathcal{A}$ сильно связен (теорема 3,§I.2), найдется слово $p\in X^*$ такое, что $\delta(\varphi(s),p)=s$. Тогда для $s^*=\delta(s,p)$ будет $\varphi(s^*)=\varphi(\delta(s,p))=\delta(\varphi(s),p)=s$. Следовательно, любое состояние s попадает в область значений эндоморфизма φ. ▨

Лемма и теоремы 5, 6 принадлежат Вигу [37].

5. Теперь обратимся к простым автоматам $\mathcal{A}$ – у которых двухэлементна решетка $Con\,\mathcal{A}$, и следовательно, нет нетождественных собственных конгруэнций.

Элемент a моноида $(A,\cdot,e)$ называется сократимым справа, если для любых $x,y\in A$ из $xa=ya$ следует равенство $x=y$.

Элемент a называется правым нулем в $(A,\cdot,e)$, если $xa=a$ для любого $x\in A$.

ТЕОРЕМА 7. Если $\mathcal{A}$ – простой автомат, то каждый элемент моноида $End\,\mathcal{A}$ либо сократим справа, либо является правым нулем.

Доказательство. Пусть φ_0 – произвольный эндоморфизм простого автомата $\mathcal{A}$. По теореме I(§I) ядро $Ker\varphi_0$ является конгруэнцией на $\mathcal{A}$. Но автомат $\mathcal{A}$ имеет только две конгруэнции: Δ и $S\times S$. Следовательно, $Ker\varphi_0=\Delta$ или $Ker\varphi_0=S\times S$.

Если $Ker\varphi_0=\Delta$, то φ_0 – взаимно однозначное преобразование множества S. Пусть $\varphi_1,\varphi_2\in End\,\mathcal{A}$ и $\varphi_0\circ\varphi_1=\varphi_0\circ\varphi_2$. Тогда для любого $s\in S$ будет $\varphi_0(\varphi_1(s))=(\varphi_0\circ\varphi_1)(s)=(\varphi_0\circ\varphi_2)(s)=\varphi_0(\varphi_2(s))$ и, в силу взаимной однозначности, $\varphi_1(s)=\varphi_2(s)$, т.е. $\varphi_1=\varphi_2$. Значит, φ_0 – сократимый справа элемент моноида $End\,\mathcal{A}$.

Если $Ker\varphi_0=S\times S$, то все элементы множества S имеют один и тот же φ_0-образ, скажем, s_0. В этом случае для любого $s\in S$ и любого $\varphi\in End\,\mathcal{A}$ имеем: $(\varphi_0\circ\varphi)(s)=\varphi_0(\varphi(s))=s_0=\varphi_0(s)$, откуда $\varphi_0\circ\varphi=\varphi_0$, и значит, φ_0 – правый ноль моноида $End\,\mathcal{A}$. ▨

В следующем параграфе мы вернемся к моноидам эндоморфизмов простых автоматов, а сейчас покажем, что доказанная теорема не допускает обращения.

Пример 2. Пусть A – моноид, который образуют числа 0, I, 2 относительно умножения по модулю 3. Очевидно, что элементы I и 2 сократимы (справа и слева), а элемент 0 является (правым и левым) нулем. По теореме 2 моноид A изоморфен моноиду эндоморфизмов $End\,\mathcal{A}$ автомата $\mathcal{A}=(A,A,\delta)$, где $\delta(s,x)=xs$ для любых $s\in A$, $x\in A$. Видно, что разбиение $\theta=[0],[I,2]$ является конгруэнцией автомата $\mathcal{A}$, отличной от Δ и $S\times S$, – автомат $\mathcal{A}$ не простой.

§4. Некоторые свойства группы автоморфизмов автомата

I. Взаимно однозначные эндоморфизмы автомата называются его автоморфизмами. Можно сказать также, что автоморфизмы автомата – это его изоморфизмы на себя. Множество всех автоморфизмов автомата $\mathcal{A}$ обозначается через $Aut\,\mathcal{A}$.

ТЕОРЕМА I. Множество $Aut\,\mathcal{A}$ образует относительно суперпозиции и обращения группу, нейтральным элементом которой является тождественное преобразование Δ.

Доказательство. По определению, каждый автоморфизм представ-

ляет собой обратимое преобразование множества состояний S. Следовательно, $Aut\mathcal{A} = End\mathcal{A} \cap K(S)$. Поскольку оба множества $End\mathcal{A}$ и $K(S)$ замкнуты относительно суперпозиции преобразований и оба содержат тождественное преобразование Δ, то $(Aut\mathcal{A}, \circ, \Delta)$ будет моноидом. Пусть $\varphi \in Aut\mathcal{A}$ и φ^{-1} – обратное для φ преобразование. Для любых $s \in S$, $x \in X$ имеем:

$$\varphi^{-1}(\delta(s,x)) = \varphi^{-1}(\delta(\Delta(s),x)) = \varphi^{-1}(\delta((\varphi\circ\varphi^{-1})(s),x)) =$$

$$= \varphi^{-1}(\delta(\varphi(\varphi^{-1}(s)),x)) = \varphi^{-1}(\varphi(\delta(\varphi^{-1}(s),x))) = (\varphi^{-1}\circ\varphi)(\delta(\varphi^{-1}(s),x)) =$$

$$= \Delta(\delta(\varphi^{-1}(s),x)) = \delta(\varphi^{-1}(s),x).$$

Следовательно, φ^{-1} является автоморфизмом автомата $\mathcal{A}$, и значит, в моноиде $(Aut\mathcal{A}, \circ, \Delta)$ каждый элемент обратим. ▨

Группа $Aut\mathcal{A}$ называется группой автоморфизмов автомата $\mathcal{A}$.

2. Из теоремы 2(§3) следует ([23])

ТЕОРЕМА 2. Каждая конечная группа изоморфна группе автоморфизмов подходящего автомата.

Доказательство. Пусть G – заданная конечная группа. Как показано в теореме 2(§3), она может быть реализована как моноид эндоморфизмов автомата $\mathcal{A} = (G, G, \delta)$, где $\delta(s,x) = xs$ для любых $s \in G$, $x \in G$. При этом для любых двух состояний $s_1, s_2 \in G$ будет $s_2 = (s_2 s_1^{-1}) s_1 = \delta(s_1, s_2 s_1^{-1})$. Следовательно, в автомате $\mathcal{A}$ любые два состояния взаимно достижимы, и значит (теорема 3(§I.2)), $\mathcal{A}$ – примитивный автомат. По теореме 6(§3) каждый эндоморфизм такого автомата будет его автоморфизмом.

ЗАДАЧА I6. Какие конечные группы являются группами автоморфизмов автономных автоматов?

3. Автомат $\mathcal{A}$ называется жестким, если он не имеет нетождественных автоморфизмов.

ТЕОРЕМА 3. Для любого натурального числа n существует жесткий автономный автомат с n состояниями.

Доказательство. Пусть $S = \{1, 2, \ldots, n\}$, $n \geq 2$. Положим $\delta(1) = 1$ и $\delta(s) = s-1$ для $s \geq 2$. Граф переходов автомата $\mathcal{A}$ представляет собой петлю (в вершине 1) с одним простым хвостом.

Пусть φ – автоморфизм построенного автомата $\mathcal{A}$. Тогда $\varphi(1) = \varphi(\delta(1)) = \delta(\varphi(1))$, откуда $\varphi(1) = 1$ (в автомате

$\mathcal{A}$ есть только одно состояние, переходящее в себя под действием входного сигнала). Далее, $I = \varphi(I) = \varphi(\delta(2)) = \delta(\varphi(2))$, и следовательно, $\varphi(2) = I$ или $\varphi(2) = 2$. Первое равенство противоречит взаимной однозначности отображения φ, так что будет $\varphi(2) = 2$. Аналогичные рассуждения показывают, что $\varphi(3) = 3$ и т.д.

Таким образом, $\varphi = \Delta$, - в автомате $\mathcal{A}$ нет нетождественных автоморфизмов.

ЗАДАЧА 17. Какие свойства функции переходов автомата равносильны его жесткости?

4. Теперь исследуем строение группы автоморфизмов простого автомата. Следующий результат получил Гретцер [31].

ТЕОРЕМА 4. Циклические группы простого порядка, и только они, являются группами автоморфизмов простых автоматов.

Доказательство. I) Пусть φ - нетождественный автоморфизм простого автомата $\mathcal{A} = (S, X, \delta)$. На множестве S рассмотрим отношение $\theta_\varphi = \{(s_1, s_2) : (\exists k \in \mathbb{Z})(s_2 = \varphi^k(s_1))\}$. При этом, по определению,

$$\varphi^k = \begin{cases} \Delta, & \text{если } k = 0, \\ \underbrace{\varphi \circ \varphi \circ \ldots \circ \varphi}_{k}, & \text{если } k > 0, \\ (\varphi^{-1})^{|k|}, & \text{если } k < 0. \end{cases}$$

Отношение θ_φ является конгруэнцией автомата $\mathcal{A}$:

а) $s = \Delta(s) = \varphi^0(s)$ (рефлексивность),

б) $s_2 = \varphi^k(s_1) \,\&\, s_3 = \varphi^\ell(s_2) \Longrightarrow s_3 = \varphi^{k+\ell}(s_1)$ (транзитивность),

в) $s_2 = \varphi^k(s_1) \Longrightarrow s_1 = (\varphi^{-1})^k(s_2)$ (симметричность),

г) $(s_1, s_2) \in \theta_\varphi \Longrightarrow (\exists k \in \mathbb{Z})(s_2 = \varphi^k(s_1)) \Longrightarrow \delta(s_2, x) = \delta(\varphi^k(s_1), x) = \varphi^k(\delta(s_1, x)) \Longrightarrow (\delta(s_1, x), \delta(s_2, x)) \in \theta_\varphi$ (устойчивость).

Так как $\mathcal{A}$ - простой автомат, то должно быть $\theta_\varphi = \Delta$ или $\theta_\varphi = S \times S$. Но равенство $\theta_\varphi = \Delta$ немедленно влечет равенство $\varphi = \Delta$. Так как φ, по предположению, есть нетождественное преобразование, остается одна возможность $\theta_\varphi = S \times S$.

Пусть ψ - произвольный автоморфизм автомата $\mathcal{A}$ и s_0 - некоторое фиксированное состояние. Поскольку $\theta_\varphi = S \times S$, найдется целое число k_0 такое, что $\psi(s_0) = \varphi^{k_0}(s_0)$.

Положим $\chi = \psi^{-1} \cdot \varphi^{k_0}$. Тогда $\chi(s_0) = (\psi^{-1} \circ \varphi^{k_0})(s_0) = \psi^{-1}(\varphi^{k_0}(s_0)) = \psi^{-1}(\psi(s_0)) = s_0$. Следовательно, $\chi^\ell(s_0) = s_0$ для любого $\ell \in \mathbb{Z}$.

Это означает, что $\theta_\chi(s_0)=\{s_0\}$, и значит, $\theta_\chi \neq S\times S$. В силу простоты автомата $\mathcal{A}$, получаем, что $\theta_\chi=\Delta$, откуда сразу $\chi=\Delta$.

Итак, $\Delta=\chi=\psi^{-1}\circ\varphi^{k_0}$, и следовательно, $\psi=\varphi^{k_0}$,- каждый элемент группы $Aut\,\mathcal{A}$ является степенью элемента φ : группа $Aut\,\mathcal{A}$ - циклическая.

Автоморфизм φ выбирался произвольно из $Aut\,\mathcal{A}\setminus\{\Delta\}$. Значит, группа $Aut\,\mathcal{A}$ порождается любым своим отличным от Δ элементом. Рассуждение, проведенное в конце п.7(§2),показывает, что порядок группы $Aut\,\mathcal{A}$ не имеет нетривиальных делителей, так что $Aut\,\mathcal{A}$ - циклическая группа простого порядка.

2) Пусть теперь G - циклическая группа простого порядка p. По теореме 2 эта группе изоморфна группе автоморфизмов автомата $\mathcal{A}=(G,G,\delta)$, где $\delta(s,x)=xs$ для любых $s\in G$, $x\in G$. Покажем, что автомат $\mathcal{A}$ - простой.

Допустим, что θ - нетождественная конгруэнция автомата $\mathcal{A}$. Тогда существуют два различных состояния - s_1, s_2 - таких, что $(s_1,s_2)\in\theta$. Состояния $e=s_1^{-1}s_1=\delta(s_1,s_1^{-1})$ и $s_0=s_1^{-1}s_2=\delta(s_2,s_1^{-1})$ (они различны) должны содержаться в одном θ-классе. Поскольку G - циклическая группа простого порядка p, будет $G=\{e, s_0, s_0^2,\dots, s_0^{p-1}\}$ (каждый отличный от единицы e элемент порождает группу G).

Теперь получаем:

$$(e,s_0)\in\theta\Longrightarrow(\delta(e,s_0),\delta(s_0,s_0))\in\theta\Longrightarrow(s_0,s_0^2)\in\theta\Longrightarrow(e,s_0^2)\in\theta\Longrightarrow$$

$$\Longrightarrow(\delta(e,s_0),\delta(s_0^2,s_0))\in\theta\Longrightarrow(s_0,s_0^3)\in\theta\Longrightarrow(e,s_0^3)\in\theta\Longrightarrow\dots\Longrightarrow(e,s_0^{p-1})\in\theta,$$

так что $\theta=G\times G$. Автомат $\mathcal{A}$ - простой.

СЛЕДСТВИЕ I. Если простой автомат, имеющий не менее трех состояний, обладает нетождественным автоморфизмом, то этот автомат примитивен.

Доказательство. По теореме 2(§П.3) простой автомат, имеющий не менее трех состояний, либо примитивен, либо содержит единственный собственный подавтомат $\mathcal{A}^*\neq\emptyset$, причем S^* - одноэлементное подмножество. Пусть $S^*=\{s_0^*\}$. Тогда для любых $\varphi\in Aut\,\mathcal{A}$, $x\in X$, будет $\varphi(s_0^*)=\varphi(\delta(s_0^*,x))=\delta(\varphi(s_0^*),x)$, так что $\{\varphi(s_0^*)\}$ - устойчивое подмножество. Отсюда сразу получаем, что $\varphi(s_0^*)=s_0^*$.

В доказательстве теоремы 4 рассматривалась конгруэнция $\theta_\varphi=\{(s_1,s_2):(\exists k\in\mathbb{Z})(s_2=\varphi^k(s_1))\}$. Так как в нашем случае получается

$\theta_\varphi(s_0^*)=\{s_0^*\}$, то $\theta_\varphi \neq S\times S$. Если φ – нетождественный автоморфизм, то, кроме того, $\theta_\varphi \neq \Delta$.

Итак, допустив, что автомат $\mathcal{A}$ не примитивный, мы построили конгруэнцию, отличную от Δ и $S\times S$, что противоречит простоте автомата $\mathcal{A}$.

Пример I. Автономный автомат с двумя состояниями и тождественной функцией переходов является простым, но имеет два собственных ненулевых подавтомата.

СЛЕДСТВИЕ 2. Если простой автомат обладает нетождественным автоморфизмом, то количество его состояний выражается простым числом.

Доказательство. Пусть $\mathcal{A}=(S,X,\delta)$ – простой автомат, у которого больше двух состояний. Согласно следствию I, $\mathcal{A}$ – примитивный автомат. По теореме 4 $Aut\mathcal{A}=\{\Delta,\varphi,\varphi^2,\dots,\varphi^{p-1}\}$ для любого нетождественного автоморфизма φ и некоторого фиксированного простого числа p. Пусть s_0 – произвольное состояние автомата $\mathcal{A}$. Согласно лемме из п.4(§3), все состояния $s_0=\Delta(s_0), s_1=\varphi(s_0), s_2=\varphi^2(s_0), \dots, s_{p-1}=\varphi^{p-1}(s_0)$ попарно различны (по теореме 3(§I.2) в автомате $\mathcal{A}$ любое состояние достижимо из s_0). Эти состояния образуют класс $\theta_\varphi(s_0)$ конгруэнции $\theta_\varphi=\{(s_1,s_2):(\exists k\in\mathbb{Z})(s_2=\varphi^k(s_1))\}$. Так как $\mathcal{A}$ – простой автомат, а $\varphi\neq\Delta$, то $\theta_\varphi=S\times S$, откуда получаем, что $S=\theta_\varphi(s_0)=\{s_0,s_1,\dots,s_{p-1}\}$.

Итак, множество S содержит точно p элементов.

5. Вернемся к исследованию моноида эндоморфизмов простого автомата (см.п.5(§3)). Теорема 4 позволяет уточнить результат, сформулированный в теореме 7 (из §3).

СЛЕДСТВИЕ 3. Если простой автомат $\mathcal{A}$ имеет не менее трех состояний, то I) $End\mathcal{A}=Aut\mathcal{A}$ или 2) $End\mathcal{A}=\{\Delta,\omega\}$, где ω – постоянное преобразование.

Доказательство. I) Если автомат $\mathcal{A}$ примитивен, то $End\mathcal{A}=Aut\mathcal{A}$, согласно теореме 6 (из §3).

2) Пусть $\mathcal{A}$ – непримитивный простой автомат, имеющий не менее трех состояний. Из следствия I получаем, что $\mathcal{A}$ не имеет нетождественных автоморфизмов. Поэтому $Ker\varphi\neq\Delta$ для любого эндоморфизма $\varphi\neq\Delta$.

По теореме 2(§II.3) в автомате $\mathcal{A}$ имеется единственное непустое устойчивое подмножество $S^*\neq S$ и оно одноэлементно: $S^*=\{s_0^*\}$. Тогда $\delta(s_0^*,x)=s_0^*$ для любого $x\in X$. При этом для всякого $\varphi\in End\mathcal{A}$ будет $\varphi(s_0^*)=\varphi(\delta(s_0^*,x))=\delta(\varphi(s_0^*),x)$, каким бы ни был $x\in X$, и значит, $\varphi(s_0^*)=s_0^*$.

Теперь определим $\omega : S \to S$, полагая $\omega(s) = s_0^*$ для всех $s \in S$. Конечно, $\omega \in End\mathcal{A}$: $\omega(\delta(s,x)) = s_0^* = \delta(s_0^*, x) = \delta(\omega(s_0^*), x)$. Далее, ω является нулем моноида $End\mathcal{A}$: $(\varphi\circ\omega)(s) = \varphi(\omega(s)) = \varphi(s_0^*) = s_0^* = \omega(s)$ и $(\omega\circ\varphi)(s) = \omega(\varphi(s)) = s_0^* = \omega(s)$ для любого эндоморфизма $\varphi \in End\mathcal{A}$.

Теорема 7 (§3) утверждает, что эндоморфизмы простого автомата являются либо автоморфизмами (сократимые справа элементы моноида $End\mathcal{A}$), либо постоянными отображениями (правые нули моноида $End\mathcal{A}$). В нашем случае нетождественных автоморфизмов нет, а поскольку ω представляет собой ноль моноида $End\mathcal{A}$, в этом моноиде нет других правых нулей (допустив наличие такого элемента φ, мы получили бы $\omega = \varphi\circ\omega = \varphi$).

Итак, $End\mathcal{A} = \{\Delta, \omega\}$. ▨

Теперь можно дать абстрактное описание класса моноидов эндоморфизмов простых автоматов.

ТЕОРЕМА 5. Моноидами эндоморфизмов простых автоматов являются (с точностью до изоморфизма) лишь следующие моноиды: 1) одноэлементный моноид, 2) циклические группы простых порядков, 3) моноид преобразований двухэлементного множества, 4) двухэлементный моноид с идемпотентным умножением.

Доказательство. Автомат с одним состоянием имеет одноэлементный моноид эндоморфизмов.

Рассмотрим автоматы с двумя состояниями (они, конечно, все являются простыми). Пусть $S = \{\alpha, \beta\}$. Эндоморфизмами автономного автомата $\mathcal{A}_0 = (S, \Delta)$ будут всевозможные преобразования множества S. Следовательно, моноид $End\mathcal{A}_0$ представляет собой моноид преобразований двухэлементного множества. У каждого из автономных автоматов $\mathcal{A}_\alpha = (S, \omega_\alpha)$ и $\mathcal{A}_\beta = (S, \omega_\beta)$, где ω_α и ω_β – постоянные отображения со значениями α и β соответственно, два эндоморфизма: Δ и функция переходов. Таким образом, моноиды эндоморфизмов $End\mathcal{A}_\alpha$ и $End\mathcal{A}_\beta$ представляют собой двухэлементные моноиды с идемпотентным умножением ($\omega_\alpha\circ\omega_\alpha = \omega_\alpha$ и $\omega_\beta\circ\omega_\beta = \omega_\beta$). Наконец, автономный автомат $\mathcal{A}_1 = (S, \delta_1)$, где $\delta_1(\alpha) = \beta$, $\delta_1(\beta) = \alpha$, имеет эндоморфизмами Δ и $\varphi: \alpha \mapsto \beta$, $\beta \mapsto \alpha$, так что будет $End\mathcal{A}_1 = Aut\mathcal{A}_1$, и это будет двухэлементная (циклическая) группа.

Моноид эндоморфизмов любого автомата является подмоноидом моноида эндоморфизмов каждой автономной компоненты этого автомата, так что мы знаем теперь моноиды эндоморфизмов всех (простых) автоматов с числом состояний $\leqslant 2$.

Если простой автомат $\mathcal{A}$ имеет не менее трех состояний и не примитивен, то, согласно теореме 6(§3), $End\mathcal{A}=Aut\mathcal{A}$, а по теореме 4, $Aut\mathcal{A}$ будет циклической группой простого порядка. Если же $\mathcal{A}$ не примитивен, то ввиду следствия 3 из теоремы 4, $End\mathcal{A}$ – двухэлементный моноид с идемпотентным умножением.

Пример 2. Пусть $S=\{\alpha,\beta\}$. Тождественное преобразование Δ вместе с постоянными преобразованиями $\omega_\alpha: s\mapsto\alpha$ и $\omega_\beta: s\mapsto\beta$ образует подмоноид $\mathbb{M}$ моноида $\mathcal{F}(S)$ всех преобразований двухэлементного множества S. В отличие от всех других подмоноидов этого моноида, $\mathbb{M}$ не может быть реализован в виде моноида эндоморфизмов какого-нибудь простого автомата (он не содержится в списке теоремы 5).

§5. Гомоморфизмы автоматов как матрицы

Здесь будет рассмотрен матричный метод нахождения всех гомоморфизмов одного автомата в другой.

Пусть $\mathcal{A}=(S,X,\delta)$ и $\mathcal{B}=(T,X,\xi)$ – автоматы с одинаковым входным алфавитом. Напомним, что отображение $\varphi: S\to T$ называется гомоморфизмом автомата $\mathcal{A}$ в автомат $\mathcal{B}$, если

$$(\forall s\in S)(\forall x\in X)(\varphi(\delta(s,x))=\xi(\varphi(s),x))$$

Пусть автомат $\mathcal{A}$ имеет n состояний. Каждому входному сигналу $x\in X$ сопоставим $(n\times n)$-матрицу $A(x)$ с элементами из решетки $\{0, I\}$ такую, что

$$[A(x)]_{ij}=\begin{cases} I, & \text{если } \delta(s_i,x)=s_j,\\ 0 & \text{в противном случае.}\end{cases}$$

Совершенно аналогично в случае, когда автомат $\mathcal{B}$ имеет m состояний, каждому $x\in X$ соотносится $(m\times m)$-матрица $B(x)$ с элементами из $\{0, I\}$ так, что

$$[B(x)]_{ij}=\begin{cases} I, & \text{если } \xi(t_i,x)=t_j,\\ 0 & \text{в противном случае.}\end{cases}$$

Отображение $\varphi: S\to T$ в свою очередь представляется $(n\times m)$-матрицей Φ с элементами из $\{0, I\}$, где

$$\Phi_{ij}=\begin{cases} I, & \text{если } \varphi(s_i)\ t_j,\\ 0 & \text{в противном случае.}\end{cases}$$

Матрицы с элементами из решетки перемножаются аналогично числовым матрицам с заменой сложения и умножения соответственно на решетчные операции объединения и пересечения.

ТЕОРЕМА. Отображение $\varphi : S \to T$ тогда и только тогда является гомоморфизмом автомата $\mathcal{A}$ в автомат $\mathcal{B}$, когда для любого $x \in X$ выполняется равенство $A(x)\Phi = \Phi B(x)$.

Доказательство. Пусть $\varphi : \mathcal{A} \to \mathcal{B}$ – гомоморфизм. Тогда для произвольного $x \in X$ имеем:

$$[A(x)\Phi]_{ik} = 1 \iff \bigvee_{j=1}^{n} (A_{ij} \wedge \Phi_{jk}) = 1 \iff (\exists j^*)(A_{ij^*} = 1 \;\&\; \Phi_{j^*k} = 1) \iff$$

$$\iff (\exists j^*)(\delta(s_i, x) = s_{j^*} \;\&\; \varphi(s_{j^*}) = t_k) \iff \varphi(\delta(s_i, x)) = t_k \iff$$

$$\iff \delta(\varphi(s_i), x) = t_k \iff (\exists j^*)(\varphi(s_i) = t_{j^*} \;\&\; \delta(t_{j^*}, x) = t_k) \iff$$

$$\iff \bigvee_{j=1}^{m} (\Phi_{ij} \wedge B_{jk}) = 1 \iff [\Phi B(x)]_{ij} = 1,$$

откуда $A(x)\Phi = \Phi B(x)$.

С другой стороны, если $A(x)\Phi = \Phi B(x)$ для любого $x \in X$, то для всех $s_i \in S$, $t_k \in T$ будет

$$\varphi(\delta(s_i, x)) = t_k \iff (\exists s_j)(\delta(s_i, x) = s_j \;\&\; \varphi(s_j) = t_k) \iff$$

$$\iff (\exists j)([A(x)]_{ij} = 1 \;\&\; \Phi_{jk} = 1) \iff 1 = \bigvee_{j=1}^{n} A_{ij}\Phi_{jk} =$$

$$= [A(x)\Phi]_{ik} = [\Phi B(x)]_{ik} \iff (\exists j)(\Phi_{ij} = 1 \;\&\; [B(x)]_{jk} = 1) \iff$$

$$\iff (\exists t_j)(\varphi(s_i) = t_j \;\&\; \delta(t_j, x) = t_k) \iff \delta(\varphi(s_i), x) = t_k,$$

и значит, φ – гомоморфизм автомата $\mathcal{A}$ в автомат $\mathcal{B}$.

Пример 1. Пусть $X = \{x_1, x_2\}$, $S = \{s_1, s_2, s_3, s_4\}$, $T = \{t_1, t_2, t_3\}$ и автоматы $\mathcal{A} = (S, X, \delta)$, $\mathcal{B} = (T, X, \delta)$ заданы таблицами 10, а), б).

Таблица 10

а)

$\delta_{\mathcal{A}}$	x_1	x_2
s_1	s_2	s_1
s_2	s_3	s_2
s_3	s_3	s_2
s_4	s_4	s_3

б)

$\delta_{\mathcal{B}}$	x_1	x_2
t_1	t_1	t_1
t_2	t_2	t_1
t_3	t_1	t_3

Найдем все гомоморфизмы автомата $\mathcal{A}$ в автомат $\mathcal{B}$.

$$A_1 = A(x_1) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \Phi = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \\ \delta_1 & \delta_2 & \delta_3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = B(x_1) = B_1.$$

Должно быть $A_1\Phi = \Phi B_1$.

Сравнивая элементы, стоящие на одинаковых местах в получающихся матрицах размерности 4×3, имеем:

$\beta_1 = \alpha_1 \vee \alpha_3$, $\gamma_1 = \beta_1 \vee \beta_3$, $\gamma_1 = \gamma_1 \vee \gamma_3$, $\delta_1 = \delta_1 \vee \delta_3$,

$\beta_2 = \alpha_2$, $\gamma_2 = \beta_2$, $\gamma_2 = \gamma_2$, $\delta_2 = \delta_2$,

$\beta_3 = 0$, $\gamma_3 = 0$, $\gamma_3 = 0$, $\delta_3 = 0$.

Искомая матрица Φ приобретает следующий вид:

$$\Phi = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \alpha_2 & 0 \\ \gamma_1 & \alpha_2 & 0 \\ \delta_1 & \delta_2 & 0 \end{pmatrix}.$$

Теперь обращаемся ко второму входному сигналу:

$$A_2 = A(x_2) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = B(x_2) = B_2.$$

Должно быть $A_2\Phi = \Phi B_2$.

Сравнивая соответствующие элементы получающихся матриц, имеем:

$\alpha_1 = \alpha_1 \vee \alpha_2$, $\beta_1 = \beta_1 \vee \alpha_2$, $\beta_1 = \gamma_1 \vee \alpha_2$, $\gamma_1 = \delta_1 \vee \delta_2$,

$\alpha_2 = 0$, $\alpha_2 = 0$, $\alpha_2 = 0$, $\alpha_2 = 0$,

$\alpha_3 = \alpha_3$, $0 = 0$, $0 = 0$, $0 = 0$.

Искомая матрица Φ приобретает следующий вид:

$$\Phi = \begin{pmatrix} \alpha_1 & 0 & \alpha_3 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ \delta_1 & \delta_2 & 0 \end{pmatrix}.$$

В каждой строке матрицы Φ должна стоять точно одна единица. Значит, существуют в точности четыре гомоморфизма автомата $\mathcal{A}$ в автомат $\mathcal{B}$, именно: $\varphi_1: s_1, s_2, s_3, s_4 \mapsto t_1$; $\varphi_2: s_1, s_2, s_3 \mapsto t_1, s_4 \mapsto t_2$; $\varphi_3: s_1 \mapsto t_3$, $s_2, s_3, s_4 \mapsto t_1$; $\varphi_4: s_1 \mapsto t_3$, $s_2, s_3 \mapsto t_1$, $s_4 \mapsto t_2$.

ЗАДАЧА 18. Предложить эффективный способ решения систем матричных уравнений, связанных с гомоморфизмами автоматов.

ЛИТЕРАТУРА

1. Богомолов А.М. Частичные тесты // Кибернетика.- 1973.- №2.- С. 10-22.

2. Богомолов А.М., Салий В.Н. Решетки в теории автоматов (некоторые нерешенные проблемы) // Междунар. матем. конгресс.- Варшава, 1983.- ХП.- С. 48.

3. Грунский И.С. Строение класса автоматов, неотличимых простыми экспериментами // Комбинаторно-алгебр. методы в прикл. мат.- Горький, 1981.- С. 50-60.

4. Дидидзе Ц.Е. О гомоморфизмах автоматов // Тр. Вычисл. центра АН ГрузССР.- 1973.- Т. 12.- №1.- С. 118-131.

5. Егорова Д.П. Структура конгруэнций унарной алгебры // Упорядоченные множества и решетки.- Саратов, 1978.- Вып. 5.- С. 11-44.

6. Егорова Д.П., Скорняков Л.А. О структуре конгруэнций унарной алгебры // Упорядоченные множества и решетки.- Саратов, 1977.- Вып. 4.- С. 28-40.

7. Ильичева И.П., Печенкин В.В. Контроль структурных автоматов по стабильным отношениям // Методы и системы техн. диагностики.- Саратов, 1985.- Вып. 5.- С. 35-43.

8. Капитонова Ю.В. Об изоморфизме абстрактных автоматов. I // Кибернетика.- 1965.- №3.- С. 25-28.

9. Карпов Ю.Г. О группе автоморфизмов конечного автомата // Автоматика и телемеханика.- 1973.- №8.- С. 70-74.

10. Когаловский С.Р., Солдатова В.В. О решетках конгруэнтностей счетных алгебр // ВИНИТИ, 1982.- №392-82.- С. 1-16.

11. Мангушева И.П. Построение решетки стабильных толерантностей конечного автомата // Методы и системы техн. диагностики.- Саратов, 1981.- Вып. 2.- С. 107-112.

12. Печенкин В.В. Структурные свойства контролирующих автоматов // Методы и системы техн. диагностики.- Саратов, 1987.- Вып. 6.- С. 46-53.

13. Плаксин В.А. Конгруэнции конечных автоматов // Кибернетика.- 1982.- №1.- С. 43-46.

I4. Плоткин Б.И. Алгебраическая модель базы данных - автомата // Латвийский матем. ежегодник.- Рига, 1983.-Вып.27.- С. 216-232.

I5. Салий В.Н. Алгебраические конструкции, связанные с булевозначными автоматами // Методы и системы техн. диагностики.- Саратов, 1985.- Вып. 5.- С. 12-20.

I6. Салий В.Н. О булевозначных автономных автоматах// Методы и системы техн. диагностики.-Саратов,1987.-Вып.6.-С. 53-59.

I7. Скорняков Л.А. Unary algebras with regular endomorphism monoids// Acta sci. math.-1978.-V.40.-N3-4.-P.375-381.

I8. Скорняков Л.А. Unars // Coll. Math. Soc. János Bolyai, 29. Universal Algebra. Esztergom, 1977.- Amsterdam, 1982.- P.735-743.

I9. Спивак М.А. Введение в абстрактную теорию автоматов.- Саратов, 1970.

20. Хрусталев П.М. Покрытия и разбиения со свойством подстановки в конечных автоматах // Методы и системы техн. диагностики.- Саратов, 1981.- Вып.2.- С. 97-107.

21. Bavel Z., Grzymała-Busse J., Soo H.K. On the connectivity of the product of auto ta // Ann. Soc. math. pol. - 1984.- Sér. 4.- V. 7.- N 2.- P. 225-266.

22. Berman J. On the congruence lattices of unary algebras // Proc. Amer. Math. Soc.-1972.-V.36.-N1.-P.34-38

23. Birkhoff G. Sobre los grupos de automorphismos // Rev. Union Math. Argentina.-1946.-V.11.-N4.-P.155-157.

24. Birkhoff G., Lipson J.D. Universal algebra and automata // Proc. Symp. Pure Math.- Providence, 1974.- V. 25.- P. 41-51.

25. Căzănescu V.E. Quelques proprietes algébriques des automates // Discrete Math.- 1972.- V. 2.- N 2.- P. 97-109.

26. Ésik Z., Imreh B. Subdirectly irreducible commutative automata // Acta cybern.- 1981.- V. 5.- N 3.- P. 251-260.

27. F a r r E.H. Lattice properties of sequential machines // J. Assoc. Comput. Mach. - I963.- V.I0.- N3.- P.365-385.

28. F l e c k A.C. Isomorphism groups of automata // J.Assoc. Comput. Mach. - I962.- V.9.- N4.- P.469-476.

29. G i l l A., F l e x e r R. Periodic decomposition of sequential machines // J. Assoc. Comput. Mach. - I967.- V.I4.- P.666-676.

30. G o g u e n J.A., T h a t c h e r J.W., W a g n e r E., W r i g h t J.B. Factorizations, congruences, and the decomposition of automata and systems // Lect. Notes Comput. Sci. - I975.- V.28.- P.33-45.

3I. G r ä t z e r G. On the endomorphism semigroup of simple algebras // Math. Ann. - I976.- V.I70.- N4.- P.334-338.

32. G r z y m a ł a - B u s s e J.W. On the representation of finite lattices in the class of finite automata // MTA Számitástechn. és autom. kut. intéz. tanul.- I982.- N I37.- P. I99-204.

33. H o e h n k e H.-J. Allgemeine Algebra der Automaten // Weiterbildungszentr. Math. Kybern. und Rechnentechn. Sekt. Math.- I973.- N2.- S.2I-43.

34. I m r e h B. On finite definite automata // Acta cybern.- I985.- V.7.- N I.- P.6I-65.

35. J ó n s s o n B. Topics in universal algebra.- Berlin, I972.

36. P u d l a k P., T ů m a J. Every finite lattice can be embedded in the lattice of all equivalences over a finite set // Comment. math. Univ. carol.- I977.- V.I8.- N2.- P. 409-4I4.

37. W e e g G.P. The structure of an automaton and its operation-preserving transformation group // J.Assoc.Comput. Mach.- I962.- V.9.- P.345-349.

38. Y o e l y M. Subdirectly irreducible unary algebras // Amer. Math. Monthly.- I967.- V.74.- N8.- P. 957-960.

10 к.

ИЗДАТЕЛЬСТВО
САРАТОВСКОГО
УНИВЕРСИТЕТА
1988