М М

Σ

В.Б. Кудрявцев
А.С. Подколзин
Ш. Ушчумлич

ВВЕДЕНИЕ В ТЕОРИЮ АБСТРАКТНЫХ АВТОМАТОВ

ИЗДАТЕЛЬСТВО
МОСКОВСКОГО
УНИВЕРСИТЕТА

МГУ

В. Б. Кудрявцев,
А. С. Подколзин,
Ш. Ушчумлич

ВВЕДЕНИЕ В ТЕОРИЮ АБСТРАКТНЫХ АВТОМАТОВ

Допущено Министерством высшего и среднего специального образования СССР в качестве учебного пособия для студентов университетов, обучающихся по специальности «Математика»

ИЗДАТЕЛЬСТВО
МОСКОВСКОГО
УНИВЕРСИТЕТА
1985

УДК 519.95

Кудрявцев В. Б., Подколзин А. С., Ушчумлич Ш. Введение в теорию абстрактных автоматов. — М.. Изд-во Моск. ун-та, 1985.— 174 с.

Теория автоматов представляет собой раздел теории управляющих систем, изучающий математические модели преобразователей дискретной информации, называемые автоматами, прототипами которых являются различные реальные устройства. Предлагаемая книга содержит достаточно обширный материал по теории абстрактных автоматов и посвящена рассмотрению основных типов поведений автоматов, таких как автоматы-акцепторы, преобразователи, перечислители и. т. п., а также изучению возникающих здесь задач анализа и синтеза автоматов, учитывающему их сложностной аспект.

Рецензенты:

кафедра математической кибернетики Саратовского государственного университета им Н. Г Чернышевского,
докт. физ.-матем. наук *Ю. И. ЯНОВ*

К $\frac{1502000000-142}{077(02)-85}$ 86—85

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Теория автоматов представляет собой раздел теории управляющих систем, изучающий математические модели преобразователей дискретной информации, называемые автоматами. С определенной точки зрения такими преобразователями являются как реальные устройства (вычислительные машины, автоматы, живые организмы и т. п.), так и абстрактные системы (математические машины, аксиоматические теории и т. д.). Характерной особенностью этих преобразователей является дискретность функционирования и конечность областей значений параметров, описывающих их. Теория автоматов возникла в середине XX столетия в связи с изучением свойств конечных автоматов. Со временем предмет ее исследований расширился за счет рассмотрения также различных обобщений конечных автоматов. Содержательно конечный автомат можно охарактеризовать как устройство, имеющее входной и выходной каналы и находящееся в каждый из дискретных моментов времени, называемых тактовыми моментами, в одном из конечного числа состояний. По входному каналу в каждый тактовый момент в устройство поступают входные сигналы (из некоторого конечного множества сигналов). При этом указываются: а) закон изменения состояний к следующему тактовому моменту в зависимости от входного сигнала и состояния устройства в предыдущий момент; б) значения выходного сигнала (из некоторого конечного множества сигналов) устройства в текущий тактовый момент как функции состояния и входного сигнала в тот же момент. Существуют различные подходы к определению понятия конечного автомата, которые могут быть разбиты на группы макроподхода и микроподхода. При макроподходе интересуются, грубо говоря, внешним поведением устройства, тем, как оно осуществляет переработку входной информации в выходную информацию и в последовательность состояний, отвлекаясь от внутреннего его строения. На этом пути приходят к понятию абстрактного конечного автомата. Тем самым абстрактный конечный автомат может быть задан с помощью набора отображений, описывающих его «внешнее» функционирование. При микроподходе учитывается структура устройства, функционирование и связь между собой его частей. На этом пути приходят к понятию структурного конечного автомата.

В соответствии с двумя подходами к понятию автомата вся теория автоматов может быть разделена на теорию абстрактных автоматов и теорию структурных автоматов, изучающих различные свойства соответственно абстрактных и структурных автоматов. Настоящая книга посвящена изучению основ теории абстрактных автоматов. С автоматами связывают различные отношения, возникающие между входной и выходной информацией и состояниями, которые называются поведениями автоматов. Вокруг изучения этих поведений автоматов группируется основная проблематика теории автоматов. Можно выделить несколько наиболее важных видов поведения, которые удобно охарактеризовать применительно к модели абстрактного автомата и изучение которых тем самым составляет определенное содержание теории абстрактных автоматов. Это — поведение автоматов как преобразователей и как акцепторов, а также некоторые их модификации. При изучении автоматов как преобразователей интересуются отображениями последовательностей входных сигналов в множество последовательностей состояний и выходных сигналов, осуществляемых автоматами. При изучении автоматов как акцепторов интересуются тем, какие множества конечных последовательностей входных сигналов можно отличать друг от друга с помощью выходных сигналов автоматов. Рассматривается также поведение автоматов как сверхакцепторов, при котором автомат используется как средство различения бесконечных последовательностей входных сигналов. Если исследуется структура допустимых последовательностей выходных сигналов автомата, то говорят, что автомат рассматривается как перечислитель. Наконец, важный класс поведений автомата возникает при рассмотрении его функционирования в различных «внешних средах» (в частности, такая среда сама может описываться посредством конечного автомата). Основными задачами, возникающими при рассмотрении перечисленных типов поведений, являются задачи анализа (т. е. описания свойств поведения автоматов) и синтеза (т. е. построения автомата, поведение которого удовлетворяет заданным условиям).

Предлагаемая книга состоит из 4 глав. В первой главе вводится понятие абстрактного конечного автомата и определяются рассматриваемые далее типы поведений автоматов, для которых формулируются соответствующие задачи анализа и синтеза. Во второй главе рассматривается поведение автоматов как преобразователей, в третьей — поведение автоматов как акцепторов. Четвертая глава посвящена некоторым задачам, связанным с автоматами-сверхакцепторами, автоматами-перечислителями и автоматами, функционирующими во «внешних средах».

Вошедший в пособие материал неоднократно использовался авторами при чтении обязательных и специальных курсов по теории автоматов.

Авторы благодарят Е. Ветренникову, Э. Гасанова, С. Карташова, К. Коляду, А. Кибкало, А. Рябинина за помощь в оформлении рукописи.

Глава I
ПОНЯТИЕ АВТОМАТА

§ 1. ПРИМЕРЫ И СОДЕРЖАТЕЛЬНАЯ МОДЕЛЬ АВТОМАТА

При изучении многих реальных устройств и процессов наряду с построением их непрерывных математических моделей часто оказываются полезными также дискретные модели, в которых указывается лишь логика происходящих изменений, без учета количественных характеристик. При построении дискретной модели процесса функционирования некоторого устройства можно выделить следующие основные этапы.

1. Процесс предполагается происходящим в дискретные моменты времени, занумерованные числами 1, 2, 3, ... Эти моменты, вообще говоря, не являются отстоящими друг от друга на одинаковые промежутки времени, и их выбор может быть связан с наступлением тех или иных внешних по отношению к изучаемому процессу событий.

2. Выбираются некоторые (вообще говоря, непрерывные) параметры, описывающие: внутреннее состояние рассматриваемого устройства; возможные воздействия внешней среды на устройство; возможные воздействия устройства на внешнюю среду. Множества допустимых значений этих параметров разбиваются на конечное число попарно не пересекающихся классов; пусть $\{q_1, q_2, ..., q_n\}$ — классы, на которые разбиваются значения параметров, описывающих внутреннее состояние устройства; $\{a_1, ..., a_m\}$ — классы, на которые разбиваются значения параметров, описывающих воздействие внешней среды на устройство, и $\{b_1, ..., b_p\}$ — классы, на которые разбиваются значения параметров, описывающих воздействие устройства на внешнюю среду. Если параметры первого из указанных типов принадлежат классу q_i; второго типа — классу a_j; третьего типа — классу b_k, то говорим, что дискретная модель устройства находится в состоянии q_i; на вход ее поступает сигнал a_j, а на выходе возникает сигнал b_k.

3. Выбор разбиения на классы q_i, a_j, b_k множеств значений соответствующих параметров часто возможно бывает сделать таким, чтобы состояние $q(t+1)$ модели в момент дискретного времени $t+1$ и выходной сигнал $b(t)$ этой модели в момент времени t однозначно определялись состоянием $q(t)$ и входным сигналом $a(t)$, наблюдаемыми в момент времени t (здесь, как и при построении непрерывных моделей, делается допущение о возмож-

ности мгновенного воздействия входных параметров устройства на выходные его параметры). В этом случае для завершения построения модели достаточно задать определенные на конечных множествах функции, описывающие указанную зависимость значений $q(t+1)$ и $b(t)$ от значений $q(t)$ и $a(t)$.

Рассмотрим ряд примеров, иллюстрирующих указанный процесс построения дискретной модели реального устройства; такие модели (а иногда и сами устройства, функционирование которых адекватно описывается дискретными моделями) обычно называются автоматами.

Разменный автомат. В этом автомате удобно выделить три параметра: а) входную информацию, т. е. сигналы, вводимые в него; б) параметр, описывающий внутреннюю переработку автоматом входного сигнала; в) выходную информацию, т. е. сигналы, выдаваемые автоматом наружу. Входные сигналы разобьем на три группы. Первая группа состоит из пустого сигнала Λ, означающего, что в вводное гнездо автомата ничего не подается. Вторая группа состоит из сигнала 10 (рассматриваемый автомат разменивает монеты достоинством в 10 копеек), а третья включает в себя все остальные входные возмущения, которые мы обозначим буквой λ. Проследим, как содержательно проходит работа нашего устройства. В первый момент автомат готов к восприятию любой входной информации. Его внутренние компоненты занимают определенные положения, создавая некоторую ситуацию, которую мы назовем состоянием q^{Λ}. Это состояние характеризуется, в частности, тем, что после подачи любого входного сигнала на вход автомата, на выходе автомата в тот же момент ничего не выдается. Отсутствие сигнала на выходе мы также будем обозначать символом Λ. Кроме того, естественно предположить, что и состояние автомата q^{Λ} после подачи на его вход Λ к следующему моменту не изменится. Предположим теперь, что на вход автомата поступил сигнал 10. Автомат должен проанализировать этот сигнал, «понять», что это действительно десятикопеечная монета, и, убедившись в этом, выдать на выходе запроектированную информацию. Можно считать, что на анализ уходит один такт времени, поэтому к следующему моменту расположение внутренних компонент автомата изменится, создав новую ситуацию — состояние q^{10}, в котором при любой входной информации в этот же момент на выходе автомата должны быть выданы в качестве выходных сигналов два пятака, символически обозначенные через (5,5). Для завершения характеристики состояния q^{Λ} остается рассмотреть подачу на вход сигнала λ. Для автомата сигнал λ представляется запретным, и можно предположить, что после анализа этого сигнала и установления того, что λ отлично от Λ и 10, к следующему моменту расположение внутренних компонент должно измениться, создав состояние q^{λ}, которое можно интерпретировать как аварийное и в котором на выходе выдается сигнал Λ при любом входном сигнале в этот момент. Перейдем к завершению характеристик состояний q^{10} и q^{λ}. Естественно ожидать, что в состоянии q^{10}

автомат после подачи в этот момент на вход сигнала 10 к следующему моменту не изменит своего состояния, а после подачи сигнала λ к следующему моменту перейдет в состояние q^{λ}. Можно считать, что сам автомат, раз оказавшись в состоянии q^{λ}, всегда остается в нем, пока его не выведет из этого состояния оператор. Изложенное полуформальное описание «работы» разменного автомата, которое в смысле переработки входных последовательностей сигналов в выходные адекватно работе реального разменного автомата, удобнее задавать с помощью диаграмм. Для нашего автомата такая диаграмма приведена на рис. 1.1.
В ней кружки соответствуют состояниям автомата, в нижних частях кружков указаны выходные сигналы, которые вырабатывает ав-

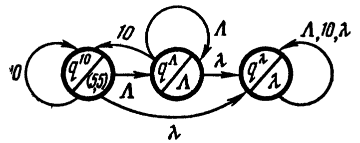

Рис. 1.1

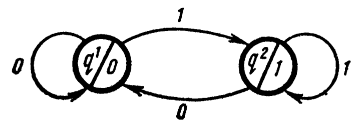

Рис 1.2.

томат, находясь в соответствующем кружку состояния. Исходящие из кружков стрелки соответствуют входным сигналам, подаваемым на вход автомата в момент, когда он находится в соответствующем кружку состоянии, и своими концами указывают, в какое состояние перейдет автомат к следующему моменту. Для экономии в состоянии q^{λ} все стрелки объединены в одну. С помощью этой диаграммы легко установить, что автомат, находясь в первый момент в состоянии q^{Λ}, «перерабатывает» входную последовательность сигналов $\Lambda\Lambda 101010 \Lambda\Lambda 10\Lambda$ в последовательность состояний $q^{\Lambda}q^{\Lambda}q^{\Lambda}q^{10}q^{10}q^{10}q^{\Lambda}q^{\Lambda}q^{10}q^{\Lambda}$ и последовательность выходных сигналов $\Lambda\Lambda\Lambda(5,5)(5,5)(5,5)\Lambda\Lambda(5,5)$.

Закон переработки автоматом последовательности входных сигналов в последовательности состояний и выходных сигналов обычно называют его функционированием.

Элемент задержки. Элемент задержки представляет собой электрическую схему, используемую в электронных вычислительных машинах и служащую для временной задержки импульсных сигналов. Входными сигналами элемента задержки служат символы 0 (отсутствие электрического импульса) и 1 (наличие импульса); выходные сигналы — также 0,1 в зависимости от отсутствия или наличия импульса. Элемент задержки имеет два состояния, q^1 и q^2. Если в момент времени t на вход элемента подается x, $x \in \{0, 1\}$, то этот же сигнал возникает на выходе элемента в момент времени $t+1$, чем и объясняется название элемента. Находясь в состоянии q^1, элемент задержки «помнит» о том, что в предыдущий момент времени на его вход поступил сигнал 0; в состоянии q^2 — «помнит» о том, что в предыдущий момент времени на вход поступил сигнал 1. Диаграмма, иллюстрирующая переходы элемента задержки из одного состояния в другое под действием входных сигналов, приведена на рис. 1.2.

В качестве примера отметим, что элемент задержки, находящийся в начальный момент времени в состоянии q^1, перерабатывает входную последовательность сигналов 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1 в последовательность выходных сигналов 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1.

Нервная клетка. Входные импульсы, поступающие на нервную клетку, разделим по их интенсивности на $n+1$ группу, обозначив эти группы $0, 1, 2, \ldots, n$. Нервная клетка может находиться в состояния покоя, состоянии возбуждения, а также в так называемых состояниях относительной рефрактерности, возникающих непосредственно после того, как клетка была возбуждена, и характеризующихся пониженной чувствительностью клетки к внешним воздей-

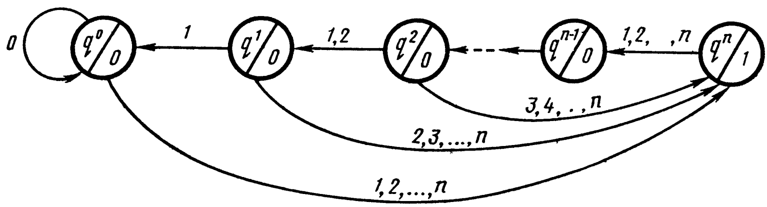

Рис. 1 3

ствиям. Указанные состояния нервной клетки также разобьем на $n+1$ группу, которые обозначим q^0, $q^1, \ldots, q^n$. При этом q^0 соответствует состоянию покоя; q^n — состоянию возбуждения, а $q^1, \ldots, q^{n-1}$ — состояниям относительности рефрактерности. Выходные сигналы нервной клетки разобьем на две группы: 0 (отсутствие импульса) и 1 (наличие импульса). Если нервная клетка находится в состоянии q^i, причем входной сигнал j таков, что $j \leqslant i$, то клетка переходит к следующему моменту времени в состояние q^{i-1}, если же $j > i$, то клетка возбуждается, переходя в состояние q^n. Выходной сигнал в состояниях $q^0 \ldots, \ldots, q^{n-1}$ есть 0; в состоянии q^n выходной сигнал есть 1. Диаграмма, иллюстрирующая изменение состояний нервной клетки под действием входных сигналов, приведена на рис. 1.3.

С учетом сформулированных в начале параграфа принципов построения дискретных моделей и рассмотренных примеров приходим к следующей **содержательной модели конечного автомата,** схематически изображенной на рис. 1.4. Эта модель имеет вход (стрелка, входящая в прямоугольник), корпус и выход (стрелка, исходящая из прямоугольника). «Работа» модели осуществляется в тактовые моменты времени 1, 2, 3, ... В каждый момент на вход модели подаются сигналы, т. е. входные буквы из некоторого конечного входного алфавита $A=\{a_1, a^2, \ldots, a^m\}$, корпус модели находится в одном из «внутренних» состояний, кодируемых буквами из конечного алфавита состояний $Q=\{q_1, q^2, \ldots, q^n\}$, а с выхода модели снимаются сигналы, т. е. выходные буквы из выходного алфавита $B=\{b^1, b^2, \ldots, b^n\}$. Входная буква и состояние модели в данный момент од-

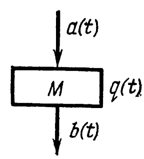

Рис. 1 4.

нозначно определяют выходную букву в этот же момент и состояние модели в следующий момент, т. е. если в момент t подавалась на вход буква $a(t)$, а модель находилась в состоянии $q(t)$, то $b(t)=\psi(q(t), a(t))$; $q(t+1)=\varphi(q(t), a(t))$. Пусть в первый момент модель M находится в некотором состоянии $q(1)$ (начальном состоянии). Используя функции φ и ψ, свяжем с M некоторую вычислительную процедуру, позволяющую по входному слову $a(1)a(2)\dots a(\tau)$ определить слово состояний $q(1)q(2)\dots q(\tau+1)$ и выходное слово $b(1)b(2)\dots b(\tau)$ следующим образом. По паре $(a(1), q(1))$ вычисляются два параметра $b(1)=\varphi(q(1), a(1))$ и $q(2)=\varphi(q(1), a(1))$, затем по паре $(a(2), q(2))$ вычисляются $b(2)=\psi(q(2), a(2))$ и $q(3)=\varphi(q(2), a(2))$, и так далее; если для $t, t\leqslant\tau$ уже вычислены значения $b(t-1)$ и $q(t)$, то вычисляются $b(t)=\psi(q(t), a(t))$ и $q(t+1)=\varphi(q(t), a(t))$.

Описанную вычислительную процедуру, устанавливающую соответствие между входными последовательностями, последовательностями состояний и выходными последовательностями, называют функционированием модели M. Модель M, у которой функционирование начинается всегда в одном и том же начальном состоянии q, называют инициальной моделью и обозначают через M_q. Описанная модель является содержательной трактовкой понятия абстрактного конечного автомата.

§ 2. ПОНЯТИЕ АБСТРАКТНОГО АВТОМАТА. СПОСОБЫ ЗАДАНИЯ АВТОМАТОВ

Абстрактным конечным автоматом $\mathfrak{A}$ называется система (A, Q, B, φ, ψ), где A, Q, B — конечные алфавиты, называемые соответственно входным алфавитом, множеством состояний и выходным алфавитом, $A=\{a^1, \dots, a^m\}$, $Q=\{q^1, \dots, q^n\}$, $B=\{b^1, \dots, b^p\}$,

φ — **функция переходов**, отображающая множество $Q\times A$ в Q;

ψ — **функция выходов**, отображающая множество $Q\times A$ в B.

Произвольные фиксированные значения из алфавитов A, Q, B будем обозначать через a, q, b соответственно, а переменные величины, принимающие значения из указанных алфавитов, через x, z, y соответственно. Число символов в алфавите C обозначаем далее посредством $|C|$.

Задание автомата $\mathfrak{A}$ фактически сводится к заданию функций φ и ψ, последнее может быть достигнуто с помощью построения таблиц с двумя входами, изображенных на рис. 1.5 и 1.6.

Иногда эти таблицы объединяют в одну, помещая на пересечении i-й строки и j-го столбца сразу $(\varphi(q^j, a^i), \psi(q^j, a^i))$. Удобным способом задания являются также так называемые **диаграммы Мура**. Они строятся следующим образом. На плоскости выбираются n кругов, которые взаимно-однозначно ставятся в соответствие состояниям автомата $\mathfrak{A}$, и внутри каждого круга пишется соответствующее ему значение. Затем из каждого круга проводят по m стрелок. Каждой стрелке, исходящей из круга состояний q^j, взаимно-однозначно соответствует буква из алфавита A. Стрелке, соответствующей букве a^i, приписывается пара (a^i, b^{n_i}), если $b^{n_i} = \psi(q^j, a^i)$. Эта стрелка упирается в круг состояния q^ω, если $q^\omega =$

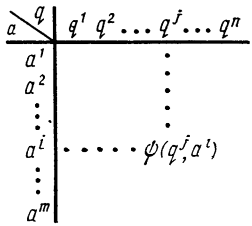

Рис. 1.5.

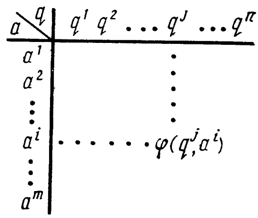

Рис. 1.6

$=\varphi(q^i, a^i)$. На рис. 1.7 приведен примерный фрагмент такой диаграммы.

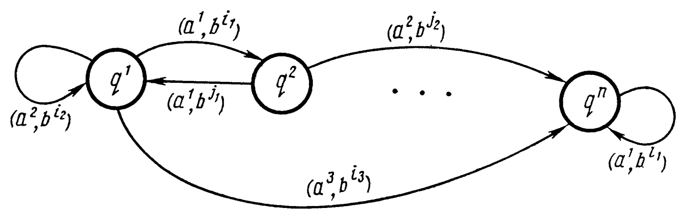

Рис. 1.7.

Пример 1. Пусть $\mathfrak{A} = (\{a^1, a^2\}, \{q^1, q^2\}, \{b^1, b^2\}, \varphi, \psi)$, где φ и ψ определены с помощью таблицы, изображенной на рис. 1.8.

$a \backslash q$	q^1	q^2
a^1	(q^1, b^1)	(q^2, b^2)
a^2	(q^2, b^1)	(q^2, b^2)

Рис. 1.8.

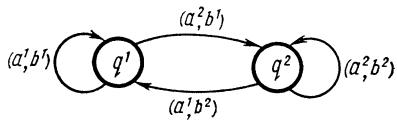

Рис. 1.9.

Диаграмма Мура автомата $\mathfrak{A}$ указана на рис. 1.9; при замене в ней символов a^1, b^1 на 0, a^2, b^2 — на 1 получаем диаграмму, иллюстрирующую работу описанного в § 1 элемента задержки.

Конечные последовательности букв из алфавитов A, Q и B автомата $\mathfrak{A}$, т. е. слова в этих алфавитах, называются соответственно **входными словами**, **словами состояний** и **выходными словами**, а бесконечные последовательности указанных букв, т. е. **сверхслова**, называются соответственно **входными сверхсловами**, **сверхсловами состояний** и **выходными сверхсловами**. Число букв в слове ξ называется **длиной слова** ξ и обозначается $|\xi|$. Для множества букв C через C^* обозначим множество всех слов ξ^m длины m,

$m=1,2,\ldots$, а через C^∞ — множество всех сверхслов ξ^∞ в этом алфавите. Иногда, когда длина слова для нас несущественна, мы будем писать ξ вместо ξ^m. Для удобства изложения функции φ и ψ распространим на множество $Q\times A^*$ следующим образом. Пусть $\alpha^m\in A^*$, $a\in A$, $q\in Q$, тогда, обозначая через Λ пустое слово, полагаем, что

$$\varphi(q,\Lambda)=q,\ \varphi(q,\alpha a)=\varphi(\varphi(q,\alpha),a),$$
$$\psi(q,\Lambda)=\Lambda,\ \psi(q,\alpha a)=\psi(\varphi(q,\alpha),a).$$

Пусть $\underset{n}{\overline{\alpha^m}|}$ обозначает начало слова α^m длины n, $n\geqslant 0$, $n\leqslant m$, при этом $\underset{0}{\overline{\alpha^m}|}$ пусть обозначает Λ. Определим слова $\overline{\varphi}(q,\alpha^m)$ и $\overline{\psi}(q,\alpha^m)$ в алфавитах Q и B соответственно следующим образом:

$$\overline{\varphi}(q,\alpha^m)=\varphi(q,\underset{0}{\overline{\alpha^m}|})\,\varphi(q,\underset{1}{\overline{\alpha^m}|})\ldots\varphi(q,\alpha^m),$$

$$\overline{\psi}(q,\alpha^m)=\psi(q,\underset{1}{\overline{\alpha^m}|})\,\psi(q,\underset{2}{\overline{\alpha^m}|})\ldots\psi(q,\alpha^m).$$

Говорим, что автомат $\mathfrak{A}$, находясь в начальном состоянии q, перерабатывает входное слово α^m в слово состояний $\overline{\varphi}(q,\alpha^m)$ и выходное слово $\overline{\psi}(q,\alpha^m)$. Преобразование входных слов автоматом $\mathfrak{A}$ можно охарактеризовать тернарным отношением $F=\{(\alpha^m,\overline{\varphi}(q,\alpha^m),\overline{\psi}(q,\alpha^m):\alpha^m\in A^*,\ q\in Q,\ m=1,2,\ldots\}$, называемым **функционированием автомата** $\mathfrak{A}$.

Исследуем функционирование некоторых примеров абстрактных конечных автоматов.

Пример 2. Пусть $\mathfrak{A}$ — автомат, определенный в примере 1. Тогда, как нетрудно видеть, $\overline{\varphi}(q^i,a^{i_1}\ldots a^{i_m})=q^iq^{i_1}\ldots q^{i_m}$; $\overline{\psi}(q^i,a^{i_1}\ldots a^{i_m})=b^ib^{i_1}\ldots b^{i_{m-1}}$. Функционирование автомата $\mathfrak{A}$ моделирует, таким образом, работу элемента задержки.

Нетрудно заметить, что и для остальных реальных автоматов, рассмотренных в § 1, диаграммы, иллюстрирующие работу этих автоматов, представляют собой диаграммы Мура некоторых абстрактных конечных автоматов. Функционирование этих абстрактных автоматов является математической моделью работы соответствующих реальных автоматов.

При изображении диаграмм Мура, во избежание излишней громоздкости, в тех случаях, когда из состояния q^i в состояние q^j ведет несколько параллельных стрелок, будем заменять эти стрелки одной такой стрелкой, приписывая ей все те пары (a^i,b^j), которые были приписаны заменяемым стрелкам.

Пример 3. Пусть $\mathfrak{A}=(\{0,1\},\{q^1,q^2,q^3\},\{0,1\},\varphi,\psi)$. Диаграмма Мура автомата $\mathfrak{A}$ приведена на рис. 1.10.
Легко видеть, что любое входное слово автомат $\mathfrak{A}$ перерабатывает в выходное слово, представляющее собой некоторый отрезок последовательности $0,0,1,0,0,1,0,0,1,\ldots$, причем выбор начала

этого отрезка определяется выбором начального состояния автомата $\mathfrak{A}$.

Пример 4. Пусть $\mathfrak{A} = (\{0, 1\}, \{q^1, q^2, q^3\}, \{0, 1\}, \varphi, \psi)$. Диаграмма Мура автомата $\mathfrak{A}$ приведена на рис. 1.11.
Находясь в начальном состоянии q^1, автомат $\mathfrak{A}$ перерабатывает входное слово $\alpha^3 = a(1) \ldots a(3)$ ($a(i)$ есть i-я буква слова α^3)

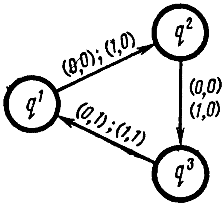

Рис. 1.10.

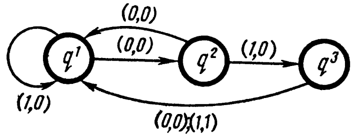

Рис. 1.11.

в такое выходное слово $\beta^3 = b(1) \ldots b(3)$, что $b(3) = 1$ тогда и только тогда, когда $a(3) = a(2) = 1$; $a(1) = 0$. Этот автомат, таким образом, распознает последовательное поступление на вход сигналов 0, 1, 1, реагируя на это сигналом 1 на выходе. Автомат $\mathfrak{B} = (A, Q', B, \varphi', \psi')$ называется **подавтоматом** автомата $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, если выполнены условия:

а) $Q' \subseteq Q$;

б) если $q \in Q'$ и $a \in A$, то $\varphi'(q, a) = \varphi(q, a)$; $\psi'(q, a) = \psi(q, a)$.

Пример 5. Пусть $\mathfrak{A} = (\{0, 1\}, \{q^1, q^2, q^3, q^4\}, \{0, 1\}, \varphi, \psi)$; диаграмма автомата $\mathfrak{A}$ указана на рис. 1.12. Автомат $\mathfrak{B} = (\{0, 1\}, \{q^3, q^4\},$

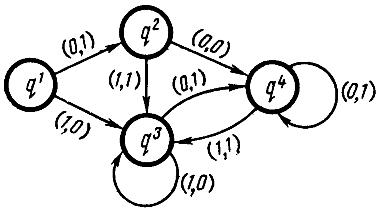

Рис 1.12.

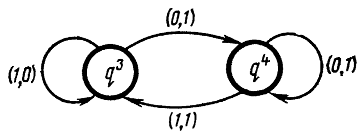

Рис. 1.13

$\{0, 1\}, \varphi', \psi')$, диаграмма которого приведена на рис. 1.13, является подавтоматом автомата $\mathfrak{A}$.

Изоморфизмом автомата $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ на автомат $\mathfrak{B} = (A', a', B', \varphi', \psi')$ называется тройка (f, g, h) взаимно-однозначных отображений $f: A \to A'$; $g: Q \to Q'$, $h: B \to B'$ таких, что имеют место тождества: $g(\varphi(q, a)) = \varphi'(g(q), f(a))$; $h(\psi(q, a)) = \psi'(g(q), f(a))$. Если (f, g, h) — изоморфизм автомата $\mathfrak{A}$ на автомат $\mathfrak{B}$, то, очевидно, (f^{-1}, g^{-1}, h^{-1}) (где посредством F^{-1} обозначается отображение, обратное к отображению F) — изоморфизм автомата $\mathfrak{B}$ на автомат $\mathfrak{A}$. Автоматы $\mathfrak{A}$ и $\mathfrak{B}$ называются **изоморфными**, если существует изоморфизм автомата $\mathfrak{A}$ на автомат $\mathfrak{B}$. Изоморфные автоматы отличаются друг от друга лишь переобозначением соответствующих алфавитов A, Q, B, поэтому во многих задачах можно не различать такие автоматы.

Гомоморфизмом автомата $\mathfrak{A}=(A, Q, B, \varphi, \psi)$ на автомат $\mathfrak{B}=(A', B', Q', \varphi', \psi')$ называется тройка (f, g, h) отображений $f: A \to A'$, $g: Q \to Q'$, $h: B \to B'$, таких, что имеют место тождества: $g(\varphi(q, \ a))=\varphi'(g(q), f(a))$; $h(\psi(q, \ a))=\psi'(g(q), f(a))$. Если существует гомоморфизм автомата $\mathfrak{A}$ на автомат $\mathfrak{B}$, то $\mathfrak{B}$ называется **гомоморфным образом** автомата $\mathfrak{A}$.

Пример 6. Пусть $\mathfrak{A}=(\{0,1,2\}, \{q^1, q^2, q^3, q^4\}, \{0,1,2\}, \varphi, \psi)$; $\mathfrak{B}=(\{a, b\}, \{p^1, p^2\}, \{c, d\}, \varphi', \psi')$, причем диаграммы автоматов $\mathfrak{A}$ и $\mathfrak{B}$ приведены на рис. 1.14, а) и б).

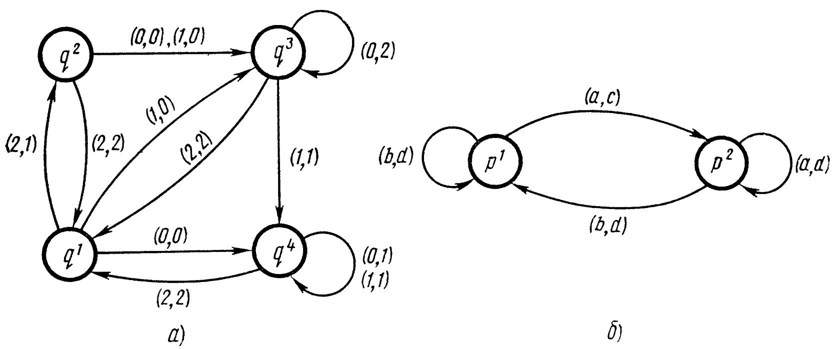

Рис. 1 14.

Пусть $f: \{0,1,2\} \to \{a, b\}$; $g: \{q^1, q^2, q^3, q^4\} \to \{p^1, p^2\}$; $h: \{0,1,2\} \to \to \{c, d\}$ — отображения, такие, что: $f(0)=f(1)=a$; $f(2)=b$; $g(q^1)=g(q^2)=p^1$; $g(q^3)=g(q^4)=p^2$; $h(1)=h(2)=d$; $h(0)=c$. Тогда, как легко проверить, тройка (f, g, h) есть гомоморфизм автомата $\mathfrak{A}$ на автомат $\mathfrak{B}$.

Определим некоторые операции над конечными автоматами. Пусть $\mathfrak{A}=(A, Q, B, \varphi, \psi)$; $\mathfrak{B}=(A, Q', B, \varphi', \psi')$, причем $Q \cap Q'=\varnothing$. **Суммой** автоматов $\mathfrak{A}$ и $\mathfrak{B}$, обозначаемой посредством $\mathfrak{A}+\mathfrak{B}$, называется автомат $(A, Q \cup Q', B, \varphi'', \psi'')$, где:

$$\varphi''(q, a)=\begin{cases}\varphi(q, a) \text{ при } q \in Q, \\ \varphi'(q, a) \text{ при } q \in Q',\end{cases} \quad \psi''(q, a)=\begin{cases}\psi(q, a) \text{ при } q \in Q, \\ \psi'(q, a) \text{ при } q \in Q'.\end{cases}$$

Пусть $\mathfrak{A}=(A, Q, B, \varphi, \psi)$; $\mathfrak{B}=(A', Q', B', \varphi', \psi')$. **Произведением** автоматов $\mathfrak{A}$ и $\mathfrak{B}$, обозначаемым $\mathfrak{A}\times\mathfrak{B}$, называется автомат $(A \times A', Q \times Q', B \times B', \varphi'', \psi'')$, где $\varphi'((q_1, q_2), (a_1 a_2))=(\varphi(q_1, a_1), \varphi'(q_2, a_2))$; $\psi''((q_1, q_2), (a_1 a_2))=(\psi(q_1 a_1), \psi'(q_2, a_2))$. Исходя из заданного набора конечных автоматов, при помощи операций суммы и произведения можно строить новые конечные автоматы. Использование этих операций можно рассматривать, таким образом, как один из способов задания конечных автоматов.

Автомат $\mathfrak{A}$ с выделенным состоянием q, именуемым начальным, называется **инициальным абстрактным конечным автоматом**, обозначается через $\mathfrak{A}_q$ и представляет собой набор $(A, Q, B, \varphi, \psi, q)$. Под функционированием автомата $\mathfrak{A}_q$ понимается тернарное отношение

$$F_q = \{(\alpha^m, \bar{\varphi}(q, \alpha^m), \bar{\psi}(q, \alpha^m)) : \alpha^m \in A^*, m = 1, 2, \dots\}.$$

В заключение параграфа отметим, что для задания инициальных автоматов и их функционирования могут быть использованы также так называемые канонические уравнения. Функционирование F_q инициального автомата $\mathfrak{A}_q = (A, Q, B, \varphi, \psi, q)$ состоит, очевидно, из всех троек слов $(\alpha, \varkappa, \beta)$, таких, что при некотором $m \in \{1, 2, \dots\}$ выполнено

$$\alpha = a(1) \dots a(m);\ \varkappa = q(1) \dots q(m+1);\ \beta = b(1) \dots b(m),$$

причем имеет место система соотношений

$$(*)\ \begin{cases} q(1) = q, \\ q(t+1) = \varphi(q(t), a(t)), \\ b(t) = \psi(q(t), a(t)) \end{cases}$$

$(t = 1, \dots, m)$, называемая **системой канонических уравнений автомата** $\mathfrak{A}_q$.

УПРАЖНЕНИЯ

1. Построить автомат $\mathfrak{A} = (\{0, 1\}, \{q^1, q^2, q^3\}, \{0, 1\}, \varphi, \psi)$, который при начальном состоянии q^1 перерабатывает слово 0010 в слово 0100, а слово 1011 — в слово 0001. Существует ли автомат с двумя состояниями, удовлетворяющий этому условию?
2. Построить автомат $\mathfrak{A} = (\{0, 1\}, \{q^1, q^2, q^3\}, \{0, 1\}, \varphi, \psi)$, удовлетворяющий условиям: $\bar{\psi}(q^1, 000) = 011$; $\bar{\psi}(q^2, 111) = 000$; $\bar{\psi}(q^3, 110) = 001$. Найти число таких автоматов.
3. Является ли автомат $\mathfrak{B}$ из примера 5 гомоморфным образом автомата $\mathfrak{A}$ из примера 6?
4. Найти число попарно неизоморфных автоматов, являющихся гомоморфными образами автомата $\mathfrak{A}$ из примера 6.
5. Изоморфен ли автомат $\mathfrak{A}$ из примера 6 произведению каких-либо двух автоматов $\mathfrak{A}_1$ и $\mathfrak{A}_2$, имеющих каждый по 2 состояния?
6. Существуют ли такие автоматы $\mathfrak{A}_1$ и $\mathfrak{A}_2$, имеющие по 3 состояния каждый, для которых автомат $\mathfrak{A}$ из примера 6 изоморфен некоторому подавтомату автомата $\mathfrak{A}_1 \times \mathfrak{A}_2$?

§ 3. НЕКОТОРЫЕ КЛАССЫ АБСТРАКТНЫХ АВТОМАТОВ

При решении различных задач теории автоматов часто возникают дополнительные условия на рассматриваемые автоматы, определяющие те или иные подклассы класса всех конечных автоматов. Важнейшие такие подклассы и будут описаны в настоящем параграфе.

Пусть $\mathfrak{A} = (A, Q, B, \varphi, \psi)$. В зависимости от вида функций φ, ψ, можно выделить следующие типы автоматов.

Автомат $\mathfrak{A}$ называется **автоматом Мура**, если функция $\varphi(q, a)$ не зависит от переменного a; $\psi(q, a) \equiv \psi(q)$. Для автоматов Мура диаграмма Мура может быть несколько изменена. Поскольку в этом случае выходная буква однозначно определяется состоянием, ее помещают в том же круге, что и состояние, а стрелкам приписываются не пары, а только входные буквы. На рис. 1.15 представлен примерный фрагмент такой диаграммы.

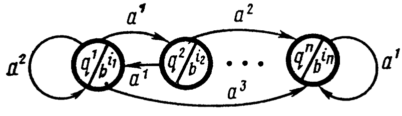

Рис. 1.15.

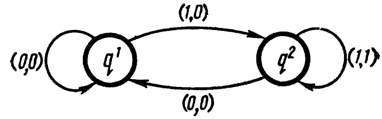

Рис. 1.16.

Аналогично можно поступать и в общем случае, помещая внутри круга, соответствующего состоянию q^i, формулу, задающую функцию $\psi_{q^i}(x) = \psi(q^i, x)$. В этом случае, во избежание излишней громоздкости, символ q^i внутри круга иногда не ставится.

Автомат $\mathfrak{A}$ называется **автоматом без памяти**, если функция $\psi(q, a)$ не зависит от переменного q; $\psi(q, a) \equiv \psi(a)$. В этом случае автомат $\mathfrak{A}$ реализует в каждый момент времени одно и то же отображение множества A входных сигналов в множество B выходных сигналов без учета информации, поступавшей на вход автомата в предыдущие моменты времени.

Автомат $\mathfrak{A}$ называется **обобщенной задержкой**, если функция $\varphi(q, a)$ не зависит от переменного q. В этом случае сигнал, возникающий на выходе автомата $\mathfrak{A}$ в момент времени t, определяется однозначно по входным сигналам, поступившим на автомат $\mathfrak{A}$ в моменты t и $t-1$. Примерами обобщенной задержки могут служить автоматы, диаграммы которых приведены на рис. 1.9, 1.16. Автомат $\mathfrak{A}$ называется **часами**, если функция $\varphi(q, a)$ не зависит от переменного a. В этом случае вне зависимости от поступающих на вход автомата $\mathfrak{A}$ сигналов, начиная с некоторого момента t состояния автомата $\mathfrak{A}$ начинают периодически повторяться: $q_1, q_2, \ldots q_n, q_1, q_2, \ldots q_n, \ldots$. Примером часов может служить автомат, диаграмма которого приведена на рис. 1.10.

В зависимости от особенностей функционирования выделяются, далее, следующие типы автоматов.

Автомат $\mathfrak{A}$ называется **самонастраивающимся**, если существует такое натуральное r_0, что для любого слова α^r, где $r \geqslant r_0$, $\alpha^r \in A^*$, и любых состояний $q_i, q_j \in Q$ имеет место $\psi(q_i, \alpha^r) = \psi(q_j, \alpha^r)$. Таким образом, для самонастраивающегося автомата выходная буква в любой момент $t \geqslant r_0$ не зависит от начального состояния автомата. Пример самонастраивающегося автомата приведен на рис. 1.17. У этого автомата можно положить $r_0 = 3$. Самонастраивающиеся автоматы находят применение в теории кодирования.

Автомат $\mathfrak{A}$ называется **автоматом без потери информации**, если для любого состояния $q \in Q$ и любых двух различных слов α_1^r и α_2^r; $\alpha_1^r, \alpha_2^r \in A^*$ имеет место $\overline{\psi}(q, \alpha_1^r) \neq \overline{\psi}(q, \alpha_2^r)$. Автомат без потери информации реализует, таким образом, в заданном начальном состоянии q взаимно-однозначное отображение множества A^* на подмножество множества B^*. Пример автомата без потери информации приведен на рис. 1.18.

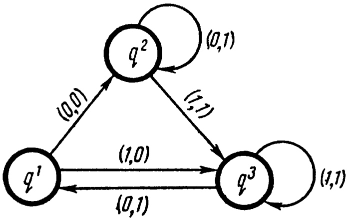

Рис. 1.17.

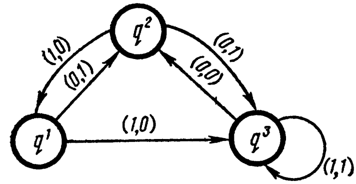

Рис. 1.18.

С произвольным автоматом $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ свяжем ориентированный граф G, называемый **графом переходов** этого автомата. Вершинами графа G служат состояния автомата $\mathfrak{A}$, причем ребро от вершины q_i к вершине q_j проводится в том и только том случае, когда существует $a \in A$, такое, что $q_j = \varphi(q_i, a)$. Нетрудно заметить, что граф $\mathfrak{A}$ получается из диаграммы Мура автомата $\mathfrak{A}$ отбрасыванием отметок, сопоставленных вершинам и ребрам этой диаграммы.

В зависимости от вида графа переходов автомата можно указать следующие важные классы автоматов.

Автомат $\mathfrak{A}$ называется **связным**, если для любых двух различных вершин q^1 и q^2 графа переходов G этого автомата существует такая последовательность $q^1 = v_0, v_1, ..., v_m = q^2$ вершин графа G, что любые две вершины v_i, v_{i+1} соединены ребром (без учета ориентации этого ребра).

Автомат $\mathfrak{A}$ называется **сильно связным**, если для любых двух различных вершин q^1 и q^2 графа переходов G автомата $\mathfrak{A}$ существует последовательность $q^1 = v_0, v_1, ..., v_m = q^2$ вершин графа G, такая, что при всех $i = 0, ..., m-1$ от v_i к v_{i+1} ведет ребро. Примеры сильно связного и связного, но не сильно связного автоматов приведены на рис. 1.19, а) и б).

Инициальный автомат $\mathfrak{A}_q$ называется **инициально связным**, если для любой отличной от q вершины q' графа переходов G автомата $\mathfrak{A}$ существует такая последовательность $q = v_0, v_1, ..., v_m = q'$ вершин графа G, что при всех $i = 0, 1, ..., m-1$ от v_i к v_{i+1} ведет ребро. Автомат $\mathfrak{A}$ называется **древовидным**, если его граф переходов представляет собой ориентированное от корня дерево, к концевым вершинам которого присоединены петли. Автоматы

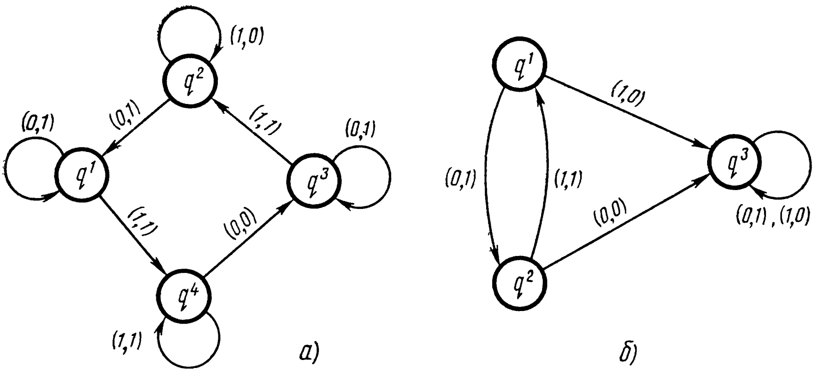

Рис. 1.19.

такого типа встречаются в некоторых задачах хранения информации. Пример древовидного автомата приведен на рис. 1.20.

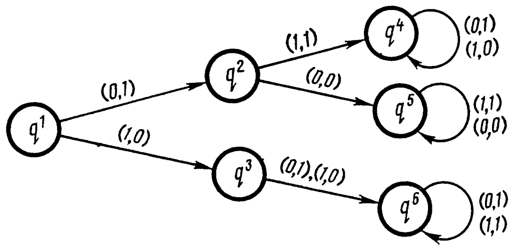

Рис. 1.20.

Естественно возникает следующий класс абстрактных конечных автоматов, описывающих работу реальных устройств, имеющих несколько входных и выходных каналов. Пусть $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, $A = A_1 \times \ldots \times A_r$; $Q = Q_1 \times \ldots \times Q_s$; $B = B_1 \times \ldots \times B_v$ — декартовы произведения соответствующих множеств. В этом случае элементы a, q, b множеств A, Q, B представимы в виде наборов $(a_1, \ldots, a_n)$; $(q_1, \ldots, q_s)$; $(b_1, \ldots, b_v)$. Если $q' = \varphi(q, a)$; $b' = \psi(q, b)$; $q' = (q_1', \ldots, q_s')$; $b' = (b_1', \ldots, b_v')$, то для подходящих функций $\varphi_1, \ldots, \varphi_s$, $\psi_1, \ldots, \psi_v$ имеем:

$$q_1' = \varphi_1(q_1, \ldots, q_s, a_1, \ldots, a_r),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$q_s' = \varphi_s(q_1, \ldots, q_s, a_1, \ldots, a_r),$$

$$b_1' = \psi_1(q_1, \ldots, q_s, a_1, \ldots, a_r),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$b_v' = \psi_v(q_1, \ldots, q_s, a_1, \ldots, a_r),$$

так что задание функций φ и ψ сводится к заданию соответствующих функций $\varphi_1, \ldots, \varphi_s, \psi_1, \ldots, \psi_v$. Автомат $\mathfrak{A}$ в этом случае называется **автоматом с r входами и v выходами.**

В случае инициального автомата $\mathfrak{A}_{q^0}$, где $\mathfrak{A}$ — рассмотренный автомат с r входами и v выходами; $q^0 = (q_1^0, \ldots, q_s^0)$, система определяющих автомат $\mathfrak{A}_{q^0}$ канонических уравнений с использованием функций $\varphi_1, \ldots, \varphi_s, \psi_1, \ldots, \psi_v$ может быть записана в виде:

$$
\begin{aligned}
&q_1(1) = q_1^0, \ldots, q_s(1) = q_s^0,\\
&q_1(t+1) = \varphi_1(q_1(t), \ldots, q_s(t), a_1(t), \ldots, a_n(t)),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&q_s(t+1) = \varphi_s(q_1(t), \ldots, q_1(t), a_1(t), \ldots, a_n(t)),\\
&b_1(t) = \psi_1(q_1(t), \ldots, q_1(t), a_1(t), \ldots, a_r(t)),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&b_v(t) = \psi_v(q_1(t), \ldots, q_s(t), a_1(t), \ldots, a_r(t)).
\end{aligned}
\qquad (*)
$$

Если $A_1 = \ldots = A_r = Q_1 = \ldots = Q_s = B_1 = \ldots = B_v = \{0, 1\}$, то для записи системы канонических уравнений могут использоваться формулы алгебры логики. Система канонических уравнений оказывается в этом случае одним из наиболее удобных способов задания инициальных конечных автоматов, позволяющим компактно описывать автоматы с большим числом состояний.

Пример 1. Пусть $r = s = v = 2$ и система канонических уравнений имеет вид:

$$
\begin{cases}
q_1(1) = q_2(1) = 1,\\
q_1(t+1) = q_2(t) \vee a_1(t)\\
q_2(t+1) = q_1(t)\bar{a}_1(t)a_2(t),\\
b_1(t) = \bar{a}_1(t) \vee q_1(t),\\
b_2(t) = q_1(t)q_2(t).
\end{cases}
$$

Данной системе уравнений соответствует инициальный автомат, диаграмма Мура которого представлена на рис. 1.21, где элементы (α_1, α_2) множеств A, Q, B обозначены посредством α_1, α_2 и начальное состояние отмечено звездочкой. Этот автомат, как нетрудно видеть, является инициально связным.

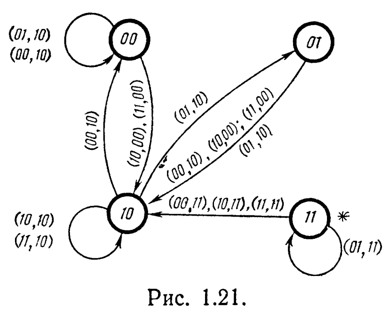

Рис. 1.21.

УПРАЖНЕНИЯ

1. Построить автомат Мура с наименьшим возможным числом состояний, удовлетворяющий условиям: $\bar{\psi}(q', 000)=101$; $\bar{\psi}(q' 1010)=1100$; $\bar{\psi}(q', 1100)=1110$.
2. Является ли самонастраивающимся автомат, определяемый диаграммой на рис 1.12?
3. Привести пример самонастраивающегося автомата без потери информации, у которого наименьшее r_0 (см. определение самонастраивающегося автомата) равно 3.
4. Выяснить, является ли инициально связным автомат, определяемый системой канонических уравнений:

$$\begin{cases} q_1(1) = q_2(1) = 0, \\ q_1(t+1) = q_1(t)\, a_1(t) \vee \bar{q}_2(t), \\ q_2(t+1) = q_1(t) \vee q_2(t) \vee a_2(t), \\ b_1(t) = \bar{a}_1(t) \vee q_2(t), \\ b_2(t) = q_1(t). \end{cases}$$

§ 4. ТИПЫ ПОВЕДЕНИЙ АВТОМАТОВ. АНАЛИЗ И СИНТЕЗ АВТОМАТОВ

В качестве главных свойств абстрактных автоматов выступают так называемые поведения. Выделяются следующие основные типы поведений автоматов.

Поведение-I инициального автомата $\mathfrak{A}_{q_0} = (A, Q, B, \varphi, \psi, q_0)$ образует словарная функция $f(\alpha^m)=\bar{\psi}(q, \alpha^m)$, отображающая множество A^* в B^*. Иногда вместо функции $f(\alpha^m)$ рассматривается функция $\bar{f}(\alpha^\infty)=\bar{\psi}(q, \alpha^\infty)$, отображающая A^∞ в B^∞. Если $\mathfrak{A}$ — автомат с n входами и k выходами: $A=A_1\times \ldots \times A_n$; $B=B_1\times \ldots \times B_k$, то слово $\alpha^m=a(1) \ldots a(m)$, $\alpha^m\in A^*$, определяется набором из слов $\alpha_1^m, \ldots, \alpha_n^m$; $\alpha_1^m = a_1(1), \ldots, a_1(m), \ldots, \alpha_n^m=a_n(1), \ldots, a_n(m)$, таких, что $a(i) = (a_1(i), \ldots, a_n(1))$, при всех $i=1, \ldots, m$. Аналогично, слово $\beta^m=b(1) \ldots b(m)$, $\beta^m\in B^*$, определяется набором $\beta_1^m, \ldots, \beta_k^m$; $\beta_1^m = b_1(1) \ldots b_1(m); \ldots ; \beta_k^m = b_k(1) \ldots b_k(m)$; $b(i) = (b_1(i), \ldots b_k(i))$ при $i=1, \ldots, m$. Слова α_j^m, β_j^m обозначаем $\mathrm{pr}_j(\alpha^m), \mathrm{pr}_j(\beta^m)$ и называем j-ми проекциями слов α^m, β^m. Если $\beta^m=f(\alpha^m)=\bar{\psi}(q, \alpha^m)$, то для подходящих функций $f_1(\alpha_1^m, \ldots, \alpha_n^m), \ldots, f_k(\alpha_1^m, \ldots, \alpha_n^m)$ имеем: $f(\alpha^m) = (f_1(\mathrm{pr}_1(\alpha^m), \ldots, \mathrm{pr}_n(\alpha^m)), \ldots, f_k(\mathrm{pr}_1\alpha^m), \ldots, \mathrm{pr}_n\alpha^m))$. Таким образом, для автоматов с n входами и k выходами поведение-I можно представлять набором k словарных функций, каждая из которых зависит от n аргументов. Если α^∞, β^∞ — сверхслова из A^∞, B^∞ соответственно; $\alpha^\infty=a(1)a(2) \ldots$; $\beta^\infty=b(1)b(2) \ldots$; $a(i) = (a_1(i), \ldots \ldots, a_n(i))$; $b(i) = (b_1(i), \ldots, b_k(i))$; $i=1, 2, \ldots$, то, обозначая посредством $\alpha_j^\infty = \mathrm{pr}_j(\alpha^\infty)$; $\beta_j^\infty = \mathrm{pr}_j(\beta^\infty)$ сверхслова $a_j(1)a_j(2) \ldots$ и $b_j(1)b_j(2) \ldots$, приходим к представлению функции $\bar{f}(\alpha^\infty)$ в виде k

определенных на сверхсловах n-местных функций $\overline{f}_1(\alpha_1^\infty, \ldots, \alpha_n^\infty)$, $\ldots, \overline{f}_k(\alpha_1^\infty, \ldots, \alpha_n^\infty)$.

Функции $f(\alpha^m)$, $f(\alpha^m)$ называются **конечно-автоматными функциями**, реализуемыми или вычисляемыми инициальным автоматом $\mathfrak{A}_q$. Инициальный автомат, рассмотрение которого осуществляется с точки зрения его поведения-I, называют **автоматом-преобразователем.**

Поведение-II. Выделим в инициальном автомате $\mathfrak{A}_q = (A, Q, B, \varphi, \psi)$ некоторое подмножество B', $B' \subseteq B$ и рассмотрим множество $L_{B'}$ слов в алфавите A, определяемое следующим образом:

$$L_{B'} = \{\alpha^m : \alpha^m \in A^*, \psi(q, \alpha^m) \in B'\}.$$

Множество $L_{B'}$ назовем **поведением-II** инициального автомата $\mathfrak{A}_q$ по отношению к подмножеству B', или **событием, представимым инициальным автоматом** $\mathfrak{A}_q$ с помощью подмножества B'. Поведение-II автомата $\mathfrak{A}_q$ представляет собой, таким образом, множество таких входных слов, на которые автомат $\mathfrak{A}_q$ реагирует появлением на его выходе сигнала из выделенного подмножества B'. Автомат $\mathfrak{A}_q$ выступает здесь как устройство, распознающее те или иные классы входных слов. Инициальный автомат, рассмотрение которого осуществляется с точки зрения его поведения-II, называют **автоматом-акцептором.**

Поведение-III. От рассмотрения инициального автомата $\mathfrak{A}_q$ как устройства, распознающего множества входных слов, можно перейти к рассмотрению $\mathfrak{A}_q$ как устройства, распознающего множества входных сверхслов. Если $\alpha^\infty = a(1)a(2)\ldots$ — некоторое входное сверхслово, перерабатываемое автоматом $\mathfrak{A}_q$ в выходное сверхслово $\beta^\infty = b(1)b(2)\ldots$, причем B' — множество всех выходных символов, бесконечное число раз встречающихся в сверхслове β^∞, то скажем, что автомат $\mathfrak{A}_q$ реагирует на входное сверхслово α^∞ посредством подмножества B' выходных символов. Пусть $N = \{B_1^*, \ldots, B_k^*\}$ — некоторый набор подмножеств множества B. Поведением-III инициального автомата $\mathfrak{A}_q$ по отношению к набору N называется множество S_N всех таких входных сверхслов, на которые автомат $\mathfrak{A}_q$ реагирует одним из подмножеств $B_1, \ldots, B_k$. Множество S_N называется также **сверхсобытием, представимым инициальным автоматом** $\mathfrak{A}_q$ **с помощью набора** N. Инициальный автомат, рассмотрение которого осуществляется с точки зрения его поведения-III, называют **автоматом-сверхакцептором**.

Поведением-IV инициального конечного автомата $\mathfrak{A}_q = (A, Q, B, \varphi, \psi, q)$ называется множество значений отображений $f: A^* \to B^*$; $f(\alpha) = \Psi(q, \alpha)$. Автомат $\mathfrak{A}_q$, рассматриваемый с точки зрения поведения-IV, называется **автоматом-перечислителем**. Такой автомат представляет собой устройство, перечисляющее при подаче на его вход всевозможных слов в алфавите A некоторое подмножество слов в алфавите B.

Поведением-V инициального конечного автомата $\mathfrak{A}_{q_0} = (A, Q, B,$

$\varphi, \psi, q_0)$ называется объект $(\mathfrak{A}'_{q'_0}, \pi)$, где $\mathfrak{A}'_{q'_0} = (B, Q', A, \varphi', \psi', q'_0)$ — инициальный конечный автомат Мура, π — последовательность наборов $(q_0, q'_0, a_0, b_0), (q_1, q'_1, a_1, b_1)\ldots$ таких, что $a_0 = \psi'(q'_0)$; $b_0 = \psi(q_0, a_0)$; $q_{i+1} = \varphi(q_i, a_i)$; $q'_{i+1} = \varphi'(q'_i, b_i)$; $a_{i+1} = \psi'(q'_{i+1})$; $b_{i+1} = \psi(q_{i+1}, a_{i+1})$. Последовательность π описывает работу системы, возникающей в результате отождествления выхода автомата $\mathfrak{A}_{q_0}$ со входом автомата $\mathfrak{A}'_{q'_0}$, а входа автомата $\mathfrak{A}_{q_0}$ — с выходом $\mathfrak{A}'_{q'_0}$. Для любого $i=0, 1, \ldots$ q_i есть состояние автомата $\mathfrak{A}_{q_0}$ в момент $t=i$; q'_i — состояние автомата $\mathfrak{A}'_{q'_0}$ в момент $t=i$; a_i — входной, b_i — выходной сигналы автомата $\mathfrak{A}_{q_0}$ в момент $t=i$. Указанное взаимодействие автоматов $\mathfrak{A}_{q_0}$ и $\mathfrak{A}'_{q'_0}$ можно рассматривать как модель процесса управления, в котором $\mathfrak{A}_{q_0}$ есть управляющее устройство, а $\mathfrak{A}'_{q'_0}$ — управляемое устройство. Автомат $\mathfrak{A}_q$, рассматриваемый с точки зрения его поведения-V, называется **управляющим автоматом**. Основными задачами, возникающими при изучении перечисленных типов поведений автоматов, оказываются задачи анализа и синтеза автоматов. Если выделен один из рассмотренных типов поведения автомата, то **задача анализа** конечного автомата заключается в нахождении по заданному автомату $\mathfrak{A}$ (либо $\mathfrak{A}_q$) тех или иных характеристик поведения этого автомата. Обратной к задаче анализа автомата является **задача синтеза** конечного автомата, заключающаяся в построении такого автомата $\mathfrak{A}$ (либо $\mathfrak{A}_q$), поведение которого обладает заданными характеристиками. Приведем примеры, иллюстрирующие некоторые простейшие задачи анализа и синтеза конечных автоматов.

Пример 1. Исследуем поведение-I автомата $\mathfrak{A}_{q^1}$, диаграмма которого приведена на рис. 1.22.

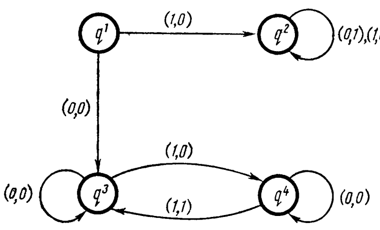

Рис 1.22

Пусть $\alpha^m = a(1)\ldots a(m)$; $\beta^m = f(\alpha^m)$. Если $a(1) = 1$, то автомат из состояния q^1 переходит в состояние q^2, в котором остается неограниченно долго. При этом слово β^m получается из слова α^m заменой в нем всех нулей на единицы и наоборот. Если же $a(1) = 0$, то автомат переходит из состояния q^1 в состояние q^3. Как видно из диаграммы, далее автомат будет совершать переходы между состояниями q^3 и q^4, меняя состояние при каждом появлении на входе символа 1. При этом появление на входе единицы с четным номером приводит к возникновению на выходе автомата символа 1, в прочих случаях на выходе автомата возникает символ 0. Таким образом, при $a(1) = 0$ слово β^m получается из α^m заменой всех «нечетных» единиц (т. е. таких $a(i) = 1$, для которых число единиц в слове $a(1)\ldots a(i)$ нечетно) на нули. Тем самым функция $f(\alpha^m)$ полностью описана.

Пример 2. Построим автомат $\mathfrak{A}_{q^1}$, реализующий следующее отображение $f: \{0, 1\}^* \to \{0, 1\}^*$,

$$f(\alpha^m) = \begin{cases} \alpha^m, \text{ если слово } \alpha^m \text{ не содержит отрезка вида } 0101; \\ a(1) \ldots a(i) 00 \ldots 0, \text{ если } \alpha^m = a(1) \ldots a(m), \text{ причем} \\ a(i-3)\, a(i-2)\, a(i-1)\, a(i) = 0101 \text{ — первое вхождение} \\ \text{в слово } \alpha^m \text{ отрезка } 0101. \end{cases}$$

Автомат, реализующий указанное отображение, распознает первое появление во входной последовательности отрезка вида 0101 и после появления такого отрезка выдает на выходе одни лишь нули. Для распознавания отрезка 0101 достаточно, например, запоминать последние три выходных символа, что означает наличие у автомата 8 состояний, соответствующих всевозможным тройкам 000,001, ..., 111. Если в состоянии, соответствующем тройке 010, на вход автомата подается символ 1, то автомат переходит в особое состояние, которое далее не изменяется и в котором на выходе автомата появляются только нули. Нетрудно заметить, что в качестве начального состояния автомата можно выбрать, например, состояние, соответствующее тройке 111. Диаграмма переходов автомата $\mathfrak{B}_{q^1}$ работающего указанным образом, приведена на рис. 1.23, где состояния обозначены посредством 000,001, ..., 111,0,

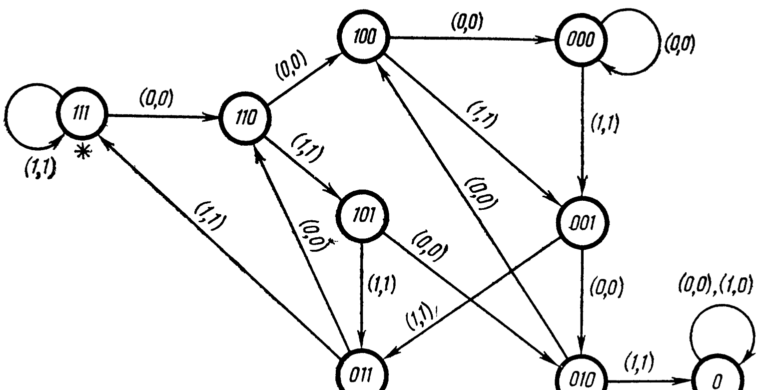

Рис. 1.23.

причем q^1 есть 111 (это состояние отмечено звездочкой). Построенный автомат $\mathfrak{B}_{q^1}$, не является минимальным по числу состояний; чтобы убедиться в этом, рассмотрим состояния 100 и 000. Если один из экземпляров автомата $\mathfrak{B}$ находится в состоянии 000, а другой — в состоянии 100, причем на входы этих автоматов подается символ 0, то автоматы переходят в одно и то же состояние 000; при этом на выходах их возникает один и тот же символ 0. Аналогично, при подаче на входы этих автоматов символа 1 они переходят в одно и то же состояние 001, а на выходах их появляется символ 1. Таким образом, в состояниях 000 и 100 автомат обнаруживает одинаковое поведение-I (в таких случаях говорят, что состояния 000 и 100 **неотличимы**). Преобразуем диаграмму автомата $\mathfrak{B}_{q'}$ удалив состояние 000 и заменив каждую стрелку, ведущую к состоянию 000 от некоторого другого состояния на

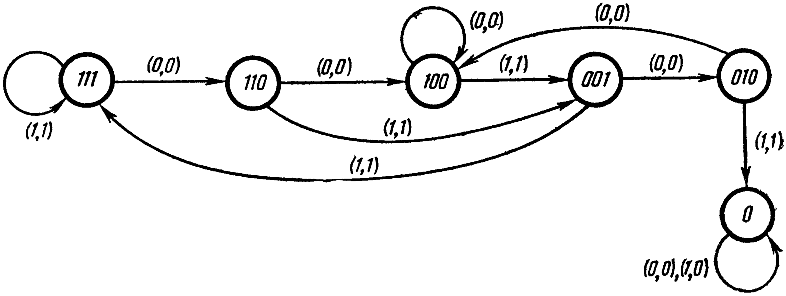

Рис. 1.24.

аналогичную стрелку, ведущую к состоянию 100; так как состояния 000 и 100 неотличимы, то, очевидно, в результате получится диаграмма некоторого автомата $\mathfrak{B}'_{q^1}$, реализующего то же отображение, что и автомат $\mathfrak{B}_{q^1}$. Из рис. 1.23 видно, что неотличимыми являются также состояния 111 и 011; 001 и 101. Удалив аналогично указанному выше также состояния 011 и 101, получим диаграмму на рис. 1.24. В этой диаграмме снова находим неотличимые состояния 110 и 100; удалив состояние 100, получаем диаграмму некоторого автомата $\mathfrak{A}_{q^1}$, которая уже не допускает дальнейшего упрощения. Эта диаграмма приведена на рис. 1.25.

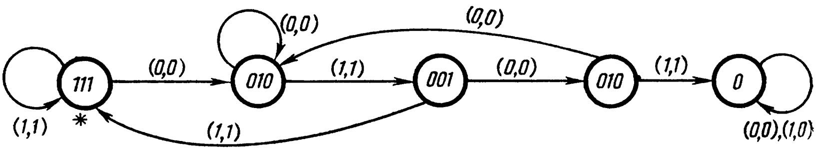

Рис. 1.25.

Пример 3. Пусть $\mathfrak{A}_{q^1}$ — инициальный автомат, диаграмма которого приведена на рис. 1.26, $\mathfrak{A}_{q^1} = (\{0, 1\}, \{q^1, q^2, q^3\}, \{0, 1\}, \psi, \psi, q^1)$; $B' = \{1\} \subseteq B = \{0, 1\}$. Найдем событие, представимое автоматом $\mathfrak{A}_{q^1}$ с помощью подмножества B'.

Нетрудно заметить, что сигнал 1 на выходе автомата $\mathfrak{A}$ появляется только тогда, когда $\mathfrak{A}$ находится в состоянии q^2 и на вход автомата $\mathfrak{A}_{q^1}$ подается символ 0. Из рис. 1.26 видно, что переход автомата $\mathfrak{A}_{q^1}$ в состояние q^2 происходит под действием слов вида $\underbrace{1\dots1}_{n_1}0\underbrace{1\dots1}_{m_1}0x_1\underbrace{1\dots1}_{n_2}0\underbrace{1\dots1}_{m_2}0x_2\dots\underbrace{1\dots1}_{n_k}0\underbrace{1\dots1}_{m_k}$, где $x_i \in \{0, 1\}$; n_i, $m_i \geqslant 0$; $k \geqslant 1$. Поэтому 1 на выходе автомата $\mathfrak{A}_q$ возникает при поступлении на вход этого автомата слов вида

$\underbrace{1\dots1}_{n_1}0\underbrace{1\dots1}_{m_1}0x_1\underbrace{1\dots1}_{n_2}0\underbrace{1\dots1}_{m_2}0x_2\dots\underbrace{1\dots1}_{n_k}0\underbrace{1\dots1}_{m_k}0$. Множество таких слов и образует искомое событие.

Пример 4. Пусть S — множество сверхслов в алфавите 0, 1, представимых в виде $p_1p_2p_3\dots$, где каждое слово p_i есть либо 01, либо 10. Построим инициальный автомат $\mathfrak{A}_{q^1}=(A, Q, B, \varphi, \psi, q_1)$, представляющий сверхсобытие S с помощью некоторого набора N подмножеств множества B. Проверка принадлежности сверхслова α^∞ множеству S сводится к представлению α^∞ в виде $p_1p_2p_3\dots$,

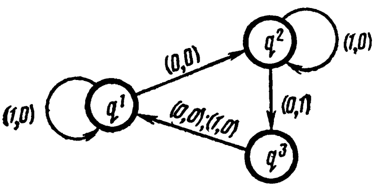

Рис 1.26.

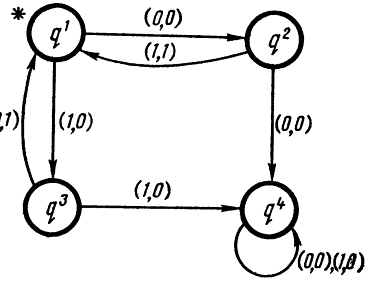

Рис. 1.27.

где p_i — слова длины 2, и к проверке включения $p_i\in\{01, 01\}$ ($i=1, 2, 3, \dots$). Такая процедура может быть реализована, например, при помощи автомата $\mathfrak{A}_{q^1}$, диаграмма переходов которого приведена на рис. 1.27.

Нетрудно видеть, что сверхслово, принадлежащее S, переводится этим автоматом в сверхслово 010101..., а любое другое сверхслово — в сверхслово вида 010101 ..., имеющее лишь конечное число единиц. Поэтому $\mathfrak{A}_{q^1}$ представляет сверхсобытие S с помощью набора ($N=\{\{1\}\}$.

Пример 5. Пусть $\mathfrak{A}_{q^1}$ — инициальный автомат, диаграмма которого приведена на рис. 1.28. Исследуем поведение-IV этого автома-

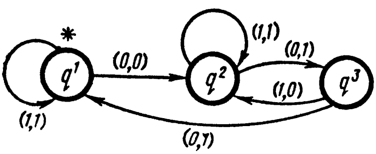

Рис. 1.28.

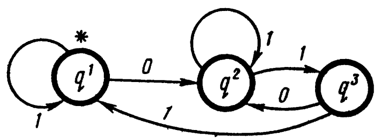

Рис. 1.29.

та, т. е. множество M всех таких слов в алфавите $\{0, 1\}$, которые могут появляться на выходе автомата $\mathfrak{A}_{q^1}$. Для описания множества M удобно перейти к указанной на рис. 1.29 диаграмме, полученной из диаграммы автомата $\mathfrak{A}_{q^1}$ отбрасыванием входных символов в парах, сопоставленных стрелкам этой диаграммы. Очевидно, M есть множество всех слов $b(1)\dots b(n)$, таких, что в диаграмме на рис. 1.29 существует последовательность переходов по стрелкам, отмеченным символами $b(1), \ldots, b(n)$, начинающая с вершины q^1. Анализ рис. 1.29 показывает, что M состоит из всех слов в алфавите $\{0, 1\}$, не содержащих идущих подряд двух нулей.

Пример 6. Пусть $\mathfrak{A}$ — автомат Мура, диаграмма которого приведена на рис. 1 30. Построим такой инициальный автомат $\mathfrak{B}_{\tilde{q}^1}$, что при взаимодействии автомата $\mathfrak{B}_{\tilde{q}^1}$ с любым инициальным автоматом $\mathfrak{A}_{qi}$; $i \in \{1, 2, 3, 4\}$, начиная с некоторого момента на выходе автомата $\mathfrak{A}_{q^i}$ начинают появляться только единицы. Если в начальный момент $t=1$ на выходе автомата $\mathfrak{A}_{q^i}$ имеется сигнал 1, то $i \in \{3, 4\}$. Пусть автомат $\mathfrak{B}_{\tilde{q}_1}$, получая в состоянии $\tilde{q}_1$ входной сигнал 1, выдает сигнал 0 и остается в состоянии $\tilde{q}_1$. При $i=3$ в этом случае уже достигается требуемое поведение автомата $\mathfrak{A}_{q^i}$ В случае $i=4$ к моменту времени $t=2$ автомат $\mathfrak{A}_{q^i}$ переходит в состояние q^1 и на выходе его появляется сигнал 0. Пусть автомат $\mathfrak{B}_{\tilde{q}^1}$, получая в состоянии $\tilde{q}^1$ входной сигнал 0, переходит в состояние $\tilde{q}^2$ и выдает выходной сигнал 1. Очевидно, после перехода автомата $\mathfrak{B}_{\tilde{q}^1}$ из состояния $\tilde{q}^1$ в состояние $\tilde{q}^2$ автомат $\mathfrak{A}$ может оказаться в одном из состояний q^2 и q^4, причем в первом случае на вход автомата $\mathfrak{B}_{\tilde{q}^1}$ поступит сигнал 0, а во втором — сигнал 1. Для получения требуемого поведения автомата $\mathfrak{A}$ достаточно теперь положить, что под действием входного сигнала 0 автомат $\mathfrak{B}_{\tilde{q}^1}$ переходит из состояния $\tilde{q}^2$ в состояние $\tilde{q}^1$, выдавая на выходе сигнал 0, а под действием входного сигнала 1 — остается в состоянии $\tilde{q}^2$, выдавая выходной сигнал 1. Диаграмма переходов автомата $\mathfrak{B}_{\tilde{q}_1}$ приведена на рис. 1.31.

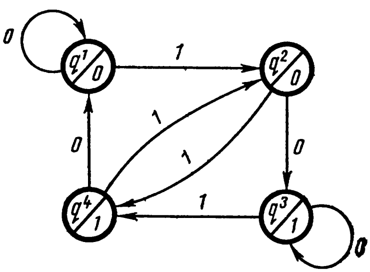

Рис 1 30

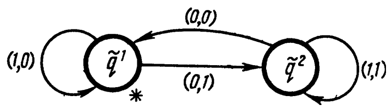

Рис 1 31.

УПРАЖНЕНИЯ

1. Является ли конечно-автоматной функция $f: \{0, 1\}^* \to \{0, 1\}^*$, определенная соотношениями: $f(a(1)a(2) \ldots a(2k)) = a(1)a(1)a(2)a(2) \ldots a(k)a(k)$; $f(a(1)a(2 \ldots (a(2k+1)) = a(1)a(1) \ldots a(k)a(k)a(k+1)$ $(k=0, 1, 2, \ldots)$?
2. Какие из следующих событий $S_1, \ldots S_5$ представимы в инициальных автоматах с помощью подмножеств выходных символов?

$$S_1 = \{0,\underbrace{1 \ldots 1}_{k}, 0, \text{ где } k = 0, 1, 2 \ldots\};$$

$$S_2 = \{\underbrace{0 \ldots 0}_{k}\ \underbrace{1 \ldots 1}_{k},\ \text{где } k = 0, 1, 2 \ldots\};$$

$$S_3 = \{010,\ 11,\ 1001,\ 0110\};$$

$$S_4 = \{\underbrace{1 \ldots 1}_{k_1}\ \underbrace{0 \ldots 0}_{l_1}\underbrace{1 \ldots 1}_{k_2}\underbrace{0 \ldots 0}_{l_2} \ldots \underbrace{1 \ldots 1}_{k_s}\underbrace{0 \ldots 0}_{l_s},\ \text{где } s = 0, 1, 2 \ldots;$$

каждое k_i не менее 2, а каждое l_i делится на 2};

$$S_5 = \{\underbrace{1 \ldots 1}_{k},\ \text{где } k \text{ — простое число}\}.$$

3. Описать сверхсобытия, представимые инициальным автоматом из примера 4 с помощью наборов $N_1 = \{\{0\}\}$; $N_2 = \{\{0\}, \{0, 1\}\}$; $N_3 = \{\{1\}, \{01\}\}$.
4. Описать множество всех слов в алфавите $\{0, 1\}$, которые могут появиться на выходе автомата $\mathfrak{A}_{q^1}$ из примера 3.
5. Найти число различных слов длины n, которые могут появиться на выходе автомата $\mathfrak{A}_{q^1}$ из примера 1.
6. Инициальный автомат Мура $\mathfrak{A}_q$ задан системой канонических уравнений:

$$q_1(1) = 0;\ q_2(1) = 1,$$

$$q_1(t+1) = (q_1(t) \vee \bar{q}_2(t))\, a_2(t),$$

$$q_2(t+1) = \bar{q}_1(t)\, a_1(t),$$

$$b_1(t) = q_1(t)\, q_2(t).$$

Построить такой инициальный автомат $\mathfrak{B}_{q^1}$ что при взаимодействии автомата $\mathfrak{B}_{q^1}$ с автоматом $\mathfrak{A}_q$ единицы на выходе автомата $\mathfrak{A}_q$ появляются с наибольшей возможной частотой. Каково наименьшее возможное число состояний автомата $\mathfrak{B}_{q^1}$?

§ 5. НЕКОТОРЫЕ МОДИФИКАЦИИ АБСТРАКТНЫХ КОНЕЧНЫХ АВТОМАТОВ

Сформулированная в § 1 содержательная модель абстрактного конечного автомата основывалась на ряде предположений относительно работы исследуемого реального устройства. Обобщая некоторые из этих предположений, можно получать различные модификации понятия абстрактного конечного автомата. Важнейшие такие модификации и будут рассмотрены в настоящем параграфе.

В § 1 предполагалось, что работа исследуемого реального устройства наблюдается лишь в выделенные моменты времени t_1, t_2, $t_3, \ldots$, причем изменения, происходящие с устройством между наблюдаемыми моментами, с точностью до несущественных деталей определяются информацией, получаемой в моменты t_1,

t_2, t_3, ... Одно из возможных обобщений этого допущения заключается в рассмотрении двух независимых последовательностей моментов времени t_1, t_2, t_3, ... и τ_1, τ_2, τ_3, ..., таких, что в моменты t_1, t_2, t_3, ... наблюдаются поступающие на вход устройства внешние сигналы, а в моменты τ_1, τ_2, τ_3, ... — наблюдаются выходные реакции устройства. При этом, как и ранее, состояние устройства в момент времени t_{n+1} предполагается однозначно определяющимся по входному сигналу и состоянию устройства в момент времени t_n, а выходные сигналы в моменты $\tau_s, \tau_{s+1}, ..., \tau_{s+l}$, такие, что $t_n \leqslant \tau_s < \tau_{s+1} < ... < \tau_{s+l} < t_{n+1}$, также однозначно определяются по входному сигналу и состоянию устройства в момент времени t_n. Возникающая в результате модель представляет собой содержательную модель **абстрактного конечного асинхронного автомата.**

Абстрактный конечный асинхронный автомат определяется как объект $\mathfrak{A}=(A, Q, B, \varphi, \psi)$, где A, Q, B — конечные множества, называемые, как и обычно, множествами входных символов, состояний и выходных символов асинхронного автомата $\mathfrak{A}$; φ — функция переходов, φ: $Q \times A \to Q$; ψ — функция выходов, $\psi: Q \times A \to B^*$. Если асинхронный автомат $\mathfrak{A}$ находится в начальном состоянии q_0 и на его вход поступает слово $\alpha^m = a(1) ... a(m)$, $\alpha^m \in A^*$, то автомат $\mathfrak{A}$ последовательно переходит в состояния $q_1 = \varphi(q_0, a(1)), ..., q_m = \varphi(q_{m-1}, a(m))$ и на его выходе возникает слово $\beta^r = \psi(q_0, a(1))\psi(q_1, a(2)), ..., \psi(q_{m-1}, a(m))$, где r — сумма длин слов $\psi(q_i, a(i+1))$; $i=0, ..., m-1$. Заметим, что некоторые слова $\psi(q_i, a(i+1))$ могут быть пустыми. Асинхронные автоматы реализуют, таким образом, преобразования слов из A^* в слова из B^*, при которых длина слова может изменяться. В частности, асинхронный автомат может заменять каждый символ $a(i)$ слова $\alpha = a(1) ... a(m)$ на кодирующее этот символ слово в алфавите B; выделять подслова слова α, заменяя их на отдельные символы алфавита B и выполнять ряд других преобразований слов, встречающихся в теории кодирования. Для задания асинхронных автоматов можно использовать таблицы и диаграммы, отличающиеся от соответствующих таблиц для обычных абстрактных конечных автоматов лишь заменой встречающихся в них символов алфавита B на слова в алфавите B. В качестве примера абстрактного конечного асинхронного автомата $\mathfrak{A}$ рассмотрим автомат, диаграмма которого приведена на рис. 1.32. Этот автомат, находясь в начальном состоянии q^1, перерабатывает, например, слово 11111 в пустое слово, а слово 10010000 — в слово 11010000000.

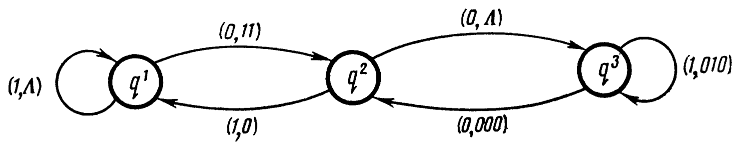

Рис. 1.32.

Другая возможная модификация понятия абстрактного конечного автомата возникает, если разбивать множество допустимых значений параметров, описывающих работу реального устройства, не на конечное, а на бесконечное число классов. В этой ситуации приходим к так называемому **абстрактному бесконечному** автомату $\mathfrak{A}=(A, Q, B, \varphi, \psi)$, где A, Q, B — уже, вообще говоря, бесконечные множества входных символов, состояний и выходных символов, φ и ψ — функции переходов и выходов, $\varphi: Q\times A\to Q$; $\psi: Q\times A\to B$. Увеличение мощности алфавитов расширяет вычислительные возможности автоматов. Так, например, если конечные автоматы реализуют ограниченно-детерминированные функции (см. § 1 гл. II), то с помощью бесконечных автоматов можно реализовать любую детерминированную функцию (см. § 1 гл. II). Более того, с помощью бесконечных автоматов может быть описано функционирование остальных модификаций понятия автомата. Вместе с тем большая общность понятия бесконечного автомата снижает его содержательное значение, так что в основном изучаются лишь специальные подклассы бесконечных автоматов, связанные с конкретными моделями управляющих систем.

Большое число различных модификаций абстрактного конечного автомата связано с отказом от требования детерминированности автомата, заключающегося в возможности однозначного определения состояния автомата в момент $t+1$ и выходного сигнала в момент t по состоянию автомата и входному сигналу, наблюдаемым в момент t. Первой из таких модификаций является **вероятностный автомат**, представляющий собой объект $\mathfrak{A}=(A, Q, B, \varphi, \psi)$, где A, Q, B — конечные алфавиты, имеющие тот же смысл, что и у абстрактного конечного автомата, а φ и ψ — случайные функции, отображающие $Q\times A$ в Q и B соответственно и задаваемые системами вероятностных мер $\varphi_{q,a}$, $\psi_{q,a}$, определенных для любых q из Q и a из A соответственно на множествах Q и B. Величина $\varphi_{q,a}(q')$ интерпретируется как вероятность того, что автомат $\mathfrak{A}$ из состояния q под действием входного сигнала a перейдет в состояние q'; величина $\psi_{q,a}(b)$ — как вероятность того, что при подаче символа a на вход автомата $\mathfrak{A}$, находящегося в состоянии q, на выходе этого автомата появится символ b. Пусть

$$A=\{a_1, ..., a_m\};\ Q=\{q_1, ..., q_n\};\ B=\{b_1, ..., b_p\}.$$

Тогда для задания мер $\varphi_{q,a}$, $\psi_{q,a}$ могут быть использованы так называемые **стохастические матрицы** $M(a_1), ..., M(a_m)$, $N(a_1), ..., N(a_m)$; $M(a_k)=\|q_{ij}(a_k)\|$ — матрица размера $n\times n$, у которой $q_{ij}(a_k)=\varphi_{q_i,a_k}(q_j)$; $N(a_k)=\|b_{ij}(a_k)\|$ — матрица размера $n\times p$, у которой $b_{ij}(a_k)=\psi_{q_i,a_k}(b_j)$.

В том случае, когда вероятностные меры φ, ψ принимают только два значения 0 и 1, понятие вероятностного автомата фактически совпадает с понятием абстрактного конечного автомата. Подобно абстрактным конечным автоматам, вероятностные автоматы по характеру поведения разделяются на преобразователи и акцепторы. В первом случае в соответствии с функционированием вероятностный автомат преобразует входные слова с некоторыми вероятностями в выходные слова и в слова в алфавите состояний. Эти вероятности для слов одинаковой длины образуют вероятностную меру, так что указанные поведения можно рассматривать как задание счетной системы таких мер. Во втором случае задается подмножество $B' \subseteq B$ выходного алфавита и число λ из отрезка $[0, 1]$, называемое **точкой сечения.** Событие, представимое вероятностным акцептором ($\mathfrak{A}$, B', λ), состоит из всех слов в алфавите A, под действием которых на выходе автомата с вероятностью, не меньшей λ, появляется символ из множества B'. В отличие от конечных автоматов, при помощи вероятностных автоматов представим континуальный класс событий. Более того, уже один вероятностный автомат при варьировании λ может представлять континуальный класс событий. В случае же однобуквенного входного алфавита каждый вероятностный автомат представляет лишь счетный класс событий, содержащий, вообще говоря, и события, не представимые в конечных автоматах. Число λ из отрезка $[0, 1]$ называется **изолированной точкой сечения** для данного вероятностного автомата, если существует такое положительное число δ, что для любого входного слова вероятность появления на выходе автомата под действием этого слова символа из B' отличается от λ не менее чем на δ. В случае, если точка сечения является изолированной, событие, представимое вероятностным автоматом, представимо также и конечным автоматом.

Большая часть понятий и задач, характерных для конечных автоматов, может быть перенесена в различных вариантах и на вероятностные автоматы. При этом часто сохраняются свойства, присущие конечным автоматам. Например, можно так ввести понятие неотличимости состояний вероятностного автомата, что сохранятся некоторые теоремы об отличимости состояний простыми экспериментами. Вместе с тем в отличие от конечных автоматов, для которых минимальная форма автомата определена с точностью до изоморфизма однозначно, для данного вероятностного автомата может существовать континуум эквивалентных минимальных форм. Следующей модификацией понятия абстрактного конечного автомата является так называемый **недетерминированный автомат**, представляющий собой объект (A, Q, B, χ), где A, Q, B — алфавиты, имеющие прежний смысл, а $\chi \subseteq Q \times A \times Q \times B$ — отношение переходов-выходов. В том случае, когда отношение χ является функцией, отображающей $Q \times A$ в $Q \times B$, недетерминированный автомат называется детерминированным и фактически совпадает с абстрактным конечным автоматом, поскольку в этом случае функцию χ можно рассматривать как пару функций φ, ψ, отображающих $Q \times A$ в Q и B соответственно. В отличие от конечного автомата, **инициальный не-**

детерминированный автомат $\mathfrak{A}_{Q_1}$ имеет несколько начальных состояний, образующих подмножество Q_1 множества Q. Под поведением автомата $\mathfrak{A}_{Q_1}$ обычно понимают одно из следующих обобщений поведения конечного автомата.

1. Вместо функции f автомат $\mathfrak{A}_{Q_1}$ реализует отношение f', состоящее из всех пар слов $(a(1)\dots a(n),\ b(1),\dots,b(n))\in A^*\times B^*$, таких, что существуют состояния $q(1),\ q(2),\dots,q(n+1)$, где $q(1)\in Q_1$ и при любом $i=1,\ 2,\dots,n$ имеет место $(q(i),\ a(i),\ q(i+1),\ b(i))\in\chi$.

2. Инициальный недетерминированный автомат $\mathfrak{A}_{Q_1}$, у которого выделено множество B', $B'\subseteq B$, представляет событие L, состоящее из всех слов $a(1)\dots a(n)\in A^*$, таких, что существуют слова $b(1)\dots b(n)\in B^*$, $q(1)\dots q(n+1)\in Q^*$, где $q(1)\in Q_1$; $b(n)\in\in B'$; $(q(i),a(i),\ q(i+1),\ b(i))\in\chi$ при всех $i=1,\ 2,\dots,n$. Класс событий, представимых недетерминированными автоматами, совпадает с классом событий, представимых конечными автоматами, т. е. относительно данного типа поведений эти автоматы эквивалентны. В то же время бо́льшая общность понятия недетерминированного автомата проявляется в том, что для представления некоторых событий с помощью недетерминированного автомата требуется меньшее число состояний. Существуют события, представимые недетерминированными автоматами с m состояниями и представимые конечными автоматами с 2^m состояниями, причем никакие конечные автоматы с меньшим числом состояний не представляют эти события.

Специальный подкласс недетерминированных автоматов образуют так называемые **частичные** автоматы, у которых отношение χ является частичной функцией, отображающей множество $Q\times A$ в $Q\times B$.

Наконец, рассматривается еще одна модификация конечного автомата — **нечеткие автоматы**. Такие автоматы получаются в результате замены функций переходов и выходов нечеткими отношениями. **Нечеткое подмножество** множества M задается функцией, отображающей M в отрезок $[0,1]$. Таким образом, роль функций переходов и выходов в нечетком автомате играют функции, отображающие множества $Q\times A\times Q$ и $Q\times A\times B$ в отрезок $[0,\ 1]$, где Q — множество состояний, A — входной алфавит, B — выходной алфавит. Для нечетких автоматов естественно обобщаются основные понятия и задачи, характерные для конечных автоматов; в частности, рассматриваются задачи представления нечетких событий и реализации нечетких отношений. Нечеткие автоматы являются математическими моделями некоторых распознающих устройств и используются в задачах распознавания образов.

Глава II
АВТОМАТЫ КАК ПРЕОБРАЗОВАТЕЛИ

§ 1. ОГРАНИЧЕННО-ДЕТЕРМИНИРОВАННЫЕ ФУНКЦИИ

Как отмечалось в § 4 гл. I, с каждым конечным инициальным автоматом $\mathfrak{A}_2=(A, Q, B, \varphi, \underline{\psi}, q_0)$ связано реализуемое этим автоматом отображение $f(\alpha^r)=\overline{\psi}(q_0, \alpha^r)$, определенное на словах $\alpha^r \in A^*$ и принимающее значения на множестве B^*. В этой связи естественно возникает задача описания всех таких отображений $f: A^* \to B^*$, которые могут быть реализованы в указанном смысле при помощи конечного автомата. Легко видеть, что произвольное реализуемое конечным автоматом отображение $f(\alpha^r)= =\overline{\psi}(q_0, \alpha^r)$ обладает следующими свойствами:

(1) для любого слова α^r, $\alpha^r \in A^*$, $|f(\alpha^r)|=r$;

(2) для любых слов α_1^r и α_2^r из A^* и любого l, $1 \leqslant l \leqslant r$, если

$$\underline{\overline{\alpha_1^r}}\Big|_l = \underline{\overline{\alpha_2}}\Big|_l, \text{ то } \underline{\overline{f(\alpha_1^r)}}\Big|_l = \underline{\overline{f(\alpha_2^r)}}\Big|_l.$$

Функции $f: A^* \to B^*$, обладающие свойствами (1) и (2), будем называть **детерминированными функциями** (д. функциями).

Для заданных слова $\alpha_1^{r_1}$ из A^* и д. функции $f: A^* \to B^*$ определим функцию $f_{\alpha_1^{r_1}}: A^* \to B^*$, которую назовем **остаточной** для функции f. Пусть $\alpha_1^{r_1}$ является началом слова $\alpha_2^{r_2}$, $r_2 \geqslant r_1$, тогда через $\alpha_2^{r_2}/\alpha_1^{r_1}$ обозначим конец слова $\alpha_2^{r_2}$, который образуется после удаления из $\alpha_2^{r_2}$ его начала $\alpha_1^{r_1}$. По определению полагаем

$$f_{\alpha_1^{r_1}}(\alpha^r) = f(\alpha_1^{r_1}\alpha^r)/f(\alpha_1^{r_1}).$$

Если функция $f: A^* \to B^*$ реализуется инициальным конечным автоматом $\mathfrak{A}_{q_0} = (A, Q, B, \varphi, \psi, q_0)$, $f(\alpha^r) = \tilde{\psi}(q_0, \alpha^r)$, то, как нетрудно заметить, $f_{\alpha_1^{r_1}}(\alpha^r) = \tilde{\psi}(\varphi(q_0, \alpha_1^{r_1}), \alpha^r)$. Таким образом, все остаточные функции $f_{\alpha_1^{r_1}}(\alpha^r)$ реализуются инициальными конечными автоматами, получающимися при выборе различных начальных состояний у автомата $\mathfrak{A} = (A, Q, B, \varphi, \psi)$. Это означает, что произвольная функция $f: A^* \to B^*$, реализуемая конечным автоматом, обладает следующим свойством:

(3) число различных остаточных функций $f_{\alpha_1^{r_1}}(\alpha^r)$ конечно. Функции $f: A^* \to B^*$, обладающие свойствами (1), (2) и (3), будем называть **ограниченно-детерминированными функциями** (о.-д. функциями). Число функций, остаточных для о.-д. функции f, называем **весом** о.-д. функции f.

Для наглядности описания о.-д. функций удобно использовать геометрический язык так называемых **информационных деревьев.** Информационное дерево в алфавитах A и B строится следующим образом. Верхняя полуплоскость разбивается параллельными прямыми на счетное число полос, называемых **ярусами.** На первой снизу прямой выбирается точка (**корень дерева**), и из нее откладывается пучок из m $(m=|A|)$ стрелок, концы которых упираются в следующую прямую. Эти стрелки образуют первый ярус дерева. Затем из конца каждой из построенных стрелок (**вершины дерева**) откладывается такой же пучок стрелок, упирающихся в третью прямую, при этом строящиеся пучки не должны пересекаться, так получается второй ярус. Это построение продолжается далее неограниченно. Стрелкам каждого пучка сопоставляются буквы из алфавита A таким образом, что i-й при отсчете слева направо соответствует буква a_i. Слову α^r, $\alpha^r \in A^*$, соответствует в информационном дереве последовательность стрелок, взятых из первого, второго, третьего и т. д. ярусов до r-го яруса включительно так, что при $\alpha^r = a(1)a(2)\ldots a(r)$ по букве $a(1)$ выбирается соответствующая ей стрелка, затем из того пучка, куда упирается эта стрелка, выбирается стрелка второго яруса, соответствующая букве $a(2)$, и т. д. На рис. 2.1 приведен фрагмент такого дерева.

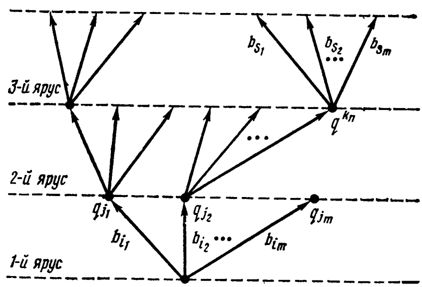

Рис. 2 1.

С помощью деревьев можно задавать отображения слов в алфавите A в слова в алфавите B следующим образом. Произвольным образом припишем каждой стрелке информационного дерева какую-нибудь букву из алфавита B и каждому слову α^r из A^* с помощью полученного, как говорят, нагруженного дерева (в дальнейшем для краткости — просто дерева), сопоставим слово β^r из B^*, образованное той последовательностью букв из B, которая возникает при прохождении последовательности стрелок, соответствующей слову α^r, начиная с первого яруса. Ясно, что полученное отображение является детерминированным. Верно, очевидно, и обратное, т. е. всякое детерминированное отображение может быть задано с помощью нагруженного дерева. Таким образом, язык нагруженных деревьев адекватен языку детерминированных функций. На рис. 2.1 приведен фрагмент такого дерева.

Выясним, что соответствует остаточным функциям в нагруженном дереве, которое однозначно определяется заданной д. функцией. Назовем две вершины дерева, лежащие в i-м и j-м ярусах, $i<j$, соединимыми, если существует последовательность стрелок в дереве, такая, что конец каждой стрелки является началом следующей за ней, причем началом первой из них является наша вершина из i-го яруса, а концом последней наша вершина из j-го яруса. Назовем **поддеревом** с корнем в некоторой вершине нашего дерева ту его часть, которая получается удалением из него всех вершин и стрелок, их соединяющих, таких, что ни одна из указанных вершин не соединима с нашей вершиной. Нетрудно видеть, что поддерево соответствует как раз остаточной функции g_{α^r}, такой, что последовательность стрелок, соединяющая корень дерева с корнем поддерева, соответствует слову α^r. Отношение совпадения поддеревьев заданного дерева разбивает множество всех его поддеревьев на классы эквивалентности. Пусть $q^1, q^2, \ldots, q^n, \ldots$ — их номера. Припишем каждой вершине нашего дерева букву q^n в том случае, если из нее исходит поддерево из класса под номером q^n. Нетрудно видеть, что если каким-либо двум вершинам дерева приписана одна и та же буква q^n, то стрелкам, исходящим из этих вершин и соответствующим букве a^i, будет приписана одна и та же буква b^j, а вершинам, куда упираются эти стрелки, будет приписана одна и та же буква q^n. Таким образом, в каждом пучке буква b, приписанная стрелке, а также буква q', приписанная концу стрелки, являются функциями буквы q, приписанной вершине пучка, и той буквы a, которая соответствует самой стрелке, т. е. для некоторых функций ψ и φ имеет место $b=\psi(q, a)$, $q'=\varphi(q, a)$.

Таким образом, д. функция f может быть описана еще и следующим образом. Пусть $\alpha^r \in A^*$ и $\alpha^r = a(1)a(2)\ldots a(r)$, рассмотрим последовательность стрелок в дереве д. функции g, соответствующую слову α^r, и восстановим по ней последовательности $\varkappa^{r+1}$, $\varkappa^{r+1} \in Q^*$, $\varkappa^{r+1} = q(1)q(2)\ldots q(r+1)$, где $q(1)$ — буква q, приписанная корню дерева, и β^r, $\beta^r \in B^*$, $\beta^r = b(1)b(2)\ldots b(r)$. Нетрудно видеть, что для этих последовательностей при $t=1, 2, \ldots, r$ справедлива следующая система рекуррентных соотношений

$$(1) \qquad \begin{cases} q(1) = q, \\ q(t+1) = \varphi(q(t), a(t)), \\ b(t) = \psi(q(t), a(t)). \end{cases}$$

Таким образом, сопоставляя это задание с системой (*) из § 2 гл. I, мы видим, что в случае, когда д. функция является о.-д. функцией, она в то же время является и конечно-автоматной функцией, которая реализуется инициальным конечным абстрактным автоматом $\mathfrak{A}_q = (A, Q, B, \varphi, \psi, q)$.

В результате получаем, что класс всех функций $f: A^* \to B^*$, реализуемых конечными автоматами, совпадает с классом всех о.-д. функций; при этом конечный автомат с n состояниями реализует о.-д. функцию, вес которой не превосходит n, и любая о.-д. функция веса n может быть реализована конечным автоматом с n состояниями.

Из наших рассмотрений, в частности, вытекает возможность использования языка деревьев для задания инициальных конечных абстрактных автоматов. На рис. 2.2 приведен фрагмент дерева для автомата-задержки $\mathfrak{A}_{q_1} = (\{\alpha^1, \alpha^2\}, \{q^1, q^2\}, \{b^1, b^2\}, \varphi, \psi, q_1)$.

В заключение параграфа опишем еще одно свойство о.-д. функций, характеризующее их поведение на сверхсловах алфавита A. Сверхслово называется **периодическим с длиной периода T и предпериодом длины l**, если оно имеет вид $\alpha^\infty = a(1)a(2)\ \dots\ a(l)a(l+1)\ \dots\ a(l+T)a(l+T+1)\ \dots$, где $a(l+i) = a(l+i+T)$ при любом i, $i \geqslant 0$.

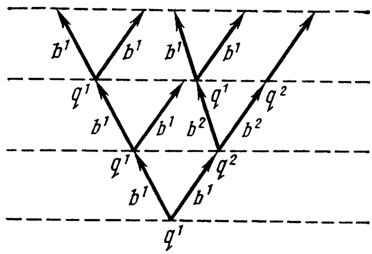

Рис 2.2

Пусть $f: A^* \to B^*$ есть некоторая о.д. функция. Если $\alpha^\infty = a(1)a(2)\ \dots$ — сверхслово из A^∞, то однозначно определяется сверхслово $\beta^\infty = b(1)b(2)\ \dots$ из B^*, такое, что для любого $l \geqslant 1$ имеет место $b(1)b(2)\ \dots\ b(l) = f(a(1)\ \dots\ a(l))$. Будем называть сверхслово β^∞ **результатом преобразования о.-д. функцией f сверхслова α^∞**. Имеет место следующее утверждение.

Теорема 2.1 [2]. Результат преобразования о.-д. функцией веса n периодического сверхслова с длиной периода T есть периодическое сверхслово с длиной периода ωT, где $\omega \leqslant n$.

Доказательство. Пусть сверхслово α^∞ имеет предпериод длины l и период длины T. Воспользуемся системой (1) для задания о.-д. функции f веса n и рассмотрим сверхслова

$$\alpha^\infty = a(1)a(2)\ \dots a(l)a(l+1)\ \dots a(l+T)a(l+T+1)\ \dots a(l+2T)\ \dots,$$
$$\varkappa^\infty = q(1)q(2)\ \dots q(l)q(l+1)\ \dots q(l+T)q(l+T+1)\ \dots q(l+2T)\ \dots,$$
$$\beta^\infty = b(1)b(2)\ \dots b(2)b(l+1)\ \dots b(l+T)b(l+T+1)\ \dots b(l+2T)\ \dots,$$

вычисленные с помощью системы (1). В последовательности столбцов

$$\begin{pmatrix} a(l+1) \\ q(l+1) \end{pmatrix}, \begin{pmatrix} a(l+T+1) \\ q(l+T+1) \end{pmatrix}, \begin{pmatrix} a(l+2T+1) \\ q(l+2T+1) \end{pmatrix}, \dots, \begin{pmatrix} a(l+iT+1) \\ q(l+iT+1) \end{pmatrix}, \dots$$

встречается не более n различных столбцов, поэтому среди них найдутся такие совпадающие между собой столбцы

$$\begin{pmatrix} a(l+jT+1) \\ q(l+jT+1) \end{pmatrix}, \begin{pmatrix} a(l+kT+1) \\ q(l+kT+1) \end{pmatrix},$$

для которых справедливы соотношения $k > j$ и $k - j \leqslant n$. Далее, так как по каждой паре $(a(t), q(t))$ с помощью системы (1) однозначно определяется пара $(b(t), q(t+1))$, то для любого $s \geqslant 0$

столбцы

$$\begin{pmatrix} a(l+jT+s+1) \\ q(l+jT+s+1) \\ b(l+jT+s+1) \end{pmatrix} \text{ и } \begin{pmatrix} a(l+kT+s+1) \\ q(l+kT+s+1) \\ b(l+kT+s+1) \end{pmatrix}$$

совпадают между собой.

Тогда для произвольного $t \geqslant l+jT+1$, представляя t в виде $l+jT+s+1$, получим, что столбцы

$$\begin{pmatrix} a(t) \\ q(t) \\ b(t) \end{pmatrix} \text{ и } \begin{pmatrix} a(t+(k-j)T) \\ q(t+(k-j)T) \\ b(t+(k-j)T) \end{pmatrix}$$

одинаковы, т. е. сверхслово β^∞ — периодическое с длиной периода $(k-j)T$. Теорема доказана.

Заметим, что если д. функция преобразует всякое периодическое сверхслово в периодическое сверхслово, то она, вообще говоря, не будет о.-д. функцией.

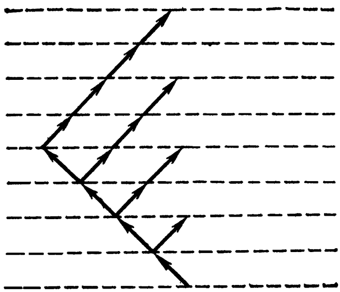

Рис. 2.3.

На рис. 2.3 приведен фрагмент дерева д. функции, которая всякое сверхслово отображает в периодическое сверхслово даже с периодом одной и той же длины, равной 1, но не является, очевидно, о.-д. функцией. Это дерево связано с алфавитами $A=\{0, 1\}$ и $B=\{0, 1\}$. Левая стрелка в пучке соответствует нулю, а правая — единице. Распределение нулей и единиц из алфавита B в этом дереве осуществляется так, что каждой стрелке из последовательности стрелок, соответствующей слову $\alpha_1^r\alpha_2^r$, где $\alpha_1^r = 00\ldots0$, $\alpha_2^r = 11\ldots1$, $r=1, 2, \ldots$, приписывается единица, а всем остальным стрелкам приписываются нули. На рис. 2.3 указан фрагмент дерева, содержащий только те стрелки, которым приписаны единицы из алфавита B. Для более точного описания преобразования автоматами периодических сверхслов введем понятие l-спектра периодичности автомата.

l-спектром периодичности инициального автомата $\mathfrak{A}_q$, где l — натуральное число, называется множество наименьших периодов сверхслов, возникающих при преобразовании автоматом $\mathfrak{A}_q$ сверхслов с наименьшим периодом l. **l-спектром периодичности класса K инициальных автоматов** называется объединение l-спектров периодичности автоматов класса K.

Теорема 2.2 [3]. l-спектр периодичности класса K_n всех инициальных автоматов, имеющих n состояний, есть множество чисел вида $l'n'$, где l' — натуральный делитель числа l и $1 \leqslant n' \leqslant n$.

Доказательство. Если сверхслово $\alpha^\infty = a(1)a(2)\ldots$ перерабатывается конечным автоматом $\mathfrak{A}_q \in K_n$ в сверхслово $\beta^\infty = b(1)b(2)\ldots$, то в силу теоремы 2.1 сверхслово β^∞ имеет период ωl, где $\omega \leqslant n$. Так как наименьший период τ сверхслова β^∞ является делителем любого периода этого сверхслова, то τ есть делитель числа ωl. Следовательно, τ представимо в виде $n'l'$; l' делит l, а n' делит ω и $n' \leqslant n$. Отсюда вытекает, что l-спектр периодичности класса K_n может состоять только из чисел указанного в условии теоремы вида. Покажем, что для любого числа вида $l'n'$, где l' делит l и $1 \leqslant n' \leqslant n$, существует периодическое сверхслово α^∞ с наименьшим периодом l и инициальный конечный автомат $\mathfrak{A}_{q_1} \in K_n$, такие, что $\mathfrak{A}_{q_1}$ перерабатывает α^∞ в сверхслово β^∞ с наименьшим периодом $l'n'$. В качестве входного алфавита автомата $\mathfrak{A}_{q_1}$ выберем множество $\{1, 2, \ldots, l\}$, а в качестве выходного алфавита — $\{0, 1\}$. Автомат $\mathfrak{A}_q$ определяется диаграммой на рис. 24, где посредством $\bar{i}$ обозначается остаток от деления числа i на l'.

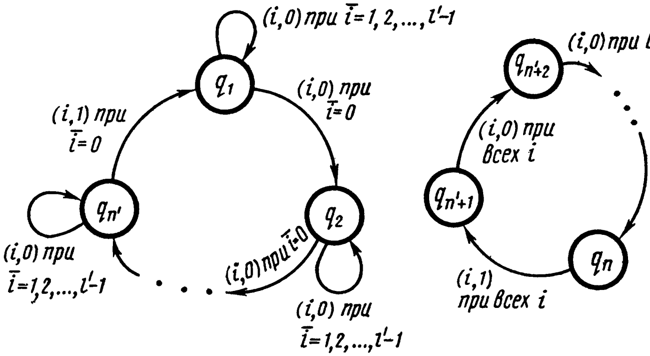

Рис. 2.4.

Как нетрудно проверить, построенный автомат $\mathfrak{A}_{q_1}$ перерабатывает сверхслово $\alpha^\infty = 12\ldots l12\ldots l\ldots$ в сверхслово $\beta^\infty = \underbrace{0\ldots01}_{l'n'}\underbrace{0\ldots01}_{l'n'}\ldots$, имеющее наименьший период $l'n'$. Теорема доказана.

УПРАЖНЕНИЯ

1. Пусть $A = B = \{0, 1, \ldots, 9\}$. Для произвольного слова $\alpha^r = a(1)\ldots a(r) \in A^*$ рассмотрим число a, имеющее десятичную запись $0a(1)\ldots a(r)$, и найдем десятичную запись $0b(1)\ldots b(q)$ числа a^2. Является ли детерминированной функция f: $A^* \to B^*$, определяемая соотношением: $f(a(1)\ldots a(r)) = b(1)\ldots b(r)$?
2. Пусть $A = B = \{0, 1\}$. Функция f_1: $A^* \to B^*$; $f_1(a(1)\ldots a(r)) = b(1)\ldots b(r)$ определяется следующим образом: $b(1) = 0$; $b(i) = a(i)\overline{a(i-1)} \vee \overline{a(i)}a(i-1)$ при $i > 1$. Функция f_2: $A^* \to B^*$; $f_2(a(1)\ldots a(r)) = b(1)\ldots b(r)$, определяется соотношениями: $b(1) = 0$; $b(i) = a(i) + b(i-1) \pmod 2$ при $i > 1$. Является ли функция f_1 остаточной для функции f_2?
3. Найти вес ограниченно-детерминированной функции $f =$

$=\{0,\ 1\}^*\to\{0,\ 1\}^*$; $f(a(1)\dots a(r))=b(1)\dots b(r)$, определяемой соотношениями: $b(1)=b(2)=1$; $b(i)=a(i-2)$ при $i\geqslant 3$.

4. Описать l-спектр периодичности автомата $\mathfrak{A}$ из примера 6 § 2 гл. I, у которого в качестве начального состояния выбрано состояние q^1.
5. Доказать, что если автомат $\mathfrak{A}$ сильно связный, и q^1, q^2 — два различных состояния автомата $\mathfrak{A}$, то l-спектры периодичности автоматов $\mathfrak{A}_{q^1}$ и $\mathfrak{A}_{q^2}$ совпадают.
6. Существует ли автомат $\mathfrak{A}_{q^0}=(\{0,1\}, Q, \{0,\ 1\}, \varphi, \psi, q_0)$, преобразующий каждое периодическое сверхслово с наименьшей длиной периода T ($T=1,\ 2,\ 3,\ \dots$) в периодическое сверхслово с наименьшей длиной периода $2T$?

§ 2. ЭКВИВАЛЕНТНОСТЬ АВТОМАТОВ

В предыдущем параграфе было установлено, что произвольная о.-д. функция f: $A^*\to B^*$ может быть реализована некоторым инициальным конечным автоматом $\mathfrak{A}_q=(A,\ Q,\ B,\ \varphi,\ \psi,\ q)$. Различные конечные автоматы могут определять, однако, одну и ту же о.-д. функцию. Так, автоматы $\mathfrak{A}_{q_1}$ и $\mathfrak{B}_{q_1'}$, приведенные на рис. 2.5., задают одну и ту же о.-д. функцию, преобразующую произвольное сверхслово $\alpha^\infty\in\{0,\ 1\}^\infty$, $\alpha^\infty=a(1)a(2)\dots$ в сверхслово $\beta^\infty\in\{0,1\}^\infty$, $\beta^\infty=b(1)b(2)b(3)\dots$, определяемое следующим образом:

а) если $a(i)=0$, то $b(i)=0$;

б) если $a(i)=1$, причем число единиц в последовательности $a(1),\ a(2),\dots,a(i)$ четно, то $b(i)=1$, в противном случае $b(i)=0$.

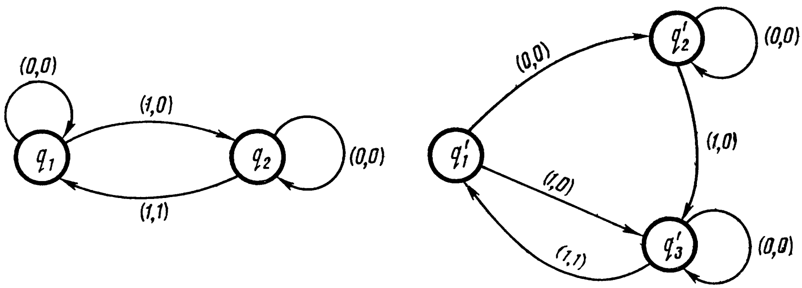

Рис. 2.5.

В связи с тем, что различные автоматы, рассматриваемые как преобразователи входных последовательностей, могут обладать одинаковым поведением, возникает ряд естественных отношений эквивалентности, связанных с функционированием автоматов. Эти отношения эквивалентности и будут рассмотрены в данном параграфе.

Пусть имеется два автомата $\mathfrak{A}=(A, Q, B, \varphi, \psi)$ и $\mathfrak{A}'=(A', Q', B', \varphi', \psi')$, будем говорить, что состояния q и q'; $q\in Q$, $q'\in Q'$ являются **неотличимыми**, если для любого слова α, $\alpha\in A^*$ имеет место $\overline{\psi}(q, \alpha)=\overline{\psi}'(q', \alpha)$. В противном случае говорим, что **состояния отличимые.** Неотличимость состояний q и q' обозначаем $q\sim q'$.

Теорема 2.3 [4]. Состояния q^i и q^j автомата $\mathfrak{A}=(A, Q, B, \varphi, \psi)$, имеющего хотя бы два отличимых состояния, неотличимы тогда и только тогда, когда для любого слова $\alpha^{|Q|-1}$ из A^* имеет место $\overline{\psi}(q^i, \alpha^{|Q|-1})=\overline{\psi}(q^j, \alpha^{|Q|-1})$.

Доказательство. Ясно, что если q^i и q^j неотличимы, то для любого слова $\alpha^{|Q|-1}$ справедливо $\overline{\psi}(q^i, \alpha^{|Q|-1})=\overline{\psi}(q^j, \alpha^{|Q|-1})$. Покажем, что справедливо и обратное утверждение, т. е. что в случае отличимости состояний q^i и q^j найдется слово $\alpha^{|Q|-1}$, такое, что $\overline{\psi}(q^i, \alpha^{|Q|-1})=\overline{\psi}(q^1, \alpha^{|Q|-1})$. Для этого на множестве Q введем отношение эквивалентности R_k; $k=1, 2, \ldots$, такое, что состояния q^i и q^j находятся в отношении R_k (обозначение: $q^iR_kq^j$) тогда и только тогда, когда для любого слова α^k из A^* имеет место $\overline{\psi}(q^i, \alpha^k)=\overline{\psi}(q^j, \alpha^k)$. В этом случае говорят также, что состояния q^i и q^j не отличимы словами длины k. Пусть P_k — разбиение множества Q на классы эквивалентности, индуцируемой отношением R_k. Ясно, что P_{k+1} является подразбиением P_k. Покажем, что если при некотором l имеет место $P_l=P_{l+1}$ и $P_l=\{Q_1, \ldots, Q_r\}$, то для любых состояний q^u и q^v из любого заданного класса Q_ω $\omega=1, 2, \ldots, r$ справедливо $q^u\sim q^v$. В самом деле, предположим, что это не так, и пусть в некотором классе Q_ω содержатся отличимые состояния q^u и q^v. Тогда найдется такое слово α, что $\overline{\psi}(q^u, \alpha)\neq\overline{\psi}(q^v, \alpha)$. Пусть α^t — кратчайшее такое слово. Очевидно, что $t>l+1$. Пусть $\alpha^t=a(1)a(2)\ldots a(l)a(l+1)\ldots a(l+s)$. Рассмотрим слово $\alpha_1^{l+1}=a(s)\ldots a(l+s)$, которое является окончанием слова α^t. Пусть $q'=\varphi(q^u, a(1)\ldots a(s-1))$ и $q''=\varphi(q^v, a(1)\ldots a(s-1))$. В силу того что α^t — кратчайшее слово из всех слов α, отличающих q^u и q^v, должно быть $q'R_lq''$. С другой стороны, так как $\overline{\psi}(q^u, \alpha^t)\neq\overline{\psi}(q^v, \alpha^t)$, то должно быть $\overline{\psi}(q', \alpha_1^{l+1})\neq\overline{\psi}(q'', \alpha_1^{l+1})$, т. е. неверно, что $q'R_{l+1}q''$. Таким образом, получаем, что $P_l\neq P_{l+1}$, а это противоречит нашему предположению.

Пусть построена последовательность $P_1, P_2, \ldots, P_l$, такая, что при $l>1$ каждое последующее разбиение является собственным подразбиением предыдущего и $P_{l+1}=P_l$. Заметим, что если в Q имеются хотя бы два отличимых состояния, то P_1 содержит не менее двух классов эквивалентности, отсюда следует, что $l\leqslant|Q|-1$. Пусть теперь q^u и q^v — произвольные состояния автомата $\mathfrak{A}$. В силу изложенного, для того чтобы установить их неотличимость, достаточно посмотреть, в какие классы разбиения P_l они попадают. Если они лежат в разных классах, то они отличимы, и даже словом длины $|Q|-1$, если же они попали в один и тот же класс, то они неотличимы. Теорема доказана.

Заметим, что приведенное доказательство конструктивное, так как оно фактически указывает алгоритм построения всех классов неотличимых между собой состояний. Отметим также, что в общем случае оценка $|Q|-1$ длин слов, осуществляющих распознавание отличимости состояний не может быть улучшена. В этом легко убедиться, рассмотрев в качестве примера автомат, диаграмма Мура которого приведена на рис. 2.6.

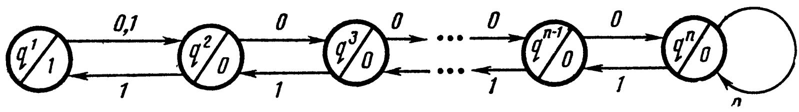

Рис 2.6.

Теорема 2.4 [4]. Состояния q и q' автоматов $\mathfrak{A}=(A, Q, B, \varphi, \psi)$ и $\mathfrak{A}'=(A, Q', B, \varphi' \psi')$, таких, что $Q\cap Q'=\varnothing$, неотличимы тогда и только тогда, когда для любого слова $\alpha^{|Q|+|Q'|-1}$ из A^* имеет место

$$\bar{\varphi}(q, \alpha^{|Q|+|Q'|-1}) = \bar{\varphi}(q', \alpha^{|Q|+|Q'|-1}).$$

Доказательство. Рассмотрим автомат $\mathfrak{B}=\mathfrak{A}+\mathfrak{A}'$. Если в этом автомате состояния q и q' отличимы, то, пользуясь теоремой 2.3, получаем утверждение нашей теоремы. Если состояния q и q' неотличимы, то утверждение очевидно. Теорема доказана.

Заметим, что так же, как в теореме 2.3, оценка теоремы 2.4, вообще говоря, неулучшаемая, в чем легко убедиться, взяв в качестве примера автоматы $\mathfrak{A}$ и $\mathfrak{A}'$, где диаграмма переходов автомата $\mathfrak{A}'$ приведена на рис. 2.6, а диаграмма переходов автомата $\mathfrak{A}'$ — на рис. 2.7, причем $m=|Q'|\geqslant|Q|=n$. В качестве состояний q и q' здесь берутся состояния q и $q^{1'}$.

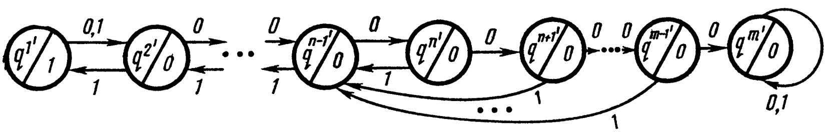

Рис 2.7

Автомат $\mathfrak{A}=(A, Q, B, \varphi, \psi)$ называется **слабо вложимым в** автомат $\mathfrak{A}'=(A, Q', B, \varphi', \psi')$ (обозначается $\mathfrak{A}\leqslant\mathfrak{A}'$), если для любого состояния $q, q\in Q$, и любого слова $\alpha, \alpha\in A^*$, найдется такое состояние $q', q'\in Q'$, что $\bar{\psi}(q, \alpha)=\bar{\psi}'(q', \alpha)$.

Автомат $\mathfrak{A}=(A, Q, B, \varphi, \psi)$ называется **вложимым** в автомат $\mathfrak{A}'=(A, Q', B, \varphi', \psi')$, если для любого состояния q автомата $\mathfrak{A}$ существует неотличимое от него состояние q' автомата $\mathfrak{A}'$. Как легко заметить, если автомат $\mathfrak{A}$ вложим (слабо вложим) в автомат $\mathfrak{A}'$, а $\mathfrak{A}'$ — вложим (слабо вложим) в $\mathfrak{A}''$ то $\mathfrak{A}$ вложим (слабо вложим) в $\mathfrak{A}''$. Кроме того, из вложимости автомата $\mathfrak{A}$ в автомат $\mathfrak{B}$ вытекает слабая вложимость $\mathfrak{A}$ в $\mathfrak{B}$.

Теорема 2.5 [4]. Для любого автомата $\mathfrak{A}=(A, Q, B, \varphi, \psi)$, где $|B|\geqslant 2$, существует автомат $\mathfrak{A}'=(A, Q', B, \varphi, \psi')$ со следующими свойствами:

1) $\mathfrak{A}'$ не является слабо вложимым в $\mathfrak{A}$;

2) автомат $\mathfrak{A}$ вложим в автомат $\mathfrak{A}'$

Доказательство. Пусть $Q=\{q_0, q_1, ..., q_{n-1}\}$ и $a_1 \in A$; образуем n слов: $\alpha_0=a_1$; $\alpha_1=a_1 a_1; ...; \alpha_{n-1}=\underbrace{a_1 a_1 \ldots a_1}_{n}$. Построим автомат $\mathfrak{B}=(A, Q', B, \varphi', \psi')$, где $Q'=\{q_0', \ldots, q_{n-1}'\}$; $Q \cap Q' = \varnothing$; $\varphi'(q_i', a_1)=q_{i+1 (\mathrm{mod}\, n)}$ и $\varphi'(q_i', a)=q_0'$ при $a \neq a_1$; $\psi'(q_i', a_1) \neq \psi(q_i, \alpha_i)$ и для некоторого фиксированного b_1 имеет место $\psi'(q_i', a)=b_1$ при любом $a \neq a_1$; $i=1, 2, ..., n$. Нетрудно видеть, что для любого $q, q \in Q$, имеет место $\bar{\psi}(q, \alpha_n) \neq \bar{\psi}(q_0', \alpha_n)$. Поэтому автомат $\mathfrak{B}$ не является слабо вложимым в $\mathfrak{A}$. В качестве автомата $\mathfrak{A}'$ выбираем теперь автомат $\mathfrak{A}+\mathfrak{B}$. Так как, очевидно, автомат $\mathfrak{B}$ слабо вложим в автомат $\mathfrak{A}'$, то $\mathfrak{A}'$ не может быть слабо вложимым в $\mathfrak{A}$. Вложимость автомата $\mathfrak{A}$ в автомат $\mathfrak{A}'=\mathfrak{A}+\mathfrak{B}$ очевидна. Теорема доказана.

Теорема 2.5 показывает, что отношения вложимости и слабой вложимости автоматов не симметричны.

Введем еще два соотношения, характеризующих «похожесть» автоматов.

Автоматы $\mathfrak{A}$ и $\mathfrak{A}''$ назовем **слабо неотличимыми** (обозначается $\mathfrak{A} \sim \mathfrak{A}'$), если каждый из них слабо вложим в другой.

Автоматы $\mathfrak{A}$ и $\mathfrak{A}'$ назовем **неотличимыми** (обозначается $\mathfrak{A} \approx \mathfrak{A}'$), если каждый из них вложим в другой. Ясно, что из неотличимости автоматов $\mathfrak{A}$ и $\mathfrak{A}'$ следует их слабая неотличи-

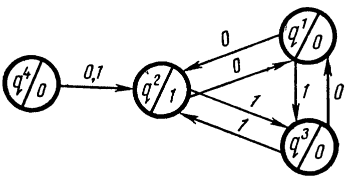

Рис. 2.8.

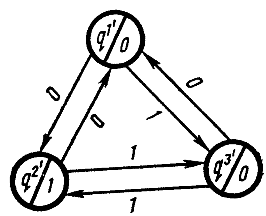

Рис. 2.9.

мость, но, как показывает пример автоматов, чьи диаграммы Мура приведены на рис. 2.8 и 2.9, обратное, вообще говоря, неверно.

Если ограничиться лишь классом сильно связных автоматов, то, как показывает следующая теорема, введенные понятия слабой вложимости, вложимости, слабой неотличимости и неотличимости автоматов оказываются эквивалентными.

Теорема 2.6 [4]. Если автоматы $\mathfrak{A}$ и $\mathfrak{A}'$ сильно связны и $\mathfrak{A}$ слабо вложим в $\mathfrak{A}'$, то автоматы $\mathfrak{A}$ и $\mathfrak{A}'$ неотличимы.

Доказательство. Пусть $\mathfrak{A}=(A, Q, B, \varphi, \psi)$, $\mathfrak{A}'=(A, Q', B, \varphi', \psi')$, где $Q=\{q^0, q^1, ..., q^{n-1}\}$, $Q'=\{q^{0'}, q^{1'}, \ldots, q^{m-1'}\}$ и $\alpha_1 \in A^*$.

Так как $\mathfrak{A} \leqslant \mathfrak{A}'$, то найдется такое состояние q' из Q', что $\overline{\psi}(q^0, \alpha_1) = \overline{\psi}'(q', \alpha_1)$. Пусть $\{q'^{i_1}, q'^{i_2}, \ldots, q'^{i_l}\}$ — множество всех таких состояний q' из Q'. Рассмотрим множество $Q(\alpha_1) = \{\varphi'(q'^{i_1}, \alpha_1), \ldots, \varphi'(q'^{i_p}, \alpha_p)\}$. Очевидно, $Q(\alpha_1) \neq \varnothing$ и для любого слова γ из A^* имеет место $|Q(\alpha_1)| \geqslant |Q(\alpha_1\gamma)|$. Если слово γ таково, что $|Q(\alpha_1\gamma)| < |Q(\alpha_1)|$, то рассмотрим слово $\alpha_2 = \alpha_1\gamma$. Для него строим свое множество $Q(\alpha_2)$ и снова выясняем, существует ли такое слово γ' из A^*, что $|Q(\alpha_2\gamma')| < |Q(\alpha_2)|$, или нет. Если существует, то продолжаем процесс наращивания слова α_1. Ясно, что в результате наших построений мы получим некоторое слово α из A^*, такое, что $Q(\alpha) \neq \varnothing$, и для любого слова γ из A^* справедливо равенство $|Q(\alpha)| = |Q(\alpha\gamma)|$. Далее, так как автомат $\mathfrak{A}$ является сильно связным, то существуют такие слова $\delta_0, \delta_1, \ldots, \delta_{n-1}$ из A^*, что для любого i, $i = 0, 1, \ldots, n-1$, будет иметь место $\varphi(q^i, \delta_i) = q^{i+1 (\mathrm{mod}\, n)}$. Пусть $\varphi(q^0, \alpha) = q^k$, построим слово $\alpha\delta_k\delta_{k+1} \ldots \delta_{n-1}\delta_0\delta_1 \ldots \delta_{k-1}$ и по нему — множества $Q(\alpha\delta_k)$, $Q(\alpha\delta_k\delta_{k+1}), \ldots, Q(\alpha\delta_k\delta_{k+1} \ldots \delta_{n-1}\delta_0\delta_1 \ldots \delta_{k-1})$. Покажем, что для любого состояния q^i из Q и любого состояния q' из $Q(\alpha\delta_k\delta_{k+1} \ldots \delta_{n-1}\delta_0\delta_1 \ldots \delta_{i-1})$ имеет место $q^i \sim q'$. В самом деле, если бы для некоторых q^i и q', удовлетворяющих нашим условиям, имела место отличимость, то нашлось бы такое слово γ из A^*, что $\overline{\psi}(q^i, \gamma) \neq \overline{\psi}'(q', \gamma)$. А это означало бы, очевидно, справедливость неравенства

$$|Q(\alpha\delta_k\delta_{k+1} \ldots \delta_{n-1}\delta_0\delta_1 \ldots \delta_{i-1}\gamma)| < |Q(\alpha\delta_k\delta_{k+1} \ldots \delta_{n-1}\delta_0\delta_1 \ldots \delta_{i-1})|,$$

что противоречило бы выбору слова α. Покажем теперь, что для любого состояния q'_i автомата $\mathfrak{A}'$ найдется такое состояние q_j автомата $\mathfrak{A}$ что $q'_i \sim q_j$. Зафиксируем какое-нибудь состояние q автомата $\mathfrak{A}$, и пусть q' — такое состояние автомата $\mathfrak{A}'$, что $q \sim q'$. В силу сильной связности автомата $\mathfrak{A}'$ найдется такое слово α, что $\varphi'(q', \alpha) = q'_i$. Рассмотрим состояние $q_j = \varphi(q, \alpha)$; нетрудно видеть, что, $q_j \sim q'_i$. Теорема доказана.

Класс всех автоматов с заданными входным и выходным алфавитами A и B, множества состояний которых суть подмножества фиксированного счетного множества $\{q_1, q_2, \ldots, q_n, \ldots\}$, обозначим $K(A, B)$. Ясно, что отношения слабой неотличимости и неотличимости автоматов разбивают множество $K(A, B)$ на классы эквивалентности.

Теорема 2.7 [1]. Число классов слабой неотличимости в $K(A, B)$ при $|B| \geqslant 2$ счетно.

Доказательство. Пусть $\mathfrak{A}$ — произвольный автомат из $K(A, B)$. В силу теоремы 2.5 существует последовательность $\mathfrak{A} = \mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{A}_3, \ldots$ автоматов, принадлежащих $K(A, B)$, такая, что $\mathfrak{A}_{j+1}$ не является слабо вложимым в $\mathfrak{A}_j$ и $\mathfrak{A}_j \leqslant \mathfrak{A}_{j+1}$ $(i = 1, 2, \ldots, n)$. Покажем, что автоматы $\mathfrak{A}_i$ и $\mathfrak{A}_j$ при $i \neq j$ принадлежат различимым классам слабой неотличимости, из этого и будет вытекать утверждение теоремы. Пусть $i \neq j$, $i<j$. Если $\mathfrak{A}_j \sim \mathfrak{A}_i$, то $\mathfrak{A}_j \leqslant \mathfrak{A}_i$, а так как $\mathfrak{A}_i \leqslant \mathfrak{A}_{i+1}, \ldots, \mathfrak{A}_{j-2} \leqslant \mathfrak{A}_{j-1}$, то получаем $\mathfrak{A}_j \leqslant \mathfrak{A}_{j-1}$, что противоречит условию, наложенному на рассматриваемую последовательность. Теорема доказана.

Следствие. Число классов неотличимости в $K(A, B)$ при $|B| \geqslant 2$ счетно. Класс всех автоматов, принадлежащих $K(A, B)$ и неотличимых от автомата $\mathfrak{A}$, $\mathfrak{A} \in K(A, B)$, обозначаем $K_{\mathfrak{A}}(A, B)$. Для класса всех автоматов, принадлежащих $K(A, B)$ и слабо неотличимых от $\mathfrak{A}$, используем обозначение $T_{\mathfrak{A}}(A, B)$.

Автомат $\mathfrak{A}$, все состояния которого неотличимы друг от друга, называется **автоматом приведенного вида**.

Следующее утверждение позволяет достаточно полно охарактеризовать класс $K_{\mathfrak{A}}(A, B)$ в терминах автоматов приведенного вида.

Теорема 2.8 [4]. Для любого автомата $\mathfrak{A}$ класс $K(A, B)$ содержит с точностью до изоморфизма единственный автомат приведенного вида.

Доказательство. Отношение неотличимости состояний автомата $\mathfrak{A}$, которое является отношением эквивалентности, разбивает множество Q его состояний на классы эквивалентности $Q_1, Q_2, \ldots, Q_k$. Пусть φ — функция переходов автомата $\mathfrak{A}$; покажем, что для любого Q_i, $i=1, 2, \ldots, k$, любых состояний q и q' из Q_i и любого a из A, если $\varphi(q, a) \in Q_j$, $j=1, 2, \ldots, k$, то $\varphi(q', a) \in Q_j$, т. е. неотличимые состояния под действием одной и той же буквы переходят снова в неотличимые состояния. В самом деле пусть это не так, т. е. нашлись такие Q_i, q, q' из Q_i и a из A, что для некоторого j $\varphi(q, a) \in Q_j$, а $\varphi'(q', a) \in Q_l$, $l \neq j$. Ясно, что состояния $\varphi(q, a)$ и $\varphi(q', a)$ в этом случае окажутся отличимыми, т. е. найдется такое слово $\alpha, \alpha \in A^*$, для которого будет иметь место $\bar{\psi}(\varphi(q, a), \alpha) \neq \bar{\psi}(\varphi(q', a), \alpha)$, где ψ — функция переходов автомата $\mathfrak{A}$. С другой стороны, $\bar{\psi}(q, a\alpha) = \psi(q, a)\bar{\psi}(\varphi(q, a), \alpha)$ и $\bar{\psi}(q', a\alpha) = \psi(q', a)\bar{\psi}(\varphi(q', a), \alpha)$, откуда, в силу полученного неравенства, $\bar{\psi}(q, a\alpha) \neq \bar{\psi}(q', a\alpha)$, т. е. q и q' отличимы и не могли принадлежать одному и тому же классу Q_i. Полученное противоречие доказывает наше утверждение. Далее, для любых Q_i, q, q', очевидно, справедливо равенство $\psi(q, a) = \psi(q', a)$, если q и q' из Q_i. Установленные свойства функций φ и ψ делают корректным определение автомата $\mathfrak{A}' = (A, Q', B, \varphi', \psi')$, где $Q = \{q^{1'}, q^{2'}, \ldots, q^{k'}\}$, $\varphi'(q^{i'}, a) = q^{j'}$, если существуют такие состояния q из Q_i и q' из Q_j, что $\varphi(q, a) = q'$ и $\psi'(q^{i'}, a) = \psi(q, a)$, если q из Q_i. Из построения автомата $\mathfrak{A}'$ следует, что все его состояния попарно отличимы и любое состояние $q^{i'}$ из Q' неотличимо от любого состояния q из Q_i автомата $\mathfrak{A}$. Верно и обратное, т. е. каждое состояние q из Q_i автомата $\mathfrak{A}$ неотличимо от состояния $q^{i'}$ автомата $\mathfrak{A}'$. Таким образом, $\mathfrak{A}'$ является приведенным и содержится в $K_{\mathfrak{A}}(A, B)$. Пусть теперь $\mathfrak{A}''$ из $K_{\mathfrak{A}}(A, B)$ — любой приведенный автомат, покажем, что $\mathfrak{A}''$ и

$\mathfrak{A}'$ изоморфны. В самом деле, из приведенности каждого из этих автоматов и их неотличимости следует, что число состояний у них одно и то же. Пусть $Q'' = \{q^{1''}, q^{2''}, \ldots, q^{k''}\}$ — множество состояний автомата $\mathfrak{A}''$. Определим функцию ξ, отображающую Q' на Q'', следующим образом: $\xi(q^{i''}) = q^{i''}$ тогда и только тогда, когда $q^{i'} \sim q^{i''}$; $i, j = 1, 2, \ldots, k$. Ясно, что отображение ξ взаимнооднозначно и для функций выходов автоматов $\mathfrak{A}'$ и $\mathfrak{A}''$ имеет место равенство $\psi'(q^{i'}, a) = \psi''(\xi(q^{i'}), a)$. Таким образом, для изоморфизма автоматов $\mathfrak{A}'$ и $\mathfrak{A}''$ остается показать, что для любых i, $i = 1, 2, \ldots, k$ и a из A справедливо $\xi(\varphi(q^{i'}, a)) = \varphi''(\xi(q^{i'}), a)$, где φ'' — функция переходов автомата $\mathfrak{A}''$. Как и выше, последнее следует из того, что под действием одной и той же буквы a автоматы $\mathfrak{A}'$ и $\mathfrak{A}''$ из неотличимых состояний должны перейти также в неотличимые состояния, так как в противном случае исходные состояния были бы отличимы. Тем самым теорема доказана.

Аналог теоремы 2.8 для класса $T_{\mathfrak{A}}(A, B)$ уже не имеет места; более того, множество неизоморфных друг другу автоматов приведенного вида, содержащихся в классе $T_{\mathfrak{A}}(A, B)$, может быть бесконечным. Для формулировки необходимого и достаточного условия конечности множества таких автоматов, содержащихся в $T_{\mathfrak{A}}(A, B)$, введем ряд понятий.

Состояние q автомата $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ называется **состоянием с конечной памятью**, если существует такое натуральное k, что для любых слов α^k, $\alpha^k \in A^*$, и состояния q', $q' \in Q$, из совпадения слов $\bar{\psi}(q, \alpha^k)$ и $\bar{\psi}(q', \alpha^k)$ вытекает совпадение состояний $\varphi(q, \alpha^k)$ и $\varphi(q', \alpha^k)$. Наименьшее из таких k называется **порядком памяти состояния** q. Автомат $\mathfrak{A}$ называется **автоматом с конечной памятью**, если все его состояния имеют конечную память. При этом **порядком памяти автомата** $\mathfrak{A}$ называется наибольший из порядков памяти состояний автомата $\mathfrak{A}$.

Теорема 2.9 [5]. Для любого автомата $\mathfrak{A}$, $\mathfrak{A} \in K(A, B)$, множество рассматриваемых с точностью до изоморфизма автоматов приведенного вида, содержащихся в $T_{\mathfrak{A}}(A, B)$, конечно тогда и только тогда, когда автомат приведенного вида, неотличимый от $\mathfrak{A}$, есть автомат с конечной памятью.

Для доказательства теоремы установим ряд вспомогательных утверждений.

Лемма 2.1. Если автоматы $\mathfrak{A}$ и $\mathfrak{B}$ приведенного вида слабо неотличимы, причем $\mathfrak{A}$ — автомат с конечной памятью, то и $\mathfrak{B}$ — автомат с конечной памятью, причем порядки памяти автоматов $\mathfrak{A}$ и $\mathfrak{B}$ равны.

Доказательство. Пусть $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ — автомат приведенного вида с конечной памятью и k — его порядок памяти. Пусть также $\mathfrak{B} = (A, Q', B, \varphi', \psi')$ — автомат приведенного вида, слабо неотличимый от $\mathfrak{A}$. Достаточно показать, что $\mathfrak{B}$ имеет конечную память и порядок ее не превосходит k, т. е. что для любых состояний $q, q' \in Q'$ и слова α длины k, $\alpha \in A^*$, из совпадения слов $\bar{\psi}'(q, \alpha)$ и $\bar{\psi}'(q', \alpha)$ вытекает совпадение состояний $\varphi'(q, \alpha)$ и $\varphi'(q', \alpha)$. Пусть $q, q' \in Q'$; $\alpha \in A^*$; $|\alpha| = k$ и $\bar{\psi}'(q, \alpha) = \bar{\psi}'(q', \alpha)$. Пусть также $\gamma \in A^*$. Так как $\mathfrak{A}$ и $\mathfrak{B}$ слабо неотличимы, то найдутся состояния $s, s' \in Q$, такие, что

$$\bar{\psi}(s, \alpha\gamma) = \bar{\psi}'(q, \alpha\gamma); \; \bar{\psi}(s', \alpha\gamma) = \bar{\psi}'(q', \alpha\gamma).$$

Имеем: $\bar{\psi}(s, \alpha) = \overline{\bar{\psi}(s, \alpha\gamma)}\Big|_k = \overline{\bar{\psi}'(q, \alpha\gamma)}\Big|_k = \bar{\psi}'(q', \alpha) = \bar{\psi}(s', \alpha)$.

Но k — порядок памяти автомата $\mathfrak{A}$, поэтому $\varphi(s, \alpha) = \varphi(s', \alpha)$,

$$\bar{\psi}'(q, \alpha\gamma) = \bar{\psi}(s, \alpha\gamma) = \bar{\psi}(s, \alpha)\bar{\psi}(\varphi(s, \alpha), \gamma) =$$
$$= \bar{\psi}(s', \alpha)\bar{\psi}(\varphi(s', \alpha), \gamma) = \bar{\psi}(s', \alpha\gamma) = \bar{\psi}'(q', \alpha\gamma).$$

Так как

$$\bar{\psi}'(q, \alpha\gamma) = \bar{\psi}'(q, \alpha)\bar{\psi}'(\varphi'(q, \alpha), \gamma); \; \bar{\psi}'(q', \alpha\gamma) =$$
$$= \bar{\psi}'(q', \alpha)\bar{\psi}'(\varphi'(q, \alpha), \gamma),$$

причем $\bar{\psi}'(q, \alpha) = \bar{\psi}'(q', \alpha)$, то $\bar{\psi}'(\varphi'(q, \alpha), \gamma) = \bar{\psi}'(\varphi'(q', \alpha), \gamma)$. В силу произвольности слова $\gamma \in A^*$ состояния $\varphi'(q, \alpha)$ и $\varphi'(q', \alpha)$ неотличимы, а так как автомат $\mathfrak{B}$ — автомат приведенного вида, то $\varphi'(q, \alpha) = = \varphi'(q', \alpha)$, и лемма доказана.

Лемма 2.2. Если $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ — автомат приведенного вида, имеющий конечную память порядка k, то $|Q| \leqslant |B|^{k|A|^k}$.

Доказательство. Сопоставим каждому состоянию $q \in Q$ функцию $\bar{\psi}_q$, определенную на словах α длины k в алфавите A, такую, что $\bar{\psi}_q(\alpha) = \bar{\psi}(q, \alpha)$. Если $q \neq q'$ и $\bar{\psi}_q = \bar{\psi}_{q'}$, то для любого α^k $\bar{\psi}(q, \alpha) = \bar{\psi}(q', \alpha)$, и так как порядок памяти $\mathfrak{A}$ равен k, то $\varphi(q, \alpha) = \varphi(q', \alpha)$, откуда вытекает неотличимость состояний q и q', т. е. $q = q'$, и приходим к противоречию. Следовательно, $|Q|$ не превосходит числа функций, определенных на множестве слов длины k в алфавите A, значениями которых служат слова длины k в алфавите B, т. е. $|Q| \leqslant (|B|^k)^{|A|^k} = |B|^{k|A|^k}$.

Лемма 2.3. Если автомат приведенного вида $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ не является автоматом с конечной памятью, то существуют слово α, $\alpha \in A^*$, $\alpha \neq \Lambda$, и состояния $q, q' \in Q$, $q \neq q'$, такие, что $\varphi(q, \alpha) = q$; $\varphi(q', \alpha) = q'$, причем для некоторого слова $\alpha' \in A^*$, первая буква которого отлична от первой буквы слова α, $\bar{\psi}(q, \alpha') \neq \bar{\psi}(q', \alpha')$.

Доказательство. Так как $\mathfrak{A}$ не является автоматом с конечной памятью, то существуют состояния q_0, q_0' и слово $\beta \in A^*$ длины $|Q|^2$, такие, что $\bar{\psi}(q_0, \beta) = \bar{\psi}(q_0', \beta)$ и $\varphi(q_0, \beta) \neq \varphi(q_0', \beta)$. Обозначим

$$q_i = \eta(q_0, \overline{\beta}\big|_i); \; q_i' = \varphi(q_0', \overline{\beta}\big|_i;$$

тогда для любого $i \in \{0, 1, \ldots, |Q|^2\}$ $q_i \neq q_i'$. Так как число различных пар (q^1, q^2), таких, что $q^1, q^2 \in Q$, не превосходит $|Q|^2$, то среди пар $(q_0, q'_0), \ldots, (q_{|Q|^2}, q'_{|Q|^2})$ найдутся две одинаковые пары, скажем, $(q_{i_1}, q'_{i_1}) = (q_{i_2}, q'_{i_2})$ при $i_1 < i_2$. Если $\beta = b(1) \ldots b(|Q|^2)$; $\gamma = b(i_1+1) \ldots b(i_2)$, то

$$\varphi(q_{i_1}, \gamma) = q_{i_1};\ \varphi(q'_{i_1}, \gamma) = q'_{i_1},$$

при этом $\overline{\psi}(q_{i_1}, \gamma) = \overline{\psi}(q'_{i_1}, \gamma)$. Состояния q_{i_1} и q'_{i_1} отличимы; рассмотрим кратчайшее слово $\delta = d(1) \ldots d(m)$, различающее эти состояния. Если δ представимо в виде $\gamma\delta'$, то слово δ' также различает состояния q_{i_1}, q'_{i_1}. Поэтому δ не представимо в таком виде и существует i_3, $i_1 < i_3 \leqslant i_2$, такое, что

$$b(i_1+1) = d(1), \ldots, b(i_3-1) = d(i_3-i_1-1),\ b(i_3) \neq d(i_3-i_1).$$

Положим

$$q = \varphi(q_{i_1}, \overline{\gamma}|_{i_3-i_1});\ q' = \varphi(q'_{i_1}, \overline{\gamma}|_{i_3-i_1});\ \alpha = |\overline{\gamma}_{i_3-i_1}\,\overline{\gamma}|_{i_3-i_1};\ \alpha' = |\overline{\delta}_{i_3-i_1-1}.$$

Здесь посредством $|\overline{p}_{l}$ обозначено слово, получающееся из слова p отбрасыванием начала $\overline{p}|_{l}$. Тогда

$$\varphi(q, \alpha) = \varphi(\varphi(q_{i_1}, \overline{\gamma}|_{i_3-i_1}), |\overline{\gamma}_{i_3-i_1}\,\overline{\gamma}|_{i_3-i_1}) = \varphi(\varphi(q_{i_1}, \gamma), \overline{\gamma}|_{i_3-i_1}) =$$
$$= \varphi(q_{i_1}, \overline{\gamma}|_{i_3-i_1}) = q$$

и, аналогично, $\varphi(q', \alpha) = q'$; при этом, очевидно, $q \neq q'$ и $\overline{\psi}(q, \alpha') \neq \overline{\psi}(q', \alpha')$. Лемма доказана.

Доказательство теоремы 2.9. Пусть $\mathfrak{A}' = (A, Q, B, \varphi, \psi)$ — автомат приведенного вида, неотличимый от $\mathfrak{A}$. Тогда, очевидно, $T_{\mathfrak{A}}(A, B) = T_{\mathfrak{A}'}(A, B)$. Если $\mathfrak{A}'$ — автомат с конечной памятью и порядок его памяти равен k, то по лемме 2.1 любой автомат приведенного вида $\mathfrak{A}'' \in T_{\mathfrak{A}'}(A, B)$ имеет порядок памяти k, т. е. по лемме 2.2 число состояний любого такого автомата не превосходит $|B|^{k|A|^k}$. Отсюда и вытекает конечность множества рассматриваемых с точностью до изоморфизма автоматов приведенного вида, содержащихся в $T_{\mathfrak{A}}(A, B)$.

Пусть теперь $\mathfrak{A}'$ не является автоматом с конечной памятью. Предположим, что множество автоматов приведенного вида, содержащихся в $T_{\mathfrak{A}}(A, B)$, конечно. Тогда существует автомат приведенного вида из $T_{\mathfrak{A}}(A, B)$, имеющий наибольшее число состояний; без ограничения общности можно считать, что этот автомат есть $\mathfrak{A}'$. Построим автомат $\mathfrak{A}''$, получающийся присоединением новых состояний к автомату $\mathfrak{A}'$, слабо неотличимый от $\mathfrak{A}'$ и такой, что хотя бы одно из присоединенных состояний отличимо от всех состояний автомата $\mathfrak{A}'$. Функции переходов и выходов автомата $\mathfrak{A}''$ получаются доопределением функций φ и ψ и обозначаются φ', ψ'. По лемме 2.3 существуют состояния $q, q' \in Q$ и слова $\alpha = a(1) \ldots a(k)$; $\alpha' = a'(1) \ldots a'(l)$, $a'(1) \neq a(1)$, для которых $\varphi(q, \alpha) = q$; $\varphi(q', \alpha) =$

$=q'$; $q\neq q'$; $\overline{\psi}(q, \alpha')\neq\overline{\psi}(q', \alpha')$. Рассмотрим новые состояния s_{ij}, где $i\in\{0, 1,\dots,n-1\}$; $n=|Q|$, $j\in\{0, 1,\dots; k-1\}$. Обозначим $q_i=\varphi(q, \underset{i}{\underline{\alpha|}})$ $(i=0, 1,\dots,k-1)$. Положим $\varphi'(s_{ij}, a(j+1))=s_{i,j+1}$ при $j<k-1$; $\varphi'(s_{i,k-1}, a(k))=s_{i+1,0}$ при $i<n+1$ и $\varphi'(s_{n-1,k-1}, a(k))=q$. Пусть также $\psi'(s_{ij}, a(j+1))=\psi(q_j, a(j+1))$. Для дальнейшего доопределения функций φ' и ψ' рассмотрим множество $Q=\{s_0,\dots,s_{n-1}\}$. Слово $\overline{\psi}(s_i, \alpha^i\alpha')$ отличается от одного из слов $\overline{\psi}(q, \alpha^i\alpha')$; $\overline{\psi}(q', \alpha^i\alpha')$ $(i=0, 1,\dots,n-1)$. Если оно отличается от $\overline{\psi}(q, \alpha^i\alpha')$, то полагаем $\varphi'(s_{i0}, a'(1))=\varphi(q', a'(1))$; $\psi'(s_{i0}, a'(1))=\psi(q, a'(1))$; если же оно отличается от $\overline{\psi}(q', \alpha^i\alpha')$, то полагаем $\varphi'(s_{i0}, a'(1))=\varphi(q, a'(1))$; $\psi'(s_{i0}, a'(1))=\psi(q', a'(1))$. В первом случае $\overline{\psi}(s_{00}, \alpha^i\alpha')=\overline{\psi}(q, \alpha^i\alpha')$, во втором случае $\overline{\psi}(s_{00}, \alpha^i\alpha')=\overline{\psi}(q', \alpha^i\alpha')$, т. е. состояние s_{00} отличимо от всех состояний $s_0,\dots,s_{n-1}$. В тех случаях, в которых $\varphi'(s_{ij}, a)$ и $\psi'(s_{ij}, a)$ еще не определены, положим $\varphi'(s_{ij}, a)=\varphi(q_j, a)$; $\psi'(s_{ij}, a)=\psi(q_j, a)$. Нетрудно проверить, что для любых состояния s_{ij} и слова $\gamma, \gamma\in A$, существует состояние $s\in Q$, такое, что $\overline{\psi}'(s_{ij}, \gamma)=\overline{\psi}(s, \gamma)$, так что автоматы $\mathfrak{A}'$ и $\mathfrak{A}''$ слабо неотличимы. Пусть $\mathfrak{A}'''$ — неотличимый от $\mathfrak{A}''$ автомат приведенного вида. Тогда число состояний автомата $\mathfrak{A}'''$ хотя бы на единицу больше числа состояний автомата $\mathfrak{A}'$, причем $\mathfrak{A}'''\in T_{\mathfrak{A}}(A, B)$, что противоречит предположению о том, что $\mathfrak{A}'$ имеет наибольшее число состояний. Теорема доказана.

В заключение заметим, что для сильно связного автомата $\mathfrak{A}$, как это вытекает из теорем 2.6 и 2.8, в классе $T_{\mathfrak{A}}$ (A, B) имеется единственный сильно связный автомат приведенного вида. Отношение неотличимости можно ввести также и на множестве инициальных автоматов $\mathfrak{A}_q$, полагая неотличимыми автоматы $\mathfrak{A}_q$ и $\mathfrak{B}_{q'}$, тогда и только тогда, когда неотличимы состояния q и q'. Инициальный автомат $\mathfrak{A}_q$ называется **автоматом приведенного вида**, если $\mathfrak{A}$ есть автомат приведенного вида, причем $\mathfrak{A}_q$ — инициально связный. Как несложное следствие теоремы 2.8 получаем, что в классе всех инициальных автоматов, неотличимых от заданного инициального автомата, имеется единственный с точностью до изоморфизма автомат приведенного вида.

УПРАЖНЕНИЯ

1. Пусть $n_1, n_2,\dots,n_k$ — последовательность натуральных чисел, удовлетворяющая условиям: $n_1\geqslant 2$; $n_{i+1}>n_i$. $(i=1,\dots k-1)$. Всегда ли возможно построить конечный автомат с n_k состояниями, у которого число классов введенного при доказательстве теоремы 2.3 отношения эквивалентности R_i равно n_i $(i=1,\dots k)$?
2. Может ли автомат $\mathfrak{A}$ с 5 попарно отличимыми состояниями быть слабо вложим в автомат $\mathfrak{B}$ с 3 состояниями?

3. Является ли автомат Мура, диаграмма которого приведена на рис. 2.8, автоматом с конечной памятью?
4. Построить конечный автомат, у которого порядок памяти равен 2. Каково наименьшее возможное число состояний такого автомата?
5. Для каких n существует конечный автомат $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ с n попарно отличимыми состояниями, у которого при любом слове $\alpha \in A^*$ длины $n-1$ множество $\{\bar{\psi}(q, \alpha) : q \in Q\}$ имеет не более двух элементов?

§ 3. ЭКСПЕРИМЕНТЫ С АВТОМАТАМИ

При изучении автоматов как преобразователей входных последовательностей типичной является задача восстановления свойств автомата по его реакциям на входные слова.

Без ограничения общности рассматриваем в этом параграфе лишь такие автоматы $\mathfrak{A}_q = (A, Q, B, \varphi, \psi, q)$, что $A \subseteq N$; $B \subseteq N$, где $N = \{1, 2, 3, \ldots\}$.

Процесс подачи на инициальный автомат $\mathfrak{A}_q$ входных слов и наблюдения за выдаваемыми автоматом словами будем называть экспериментом с автоматом $\mathfrak{A}$.

Эксперимент, состоящий в подаче на автомат $\mathfrak{A}_q$ единственного входного слова, называется **простым**; если же мы располагаем несколькими экземплярами одного и того же автомата $\mathfrak{A}_q$ и подаем на каждый из них различные входные слова, то эксперимент называется **кратным**. Если в случае простого эксперимента очередной символ, подаваемый на автомат $\mathfrak{A}_q$, выбирается в зависимости от реакции $\mathfrak{A}_q$ на ранее поданные символы, то этот эксперимент называется **простым условным экспериментом**; в противном случае он называется **простым безусловным экспериментом**. Кратный эксперимент, у которого входное слово, подаваемое на очередной экземпляр автомата $\mathfrak{A}_q$, зависит от реакций этого автомата на ранее поданные слова, называется **кратным условным** экспериментом; в противном случае он называется **кратным безусловным** экспериментом.

Более формально указанные типы экспериментов определяются следующим образом:

Слова в алфавите N называем **простыми безусловными экспериментами**; конечные множества слов в алфавите N — **кратными безусловными экспериментами.**

Простой безусловный эксперимент E применим к инициальному автомату $\mathfrak{A}_q = (A, Q, B, \varphi, \psi)$, если $E \in A^*$; результатом применения E к $\mathfrak{A}_q$ в этом случае называется пара $(E, \bar{\psi}(q, E))$.

Кратный безусловный эксперимент E применим к $\mathfrak{A}_q$, если $E \subset A^*$; результатом применения E к $\mathfrak{A}_q$ в этом случае называется множество пар $(\alpha, \bar{\psi}(q, \alpha))$, таких, что $\alpha \in E$.

Пусть $M = \{(\alpha, \beta) : \alpha \in N^*, \beta \in N^*, |\alpha| = |\beta|\}$; M' — множество конечных подмножеств множества M. **Простым условным экспе-**

риментом называется функция Φ, определенная на некотором подмножестве множества M и принимающая значения в множестве N.

Кратным условным экспериментом называется функция Ψ, определенная на некотором подмножестве множества M', значениями которой являются кратные безусловные эксперименты.

Простой условный эксперимент Ψ применим к инициальному автомату $\mathfrak{A}_q=(A, Q, B, \varphi, \psi, q)$, если существует слово $\alpha=$ $=a(1)a(2)\ldots a(l)$ в алфавите A, такое, что $a(1)=\Phi((\Lambda,\Lambda))$; $a(i+1)=\Phi((\alpha|_i, \bar{\psi}(q, \alpha|_i)))$ при $i=1, 2,\ldots, l-1$ и $\Phi(\alpha, \bar{\psi}(q, \alpha))$ не определено. Результатом применения Φ к $\mathfrak{A}_q$ в этом случае называется пара $(\alpha, \bar{\psi}(q, \alpha))$.

Кратный условный эксперимент Ψ применим к $\mathfrak{A}_q$, если существуют конечные последовательности $E_1,\ldots,E_l$ и $R_0, R_1,\ldots,R_l$, такие, что $E_1=\Psi(\varnothing)$; $R_0=\varnothing$; $E_{i+1}=\Psi(R_i)$ $(i=1,\ldots,l-1)$; $R_j=$ $=R_{j-1}\cup R_j'$, где R_j' — результат применения кратного безусловного эксперимента E_j к автомату $\mathfrak{A}_q$ $(j=1, 2,\ldots, l)$, причем $\Psi(R_l)$ не определено. Результатом применения Ψ к $\mathfrak{A}_q$ в этом случае называется множество R_l.

Пусть R — результат применения некоторого эксперимента E (произвольного типа) к инициальному автомату $\mathfrak{A}_q=(A, Q, B,$ $\varphi, \psi, q)$. Если E — простой эксперимент и $R=(\alpha, \beta)$, то **длиной** R назовем длину слова α; если же E — кратный эксперимент, то длиной R назовем наибольшую из длин слов α, таких, что $(\alpha, \bar{\psi}(q, \alpha))\in R$. Длину R обозначаем $l(R)$. В случае кратного эксперимента E введем также величины **кратности** $k(R)$ и **объема** $v(R)$. $k(R)$ есть число элементов в R; $v(R)$ — сумма длин всех слов α, для которых $(\alpha, \bar{\psi}(q, \alpha))\in R$.

Если $\mathfrak{M}$ — некоторое множество инициальных автоматов и E — эксперимент, применимый ко всем автоматам из $\mathfrak{M}$, то **длиной** $l(E, \mathfrak{M})$ (в случае кратного эксперимента E — также **кратностью** $k(E, \mathfrak{M})$) и **объемом** $v(E, \mathfrak{M})$ **эксперимента** E **относительно** $\mathfrak{M}$ называем максимум длин (соответственно кратностей и объемов) результатов применения E к автоматам из $\mathfrak{M}$. Если $\mathfrak{M}$ бесконечно и наибольшего значения длины (кратности, объема) не существует, то полагаем $l(E, \mathfrak{M})=\infty$ (соответственно $k(E, \mathfrak{M})=\infty$, $v(E, \mathfrak{M})=\infty$).

Пусть $\mathfrak{M}$ — некоторое множество инициальных автоматов и E — эксперимент, применимый ко всем автоматам из $\mathfrak{M}$. Если $\mathfrak{A}_q\in\mathfrak{M}$ и результат применения E к $\mathfrak{A}_q$ отличается от результата применения E к любому другому инициальному автомату из $\mathfrak{M}$, то E называется **тестовым** для $\mathfrak{A}_q$ относительно $\mathfrak{M}$. Если результаты применения E к любым двум различным инициальным автоматам из $\mathfrak{M}$ различны, то E называется **диагностическим** для $\mathfrak{M}$. Если E — простой эксперимент, причем для любых автоматов $\mathfrak{A}_q$ и $\mathfrak{A}'_{q'}$ из $\mathfrak{M}$ совпадение результатов $(\alpha, \bar{\psi}(q, \alpha))$ и $(\alpha', \bar{\psi}'(q', \alpha'))$ применения E к $\mathfrak{A}_q$ и $\mathfrak{A}'_{q'}$

влечет неотличимость инициальных автоматов $\mathfrak{A}_{\varphi'(q',\alpha')}$ и $\mathfrak{A}_{\varphi(q,\alpha)}$, то E называется **установочным для** $\mathfrak{M}$.

Рассмотрим сначала случай, когда в качестве $\mathfrak{M}$ берется множество $[\mathfrak{A}]$ всех инициальных автоматов $\mathfrak{A}_q$, получающихся при различных выборах начального состояния q у заданного автомата $\mathfrak{A}=(A, Q, B, \varphi, \psi)$. Некоторые другие случаи будут рассмотрены в § 4, 5.

Рассмотрение множества $[\mathfrak{A}]$ в качестве $\mathfrak{M}$ означает, что у исследуемого автомата $\mathfrak{A}_q$ неизвестным является лишь начальное состояние q; в этом случае диагностический для $[\mathfrak{A}]$ эксперимент позволяет определить неизвестное начальное состояние, а установочный для $[\mathfrak{A}]$ эксперимент — перевести автомат $\mathfrak{A}_q$ в известное экспериментатору состояние.

Теорема 2.10 [4]. Для любого натурального $n\geqslant 3$ существует такой автомат $\mathfrak{A}$ с n попарно отличимыми состояниями, что для $[\mathfrak{A}]$ отсутствует простой (как безусловный, так и условный) диагностический эксперимент.

Доказательство. Рассмотрим автомат $\mathfrak{A}$, диаграмма Мура которого приведена на рис. 2.10.

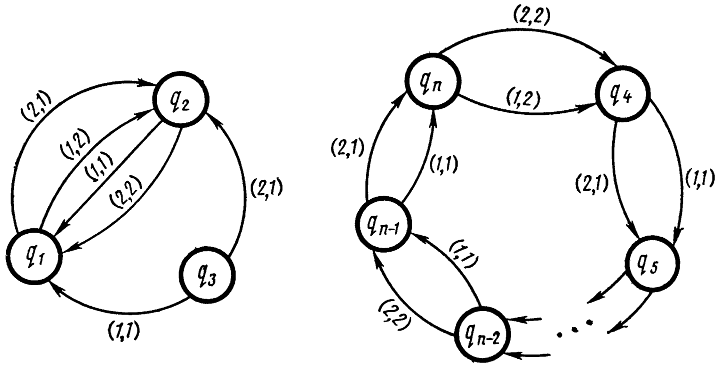

Рис. 2.10.

У этого автомата $A=B=\{1, 2\}$; $Q=\{q_1, \ldots, q_n\}$. Если $4\leqslant i<j\leqslant n$, причем $\tilde{\alpha}_0=\underbrace{1\ldots1}_{n-j+1}$, то $\overline{\psi}(q_i, \tilde{\alpha}_0)=1\ldots1$; $\overline{\psi}(q_j, \tilde{\alpha}_0)=1\ldots12$, откуда вытекает попарная отличимость состояний q_i при $i\geqslant 4$. Очевидно, что при $i\geqslant 4$ и произвольном входном слове $\tilde{\alpha}_1$ в $\overline{\psi}(q_i, \tilde{\alpha}_1)$ не могут встретиться подряд две двойки. С другой стороны, $\overline{\psi}(q_1, 12)=22$; $\overline{\psi}(q_2, 21)=22$; $\overline{\psi}(q_3, 112)=122$, так что каждое состояние q_1, q_2, q_3 отличимо от всех состояний q_i при $i\geqslant 4$. Наконец, попарная отличимость состояний q_1, q_2 и q_3 вытекает из равенств: $\overline{\psi}(q_1, 1)=2$; $\overline{\psi}(q_2, 1)=1$; $\overline{\psi}(q_3, 1)=1$; $\overline{\psi}(q_2, 2)=2$; $\overline{\psi}(q_3, 2)=1$. Таким образом, автомат $\mathfrak{A}$ имеет n попарно отличимых состояний. Если бы существовал простой безусловный эксперимент $\tilde{\alpha}$, диагностический для $[\mathfrak{A}]$, то для любых двух состояний q_i, q_j $(i\neq j)$ автомата $\mathfrak{A}$

должно было бы выполняться $\bar\psi(q_i, \tilde\alpha) \neq \bar\psi(q_j, \tilde\alpha)$. Однако при $\tilde\alpha$ вида $1\alpha_2 \dots \alpha_l$ имеем: $\bar\psi(q_2, \tilde\alpha) = \psi(q_2, 1)\bar\psi(q_1, \alpha_2 \dots \alpha_l)$; $\bar\psi(q_3, \tilde\alpha) = \psi(q_3, 1)\bar\psi(q_1, \alpha_2 \dots \alpha_l)$, и так как $\psi(q_2, 1) = \psi(q_3, 1) = 1$, то $\bar\psi(q_2, \tilde\alpha) = \bar\psi(q_3, \tilde\alpha)$. Если же $\tilde\alpha$ имеет вид $2\alpha_2 \dots \alpha_l$, то $\bar\psi(q_1, \tilde\alpha) = \psi(q_1, 2)\bar\psi(q_2, \alpha_2 \dots \alpha_l) = \psi(q_3, 2)\bar\psi(q_2, \alpha_2 \dots \alpha_l) = \bar\psi(q_3, \tilde\alpha)$. Таким образом, ни при каком $\tilde\alpha \in A^*$ неравенство $\bar\psi(q_i, \tilde\alpha) \neq \bar\psi(q_j, \tilde\alpha)$ не может выполняться одновременно для всех пар (q_i, q_j), где $i \neq j$, что и означает отсутствие простого безусловного эксперимента, диагностического для $[\mathfrak{A}]$. Легко видеть, что проведенные рассуждения позволяют установить также отсутствие простого условного эксперимента, диагностического для $[\mathfrak{A}]$. Теорема доказана.

Теорема 2.11 [4]. Если $\mathfrak{A}$ — автомат с n попарно отличимыми состояниями, то для $[\mathfrak{A}]$ существует кратный безусловный диагностический эксперимент длины $n-1$ и для некоторого автомата $\mathfrak{A}$ с n состояниями эта оценка длины как безусловного, так и условного экспериментов не может быть понижена.

Доказательство. Как установлено в теореме 2.3, любые два различных состояния автомата $\mathfrak{A}$ отличимы словом длины $n-1$. Поэтому в качестве кратного эксперимента, диагностического для $\mathfrak{A}$, достаточно взять множество всех слов длины $n-1$. Пример, приведенный после доказательства теоремы 2.3, показывает, что эта оценка длины не может быть понижена.

Теорема 2.12 [4, 6]. Если $\mathfrak{A}$ — автомат с n попарно отличимыми состояниями, то для $[\mathfrak{A}]$ существует условный установочный эксперимент длины $n(n-1)/2$ и для некоторого автомата $\mathfrak{A}$ с n состояниями эта оценка не может быть понижена.

Доказательство. Пусть $\mathfrak{A} = (A, Q, B, \varphi, \psi)$; опуская тривиальный случай $n=1$, будем считать $n \geqslant 2$. Рассмотрим простой условный эксперимент Φ, определяемый следующим образом. Пусть $\alpha \in A^*$, $\beta \in B^*$ и $|\alpha| = |\beta|$. Введем обозначения: $\mathscr{L}'(\alpha, \beta) = \{q : q \in Q,\ \bar\psi(q, \alpha) = \beta\}$; $\mathscr{L}(\alpha, \beta) = \{\varphi(q, \alpha) : q \in \mathscr{L}'(\alpha, \beta)\}$. Если $|\mathscr{L}(\alpha, \beta)| \leqslant 1$, то значение $\Phi((\alpha, \beta))$ не определено. Если же $|\mathscr{L}(\alpha, \beta)| \geqslant 2$, то рассматриваем слово $\gamma \in A^*$ наименьшей длины, для которого существуют различимые этим словом состояния q_1 и q_2 из $\mathscr{L}(\alpha, \beta)$ (берем произвольное такое слово), и полагаем по определению $\Phi((\alpha, \beta))$ равным первой букве этого слова.

Предположим, что эксперимент Φ применим к инициальному автомату $\mathfrak{A}_{q_0}$ $(q_0 \in Q)$ и (α, β) — результат применения Φ к $\mathfrak{A}_{q_0}$. Тогда $q_0 \in \mathscr{L}'(\alpha, \beta)$, так что $|\mathscr{L}(\alpha, \beta)| > 0$, а так как $\Phi((\alpha, \beta))$ не определено, то $|\mathscr{L}(\alpha, \beta)| \leqslant 1$. Это означает, что $|\mathscr{L}(\alpha, \beta)| = 1$; $\mathscr{L}(\alpha, \beta) = \{\varphi(q_0, \alpha)\}$, так что результат применения Φ к $\mathfrak{A}_{q_0}$ позволяет однозначно определить автомат $\mathfrak{A}_{\varphi(q_0, \alpha)}$. Для доказательства первой части утверждения теоремы достаточно, таким образом, доказать, что Φ применим к любому инициальному автомату $\mathfrak{A}_{q_0}$ из $[\mathfrak{A}]$ и длина результата применения Φ к $\mathfrak{A}_{q_0}$ не превосходит $n(n-1)/2$.

Пусть $q_0 \in Q$; рассмотрим последовательность $a = a(1), a(2), a(3), \dots$, где $a(1) = \Phi((\Lambda, \Lambda))$ и $a(i+1) = \Phi((a(1) \dots a(i),$

$\bar{\psi}(q_0, a(1)\ldots a(i))))$. Обозначим $\alpha_i = a(1)\ldots a(i)$; $\beta_i = \bar{\psi}(q_0, \alpha_i) = b(1)\ldots b(i)$; $\mathscr{L}'_i = \mathscr{L}'(\alpha_i, \beta_i)$ и $\mathscr{L}_i = \mathscr{L}(\alpha_i, \beta_i)$ $(i=0, 1, 2, \ldots)$. Очевидно, что $\mathscr{L}'_{i+1} \subseteq \mathscr{L}'_i$ и

(*) $\quad \mathscr{L}_{i+1} = \{\varphi(q, a(i+1)) : q \in \mathscr{L}_i, \ \psi(q, a(i+1)) = b(i+1)\}$,

откуда $|\mathscr{L}_{i+1}| \leqslant |\mathscr{L}_i|$. Предположим, что длина последовательности α больше, чем $n(n-1)/2$, и покажем, что тогда для любого $i=1, 2, \ldots, n-1$ выполняется $|\mathscr{L}_{\frac{i(i+1)}{2}}| \leqslant n-i$. При $i=0$ справедливость данного неравенства очевидна. Пусть оно верно при некотором $i \leqslant n-2$.

Если $|\mathscr{L}_{\frac{i(i+1)}{2}}| \leqslant n-i-1$, то $|\mathscr{L}_{\frac{(i+1)(i+2)}{2}}| \leqslant |\mathscr{L}_{\frac{i(i+1)}{2}}| \leqslant n-(i+1)$, что и требовалось. Пусть поэтому $|\mathscr{L}_{\frac{i(i+1)}{2}}| = n-i$. Рассмотрим отношение эквивалентности R_{i+1}, введенное при доказательстве теоремы 2.3, где было установлено, что либо определяемое отношением R_{i+1} разбиение P_{i+1} имеет не менее чем $i+2$ классов эквивалентности, либо P_{i+1} разбивает Q на одноэлементные подмножества, и тогда с учетом $i \leqslant n-2$ также имеет не менее чем $i+2$ класса эквивалентности. Если $\mathscr{L}_{\frac{i(i+1)}{2}}$ целиком расположено в одном из этих классов, то так как каждый из остальных $(i+1)$ классов имеет хотя бы один элемент, получаем, что в Q имеется не менее чем $|\mathscr{L}_{\frac{i(i+1)}{2}}| + (i+1) = n+1$ элементов, и приходим к противоречию. Поэтому существуют элементы q_1 и q_2 множества $\mathscr{L}_{\frac{i(i+1)}{2}}$, расположенные в разных классах разбиения P_{i+1}, т. е. для некоторого слова $\gamma \in A^*$ длины $i+1$ имеем $\bar{\psi}(q_1, \gamma) \neq \bar{\psi}(q_2, \gamma)$. Покажем теперь индукцией по j, что при $0 \leqslant j \leqslant i+1$ либо выполняется $|\mathscr{L}_{\frac{i(i+1)}{2}+j}| < n-i$, либо кратчайшее слово в алфавите A, для которого в $\mathscr{L}_{\frac{i(i+1)}{2}+j}$ найдутся два различимых этим словом состояния, имеет длину не более чем $i+1-j$. При $j=0$ это вытекает из различимости состояний $q_1, q_2 \in \mathscr{L}_{\frac{i(i+1)}{2}}$ словом γ длины $i+1$. Пусть данное утверждение справедливо при некотором $j \leqslant i$, покажем, что оно справедливо для $j+1$. Если $|\mathscr{L}_{\frac{i(i+1)}{2}+j}| < n-i$, то $|\mathscr{L}_{\frac{i(i+1)}{2}+j+1}| \leqslant |\mathscr{L}_{\frac{i(i+1)}{2}+j}| < n-i$, и утверждение доказано. Если же $|\mathscr{L}_{\frac{i(i+1)}{2}+j}| = n-i$, то рассмотрим такое кратчайшее слово $c(1)c(2)\ldots c(t)$, для которого существуют различимые этим словом состояния $q, q' \in \mathscr{L}_{\frac{i(i+1)}{2}+j}$, что $c(1) = \Phi((\alpha_{\frac{i(i+1)}{2}+j},$

$\beta_{\frac{i(i+1)}{2}+j}))=a\left(\frac{i(i+1)}{2}+j+1\right)$; длина t этого слова $\leqslant i+$ $+1-j$. Если $t=1$, то $\psi(q, c(1))\neq\psi(q', c(1))$, т. е. либо $\psi(q, c(1))$, либо $\psi(q', c(1))$ отлично от $b\left(\frac{i(i+1)}{2}+j+1\right)$, и из (*) находим, что $|\mathscr{L}_{\frac{i(i+1)}{2}+j+1}|<|\mathscr{L}_{\frac{i(i+1)}{2}+j}|=n-i$. Если же $t>1$, то слово $c(2)\ldots c(t)$ различает состояния $\varphi(q, c(1))$ и $\varphi(q', c(1))$, входящие в $\mathscr{L}_{\frac{i(i+1)}{2}+j+1}$, и длина $t-1$ этого слова не более $i+1-$ $-(j+1)$, что и требовалось. В частности, при $j=i+1$ имеем, что либо $|\mathscr{L}_{\frac{i(i+1)}{2}+i+1}|<n-i$, либо в $\mathscr{L}_{\frac{i(i+1)}{2}+i+1}=\mathscr{L}_{\frac{(i+1)(i+2)}{2}}$ имеются два состояния, отличимых словом длины $(i+1)-(i+1)=0$. Последнее невозможно, так что $|\mathscr{L}_{\frac{(i+1)(i+2)}{2}}|\leqslant n-(i+1)$. Таким образом, доказано, что при $i=0, 1, \ldots, n-1$ имеет место $|\mathscr{L}_{\frac{i(i+1)}{2}}|\leqslant$ $\leqslant n-i$. В частности, $|\mathscr{L}_{\frac{n(n-1)}{2}}|\leqslant 1$ и $a_{\frac{n(n-1)}{2}+1}=\Phi((\alpha_{\frac{n(n-1)}{2}}, \beta_{\frac{n(n-1)}{2}}))$ не определено, так что длина α оказывается не превосходящей $n(n-1)/2$, и приходим к противоречию. Полученное противоречие доказывает, что длина α, равная длине результата применения Φ к $\mathfrak{A}_{q_0}$, не превосходит $n(n-1)/2$, и первая часть утверждения теоремы доказана. Для доказательства, того что оценка $n(n-1)/2$ в общем случае не улучшаема, рассмотрим автомат $\mathfrak{A}=$ $=(A, Q, B, \varphi, \psi)$, диаграмма Мура которого приведена на

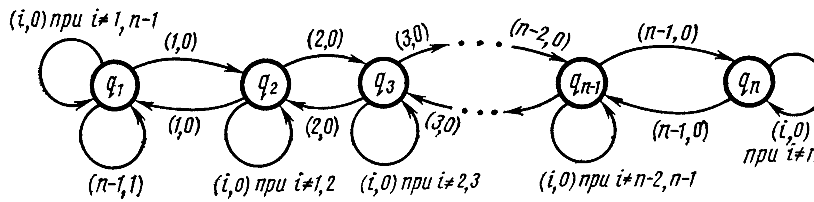

Рис. 2.11.

рис. 2.11. У этого автомата $A=\{1, 2, \ldots, n-1\}$; $Q=\{q_1, \ldots, q_n\}$; $B=$ $=\{0, 1\}$. Из диаграммы видно, что при $a\in A$ и $q_i\neq q_j$ выполняется $\varphi(q_i, a)\neq\varphi(q_j, a)$; отсюда вытекает, что и для любого слова $\alpha\in A^*$ при $q_i\neq q_j$ имеет место $\varphi(q_i, \alpha)\neq\varphi(q_j, \alpha)$. Пусть Φ — некоторый установочный эксперимент для $\mathfrak{A}$. Рассмотрим простой условный эксперимент Φ', такой, что $\Phi'((\alpha, \beta))=\Phi((\alpha, \beta))$, если $\Phi((\alpha, \beta))$ определено и слово β состоит из одних нулей, иначе $\Phi'((\alpha, \beta))$ не определено. Если $q\in Q$ и $(\tilde{\alpha}, \tilde{\beta})$ — результат применения Φ к $\mathfrak{A}_q$, причем $\tilde{\beta}$ состоит из одних нулей, то, очевидно, результат применения Φ' к $\mathfrak{A}_q$ также есть $(\tilde{\alpha}, \tilde{\beta})$. Если же в слове $\tilde{\beta}$ встречаются единицы и первая из них стоит на i-м месте, то результат применения Φ' к $\mathfrak{A}_q$ есть $(\overline{\overline{\tilde{\alpha}|}}_i, \overline{\overline{\tilde{\beta}|}}_i)$. В первом случае результат $(\tilde{\alpha}, \tilde{\beta})$ применения Φ' к $\mathfrak{A}_q$ позволяет однозначно установить состояние $\varphi(q, \tilde{\alpha})$ в силу того, что этот результат совпадает с результатом применения Φ к $\mathfrak{A}_q$ и эксперимент Φ — установочный; во втором случае слово $\overline{\overline{\tilde{\beta}|}}_i$ заканчивается на единицу, а так как единственный переход в диаграмме автомата $\mathfrak{A}$ с появлением 1 на выходе автомата есть переход из состояния q_1 в состояние q_1 под действием входного символа $n-1$, то получаем, что $\varphi(q, \overline{\overline{\tilde{\alpha}|}}_i)$ есть q_1, и результат применения эксперимента Φ' к $\mathfrak{A}_q$ снова позволяет однозначно определить заключительное состояние автомата $\mathfrak{A}$. Таким образом, Φ' — установочный для $\mathfrak{A}$ эксперимент, причем длина его, очевидно, не превосходит длины эксперимента Φ. Обозначим $(\hat{\alpha}_i, \hat{\beta}_i)$ результат применения Φ' к $\mathfrak{A}_{q_i}$ $(i=1, 2, ..., n)$; $\hat{\alpha}_i = a_i(1) ... a_i(l_i)$; $\hat{\beta}_i = b_i(1) ... b_i(l_i)$. Пусть $i \neq j$ и $l_i \leqslant l_j$. Тогда $b_i(1) = ... = b_i(l_i - 1) = b_j(1) = ... = b_j(l_j - 1) = 0$, а так как $a_i(1) = a_j(1) = \Phi'((\Lambda, \Lambda))$ и из $\overline{\overline{\hat{\alpha}_i|}}_k = \overline{\overline{\hat{\alpha}_j|}}_k$ при $k \leqslant l_i - 1$ вытекает

$$a_i(k+1) = \Phi'((\overline{\overline{\hat{\alpha}_i|}}_k, \underbrace{0 \ldots 0}_{k})) = \Phi'((\overline{\overline{\hat{\alpha}_j|}}_k, \underbrace{0 \ldots 0}_{k})) = a_j(k+1),$$ то

имеем $a_i(k) = a_j(k)$ для всех $k = 1, 2, ..., l_i$, и слово $\hat{\alpha}_i$ есть начало слова $\hat{\alpha}_j$. Так как под действием входного слова $\hat{\alpha}_i$ автомат $\mathfrak{A}$ переходит из различных состояний q_i и q_j в различные состояния $\varphi(q_i, \hat{\alpha}_i)$ и $\varphi(q_j, \hat{\alpha}_i)$, то для возможности однозначного восстановления $\varphi(q_i, \hat{\alpha}_i)$ по паре $(\hat{\alpha}_i, \hat{\beta}_i)$ необходимо, чтобы выполнялось $\hat{\beta}_i \neq \overline{\overline{\hat{\beta}_j|}}_{l_i}$, т. е. $b_i(l_i) \neq b_j(l_i)$. В частности, при $l_i < l_j$ получаем, что $b_i(l_i) = 1$, а при $l_i = l_j$ получаем $\hat{\beta}_i \neq \hat{\beta}_j$. Из последнего следует, что при $i \neq j$ пары $(\hat{\alpha}_i, \hat{\beta}_i)$ и $(\hat{\alpha}_j, \hat{\beta}_j)$ различны. Пусть $l_r = \max\limits_{1 \leqslant i \leqslant n} l_i$, тогда каждое слово $\hat{\alpha}_i$ есть начало слова $\hat{\alpha}_r$ (быть может, совпадающее с $\hat{\alpha}_r$), причем если $l_i < l_r$, то $\hat{\beta}_i$ оканчивается на 1. При $i_0 \neq r$ и $l_{i_0} = l_r$ слова $\hat{\alpha}_{i_0}$ и $\hat{\alpha}_n$ совпадают, а слова $\hat{\beta}_{i_0}$ и $\hat{\beta}_r$ отличаются лишь в последнем символе, так что существует не более одного такого i_0, и если оно существует, то можно считать r выбранным так, что слово $\hat{\beta}_r$ оканчивается нулем, а $\hat{\beta}_{i_0}$ единицей. В результате при $i = 1, ..., r-1, r+1, ..., n$ имеем $\hat{\beta}_i = \underbrace{0 \ldots 0\, 1}_{l_i}$, а так как $(\hat{\alpha}_i, \hat{\beta}_i) \neq (\hat{\alpha}_j, \hat{\beta}_j)$ при $i \neq j$, то длины слов $\hat{\alpha}_i$ при указанных i различны; эти слова суть некоторые различные непустые начала слова $\hat{\alpha}_r$. Кроме того, как уже устанавливалось выше, так как при $i = 1, 2, ..., r-1, r+1, ..., n$ слово $\hat{\beta}_i$ оканчивается на 1; то

$\varphi(q_i, \hat{\alpha}_i)$ есть q_1 и $\hat{\alpha}_i$ оканчивается на $n-1$. Из диаграммы автомата $\mathfrak{A}$ видно, что при переходе от состояния q_i, где $i>1$, к состоянию q_1 обязательно возникают все промежуточные состояния $q_{i-1}, q_{i-2}, ..., q_2, q_1$. Поэтому можно выделить такой непустой начальный отрезок $\hat{\alpha}_{ij}$ входного слова $\hat{\alpha}_i$ (а значит, и слова $\hat{\alpha}_r$), под действием которого автомат впервые перейдет из состояния q_i в состояние q_j, где $i=2, ..., r-1, r+1, ..., n$; $j=1, 2, ..., i-1$. Из рис. 2.11 видно, что $\hat{\alpha}_{ij}$ оканчивается символом j, так что при $j_1 \neq j_2$ слова $\hat{\alpha}_{i_1 j_1}$ и $\hat{\alpha}_{i_2 j_2}$ различны. Если же $j_1=j_2$ и $i_1 \neq i_2$, то $\varphi(q_{i_1}, \hat{\alpha}_{i_1 j_1}) = \varphi(q_{i_2}, \hat{\alpha}_{i_2 j_2}) = q_{j_1}$, причем $\varphi(q_{i_1}, \hat{\alpha}_{i_1 j_1}) \neq \varphi(q_{i_2}, \hat{\alpha}_{i_1 j_1})$, откуда $\hat{\alpha}_{i_1 j_1} \neq \hat{\alpha}_{i_2 j_2}$. Поэтому все слова $\hat{\alpha}_{ij}$, где $i=2, ..., r-1, r+1, ...$ $..., n$; $j=1, 2, ..., i-1$, попарно различны. Предположим сначала, что $r=n$. В этом случае каждое слово $\hat{\alpha}_{ij}$ заканчивается символом $j<n-1$ и поэтому отличается от любого слова $\hat{\alpha}_k$ ($k=1, ...$ $..., r-1, r+1, ..., n$). Таким образом, слова $\hat{\alpha}_k$ и $\hat{\alpha}_{ij}$ суть различные непустые начала слова $\hat{\alpha}_n$; число этих начал равно $\sum\limits_{i=2}^{n-1}(i-1)+(n-$ $-1)=n(n-1)/2$, откуда вытекает, что длина l_r слова $\hat{\alpha}_r$ не менее чем $n(n-1)/2$. Пусть теперь $r<n$. Тогда равенство $\hat{\alpha}_{ij}=\hat{\alpha}_k$ может выполняться только при $j=n-1$, $i=n$, так что не более чем одно из слов $\hat{\alpha}_{ij}$ может совпадать с каким-либо словом $\hat{\alpha}_k$, и число различных слов $\hat{\alpha}_{ij}$, $\hat{\alpha}_k$ не менее

$$\sum_{i \in \{2,\dots,r-1,r+1,\dots,n\}}(i-1) + (n-2) = \frac{n(n-1)}{2} - (r-1) + (n-2) =$$

$$= \frac{n(n-1)}{2} + (n-r-1) \geqslant \frac{n(n-1)}{2},$$

ибо $r \leqslant n-1$, и снова $l_r \geqslant n(n-1)/2$. Таким образом, оказывается, что длина l_r слова $\hat{\alpha}_r$, равная $\max\limits_{1 \leqslant i \leqslant n} l_i$, т. е. равная длине эксперимента Φ' относительно $[\mathfrak{A}]$, не менее чем $n(n-1)/2$. Теорема доказана.

УПРАЖНЕНИЯ

1. Найти наименьшую длину кратного безусловного диагностического для $[\mathfrak{A}]$ эксперимента, если $\mathfrak{A}$ — автомат, диаграмма которого указана на рис. 1.14, а. Существует ли в этом случае простой безусловный диагностический для $[\mathfrak{A}]$ эксперимент?
2. Найти наименьшую длину условного установочного эксперимента для $[\mathfrak{A}]$, где $\mathfrak{A}$ — автомат, диаграмма которого указана на рис. 1.19. Какова наименьшая длина безусловного установочного эксперимента для класса $[\mathfrak{A}]$ в этом случае?
3. Найти наименьший объем кратного безусловного эксперимента,

диагностического для $[\mathfrak{A}]$, где $\mathfrak{A}$ — автомат, диаграмма которого указана на рис. 1.27.

4. Существует ли конечный автомат $\mathfrak{A}$ с 4 попарно отличимыми состояниями, у которого некоторый кратный безусловный эксперимент, диагностический для $[\mathfrak{A}]$ и имеющий наименьший возможный объем, содержит слово длины, большей чем 3?
5. Существует ли конечный автомат $\mathfrak{A}$ с 4 состояниями, не имеющий кратного безусловного эксперимента, диагностического для $\mathfrak{A}$ и состоящего из 4 слов длины 3?

§ 4. НЕКОТОРЫЕ ВСПОМОГАТЕЛЬНЫЕ УТВЕРЖДЕНИЯ

В этом параграфе будет установлен ряд вспомогательных утверждений, используемых при оценке сложности экспериментов с автоматами. Эти утверждения, а также полученные с их помощью оценки принадлежат М. П. Василевскому [7, 8].

В качестве множества $\mathfrak{M}$ инициальных автоматов, к которому относится исследуемый автомат $\mathfrak{A}_q$, будем далее рассматривать множества $\mathcal{K}_{m,n}$ и $\mathcal{K}_{m,n,l}$ автоматов, у которых m есть число входных символов, n — верхняя граница числа состояний и l — верхняя граница числа выходных символов. Таким образом, вся имеющаяся до эксперимента информация об исследуемом автомате $\mathfrak{A}_q$ сводится лишь к некоторым оценкам числа состояний, входных и выходных символов этого автомата.

Более формально, $\mathcal{K}_{m,n}$ есть некоторое множество попарно отличимых инициальных автоматов $\mathfrak{A}_q=(A, Q, B, \varphi, \psi, q)$ приведенного вида, у которых $A=\{1, ..., m\}$; $|Q|\leqslant n$; $B\subseteq\{1, 2, 3, ...\}$, причем для любого автомата $\mathfrak{A}'_{q'}$ вида $(A', Q', B', \varphi', \psi', q')$, у которого $A'=\{1, ..., m\}$; $|Q'|\leqslant n$; $B'\subseteq\{1, 2, 3, ...\}$, в $\mathcal{K}_{m,n}$ существует неотличимый от $\mathfrak{A}'_{q'}$ автомат. Говоря иными словами, для произвольного класса неотличимых друг от друга инициальных автоматов вида $(\{1, ..., m\}, Q, B, \varphi, \psi, q)$, где $B\subseteq\{1, 2, 3, ...\}$, в $\mathcal{K}_{m,n}$ имеется ровно один представитель этого класса; очевидно, что в качестве такого представителя всегда может быть выбран автомат приведенного вида.

Посредством $\mathcal{K}_{m,n,l}$ обозначается подмножество множества $\mathcal{K}_{m,n}$, образованное всеми такими автоматами $\mathfrak{A}_q\in\mathcal{K}_{m,n}$; $\mathfrak{A}_q=(A, Q, B, \varphi, \psi, q)$, у которых $|B|\leqslant l$. В этом и в следующем параграфах посредством A обозначаем множество $\{1, ..., m\}$. Если не оговорено противное, посредством $\mathfrak{A}_{q_0}$, $\mathfrak{B}_{q_0}$ обозначаем инициальные автоматы из множества $\mathcal{K}_{m,n}$, а посредством $\mathfrak{A}$, $\mathfrak{B}$ — такие автоматы, что при некоторых q_0, q_1 имеет место $\mathfrak{A}_{q_0}\in\mathcal{K}_{m,n}$; $\mathfrak{B}_{q_1}\in\mathcal{K}_{m,n}$. На множестве слов A^* введем **отношение лексикографического порядка.** Если $\alpha^{k_1}=a(1)\ldots a(k_1)$; $\beta^{k_2}=b(1)\ldots b(k_2)$ — слова из A^*, причем либо $k_1<k_2$, либо $k_1=k_2$ и при некотором $i\in\{1, ..., k_2\}$ выполняется $a(1)=b(1)$, ..., $a(i-1)=b(i-1)$, $a(i)<b(i)$, то говорим, что слово α^{k_1} предшествует в лексикографическом порядке слову β^{k_2}.

Рассмотрим входные слова $v_0, \ldots, v_i, \ldots, v_s$, такие, что v_i — первое в лексикографическом порядке слово, переводящее автомат $\mathfrak{A}_{q_0}$ в состояние, отличное от состояний, в которые переводят $\mathfrak{A}_{q_0}$ слова $v_0, \ldots, v_{i-1}$ (s — наибольшее возможное). Обозначим $v_i = v_i^{\mathfrak{A}_{q_0}}$; $\{v_0, \ldots, v_s\} = V(\mathfrak{A}_{q_0})$; $\{v_0, \ldots, v_i\} = V(\mathfrak{A}_{q_0}, i)$ при $i \leqslant s$ и $V(\mathfrak{A}_{q_0}, i) = V(\mathfrak{A}_{q_0})$ при $i > s$.

Лемма 2.4. Пусть для инициального автомата $\mathfrak{A}_{q_0}$ и натурального i существует $v_{i+1}^{\mathfrak{A}_{q_0}}$. Тогда $v_{i+1}^{\mathfrak{A}_{q_0}}$ представимо в виде wa, где $w \in V(\mathfrak{A}_{q_0}, i)$ и $a \in A$.

Доказательство. Пусть $v_{i+1}^{\mathfrak{A}_{q_0}} = wa$, где $a \in A$. Покажем, что $w \in V(\mathfrak{A}_{q_0}, i)$. Если $w \notin V(\mathfrak{A}_{q_0}, i)$, то существует w', $w' \in V(\mathfrak{A}_{q_0}, i)$, переводящее автомат $\mathfrak{A}_{q_0}$ в то же состояние, что и w, и при замене w на w' в $v_{i+1}^{\mathfrak{A}_{q_0}}$ получили бы слово, расположенное в лексикографическом порядке раньше, чем v $v_{i+1}^{\mathfrak{A}_{q_0}}$, что невозможно.

Следствие. 1) $|v_i^{\mathfrak{A}_{q_0}}| \leqslant i$ при $i = 0, 1, \ldots, s$;

2) $V(\mathfrak{A}_{q_0}, i+1) \subseteq V(\mathfrak{A}_{q_0}, i) \cup V(\mathfrak{A}_{q_0}, i) \cdot A$ при $i = 0, 1, \ldots, s-1$.

Обозначим $A^0 = \{\Lambda\}$.

Лемма 2.5. Пусть множество входных слов V, содержащее пустое слово, переводит автомат $\mathfrak{A}_{q_0}$ в не менее чем $i+1$ состояние. Тогда $V(A^0 \cup A \cup \ldots \cup A^{n-i-1})$ переводит $\mathfrak{A}_{q_0}$ во все достижимые из q_0 состояния.

Доказательство. Пусть V переводит $\mathfrak{A}_{q_0}$ не во все состояния, достижимые из q_0. Если $V \cup VA$ переводит $\mathfrak{A}_{q_0}$ лишь в те же состояния, что и V, то и $V \cup VA \cup VA^2 \cup \ldots \cup VA^j$ при любом j переводит $\mathfrak{A}_{q_0}$ в те же состояния. Но $\Lambda \subset V$, так что A^j при любом j переводит $\mathfrak{A}_{q_0}$ в те же состояния — противоречие. Следовательно, $V \cup VA$ переводит $\mathfrak{A}_{q_0}$ не менее чем в $i+2$ состояния, и далее рассуждаем по индукции.

Следствие. При $0 \leqslant i \leqslant n-1$ множество $V(\mathfrak{A}_{q_0}, i)(A^0 \cup A \cup \ldots \cup A^{n-i-1})$ переводит $\mathfrak{A}_{q_0}$ во все состояния, достижимые из q_0.

Рассмотрим последовательность $w_0, w_1, \ldots, w_l$ входных слов, такую, что $w_0 = \Lambda$ и w_i — первое в лексикографическом порядке слово, различающее два состояния автомата $\mathfrak{A}$, не различимые предыдущими словами $w_0, w_1, \ldots, w_{i-1}$ (l — наибольшее возможное). Обозначим $w_i = w_i^{\mathfrak{A}}$; $\{w_0, \ldots, w_l\} = W(\mathfrak{A})$; $\{w_0, \ldots, w_i\} = W(\mathfrak{A}, i)$; при $i \leqslant l$ и $W(\mathfrak{A}, i) = W(\mathfrak{A})$ при $i > l$. Если $M \subseteq A^*$; q_1 и q_2 — состояния автоматов $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ и $\mathfrak{B} = (A, Q', B', \varphi', \psi')$, причем существует слово $\alpha \in M$, такое, что $\psi(q_1, \alpha) \neq \psi'(q_2, \alpha)$, то говорим, что состояния q_1 и q_2 **различимы множеством** M.

Лемма 2.6. Пусть для автомата $\mathfrak{A}$ и натурального i существует $w_{i+1}^{\mathfrak{A}}$. Тогда $w_{i+1}^{\mathfrak{A}} \in AW(\mathfrak{A}, i)$.

Доказательство. Пусть $w_{i+1}^{\mathfrak{A}} = aw$, где $a \in A$. Пусть $w_{i+1}^{\mathfrak{A}}$ различает состояния q' и q'' автомата $\mathfrak{A}$, не различимые множеством

$W(\mathfrak{A}, i)$. Если $w=\Lambda$, то $w \in W(\mathfrak{A}, i)$. Если $w \neq \Lambda$, то a не различает q' и q''. Состояния $\varphi(q', a)$ и $\varphi(q'', a)$ различимы множеством $W(\mathfrak{A}, i)$. Если $w \notin W(\mathfrak{A}, i)$, то существует $w' \in W(\mathfrak{A}, i)$, различающее $\varphi(q', a)$ и $\varphi(q'', a)$ и расположенное в лексикографическом порядке раньше, чем w. Но тогда aw', расположенное раньше, чем $w_{i+1}^{\mathfrak{A}} = aw$, различает q' и q'', что противоречит определению $w_{i+1}^{\mathfrak{A}}$. Лемма доказана.

Для обозначения того факта, что каждое слово из множества U есть начало некоторого слова множества V, где $U, V \subseteq A^*$, используем запись $U \leqslant V$. Вместо $\{u\} \leqslant V$ иногда пишем также $u \leqslant V$.

Следствие. 1) $|w_i^{\mathfrak{A}}| \leqslant i$ при всех $i=0, 1, ..., l-1$;

2) $W(\mathfrak{A}, i+1) \leqslant AW(\mathfrak{A}, i)$ при всех $i=0, 1, ..., l-1$.

Лемма 2.7. Пусть неразличимость множеством W, $W \subseteq A^*$, разбивает состояния автомата $\mathfrak{A}$ по меньшей мере на $i+1$ класс эквивалентности и $W \leqslant AW$. Тогда множество $A^{n-i-1}W$ различает любые два состояния автомата $\mathfrak{A}$.

Доказательство. Пусть $\mathfrak{A}$ имеет состояния, не различимые множеством W (в противном случае справедливость леммы очевидна). Если AW различает те и только те состояния $\mathfrak{A}$, которые различает W, то и A^2W различает те же состояния (если A^2W различает q' и q'', то или некоторый символ $a \in A$ различает их, и тогда AW их различает, или, при некотором $a \in A$, AW различает $\varphi(q', a)$ и $\varphi(q'', a)$, но тогда их различает и W, следовательно, AW различает q' и q''). Продолжая это рассуждение, убеждаемся, что для любого j $A^jW \geqslant A^j$ различает те и только те состояния, которые различает W, что противоречит предположению о наличии у $\mathfrak{A}$ состояний, не различимых множеством W. Следовательно, AW различает некоторую пару состояний, не различимую множеством W. Так как $AW \geqslant W$ различает и все состояния, различимые множеством W, неразличимость множеством AW разбивает состояния $\mathfrak{A}$ по меньшей мере на $i+2$ класса, и далее рассуждаем по индукции.

Следствие. При $0 \leqslant i \leqslant n-1$ множество $A^{n-i-1}W(\mathfrak{A}, i)$ различает любую пару различных состояний автомата $\mathfrak{A}$

Утверждение 1. Пусть $W \leqslant AW$, $w(1)...w(l) \in W$, $i \leqslant l$. Тогда $w(i)...w(l) \leqslant W$.

При $i=1$ утверждение очевидно. Пусть оно верно для некоторого i. Это означает, что существует $w' \in W$, такое, что $w(i)...$ $...w(l) = w'(1)...w'(l-i+1)$. Так как $W \leqslant AW$, то существует $w'' \in$ $\in W$, такое, что $w'(1)...w'(l-i+1) = w'(1)w''(1)...w''(l-i)$. Но тогда $w(i+1)...w(l) = w'(2)...w'(l+i-1) = w''(1)...w''(l-i) \leqslant W$. Если $U \subseteq A^*$, то посредством $[U]$ будем обозначать наименьшее подмножество V множества U, такое, что $U \leqslant V$.

Лемма 2.8. Пусть $V \subseteq A^*$, $V=\{v_0, ..., v_{s-1}\}$, причем для любого $v \in V$ имеет место $v \in (V \setminus \{v\}) \cdot A$. Пусть множество W, $W \subseteq A^*$, таково, что $W \leqslant AW$. Тогда:

(1) $|[VA]| \leqslant s(m-1)+1$;

(2) при любых i, j, таких, что $1 \leqslant i \leqslant j$, имеет место

$$V(A^0 \cup A \cup \ldots \cup A^i)\, W \leqslant [VA]\, A^{j-1} W.$$

Доказательство. При $s=1$ $[VA]=v_0,A$, $|v_0A|=m=1(m-1)+1$. Пусть (1) доказано для некоторого s и пусть $V=\{v_0, \ldots, v_{s-1}, v_s\}$, где слова расположены в лексикографическом порядке. Тогда существует такое $v \in \{v_0, \ldots, v_{s-1}\}$ и такое $a \in A$, что $v_s = va$. Так как $va \notin V \setminus \{v_s\}$, то $va \in [(V \setminus \{v_s\})A]$. Далее $VA=(V \setminus \{v_s, v\})A \cup vA \cup v_sA \leqslant (V \setminus \{v_s, \quad v\})A \cup v(A \setminus \{a\}) \cup vaA \leqslant [(V \setminus \{v_s\})A \setminus \{va\}] \cup vaA$. Очевидно, $|vaA|=m$. Так как $va \in [(V \setminus \{v_s\})A]$, то $|[(V \setminus \{v_s\})A \setminus \setminus \{va\}]| = |[(V \setminus \{v_s\})A]|-1 \leqslant s(m-1)$, поэтому

$$|[VA]| \leqslant s(m-1)+m=(s+1)(m-1)+1.$$

Докажем (2). Пусть $v\alpha w$ — произвольное слово из $V(A^0 \cup A^1 \cup \ldots \cup A^i)\, W$; $v \in V$; $\alpha \in A^0 \cup A^1 \cup \ldots \cup A^i$; $w=w(1) \ldots w(l) \in W$. Рассмотрим два случая:

1) $v\alpha \notin V$. Тогда существует k $(0 \leqslant k \leqslant i-1 \leqslant j-1)$, такое, что $v\alpha \in [VA]\, A^k$, и получаем: $v\alpha w \in [VA]\, A^k W \leqslant [VA]\, A^k A W = [VA]\, A^{k+1} W \leqslant \ldots \leqslant [VA]\, A^{j-1} W$.

2) $v\alpha \in V$. Если $v\alpha w \leqslant [VA]$, то $v\alpha w \leqslant [VA]\, A^{j-1}W$. В противном случае существует такое $k \leqslant l-1$, что $v\alpha w(1) \ldots w(k) \in [VA]$, но $v\alpha w(1) \ldots w(k+1) \notin [VA]$. Согласно утверждению 1, $w(k+1) \ldots \ldots w(l) \leqslant W$, поэтому $v\alpha w \leqslant [VA]\, W \leqslant [VA]\, AW \leqslant \ldots \leqslant [VA]\, A^{j-1} W$.

Утверждение 2. Если $V(\mathfrak{A}_{q_0}, i) = V(\mathfrak{B}_{q_0}, i)$, но $V(\mathfrak{A}_{q_0}, i+1) \neq \neq V(\mathfrak{A}_{q_0}, i+1)$, то множество $V(\mathfrak{A}_{q_0}, i) \cup V(\mathfrak{A}_{q_0}, i)\, A \supseteq V(\mathfrak{B}_{q_0}, i) \cup \cup V(\mathfrak{B}_{q_0}, i+1)$ содержит два слова v и v', такие, что состояния $\varphi(q_0, v)$, $\varphi(q_0, v')$ совпадают в одном из автоматов $\mathfrak{A}_{q_0}$, $\mathfrak{B}_{q_0}$ и не совпадают в другом.

Доказательство. В качестве v берем то из слов $v_{i+1}^{\mathfrak{A}_{q_0}}$, $v_{i+1}^{\mathfrak{B}_{q_0}}$ (хотя бы одно из них существует), которое идет раньше в лексикографическом порядке. Пусть это $v_{i+1}^{\mathfrak{A}_{q_0}}$. Тогда в качестве v' выбираем то из слов $v_0^{\mathfrak{B}_{q_0}}, \ldots, v_i^{\mathfrak{B}_{q_0}}$, которое переводит $\mathfrak{B}_{q_0}$ в состояние $\varphi_{\mathfrak{B}}(q_0, v_{i+1}^{\mathfrak{A}_{q_0}})$

Утверждение 3. Если $W(\mathfrak{A}, i) = W(\mathfrak{B}, i)$, но $W(\mathfrak{A}, i+1) \neq \neq W(\mathfrak{B}, i+1)$, то один из автоматов $\mathfrak{A}$, $\mathfrak{B}$ имеет состояние, отличимое от любого состояния другого множеством $AW(\mathfrak{A}, i) = = AW(\mathfrak{B}, i)$.

Доказательство. Пусть $w_{i+1}^{\mathfrak{A}}$ расположено раньше, чем $w_{i+1}^{\mathfrak{B}}$ (или $w_{i+1}^{\mathfrak{B}}$ не существует). Тогда неразличимость множеством $W(\mathfrak{A}, i+1)$ разбивает состояния $\mathfrak{B}$ на такие же классы, как и неразличимость множеством $W(\mathfrak{A}, i)$. Множество $W(\mathfrak{A}, i)$ различает любое состояние $\mathfrak{A}$ со всеми состояниями $\mathfrak{B}$, кроме, быть может, состояний одного такого класса. Но существуют два состояния автомата $\mathfrak{A}$, различимые словом $w_{i+1}^{\mathfrak{A}}$, но не различимые множеством $W(\mathfrak{A}, i)$. По меньшей мере одно из них различимо множеством $W(\mathfrak{A}, i+1)$ со всеми состояниями автомата $\mathfrak{B}$. Отсюда и из соотношения $W(\mathfrak{A}, \quad i+1) \leqslant AW(\mathfrak{A}, \quad i)$ и вытекает справедливость утверждения.

Лемма 2.9. Пусть $0 \leqslant i \leqslant n-1$, причем существует $v_i^{\mathfrak{A}_{q_0}}$. Пусть $V(\mathfrak{A}_{q_0}, i+1) \neq V(\mathfrak{B}_{q_0}, i+1)$ или $W(\mathfrak{A}, i+1) \neq W(\mathfrak{B}, i+1)$. Тогда множество $V(\mathfrak{A}_{q_0}, i) A^{n-i} W(\mathfrak{A}, i)$ различает $\mathfrak{A}_{q_0}$ и $\mathfrak{B}_{q_0}$.

Доказательство. Для краткости положим $v^{\mathfrak{A}}{}_j^{q^0} = v_j$; $V(\mathfrak{A}_{q_0}\ j) = V_j$, $w^{\mathfrak{A}}{}_j^{q_0} = w_j$; $W(\mathfrak{A}, j) = W_j$ $(j=0, 1, \ldots)$. Рассмотрим три возможные ситуации:

1) Пусть два различных слова из V_i переводят $\mathfrak{B}_{q_0}$ в одно и то же состояние. Согласно следствию леммы 2.7 и определению V_i, соответствующие состояния $\mathfrak{A}_{q_0}$ различимы множеством $A^{n-i-1}W_i$, поэтому $V_i A^{n-i-1} W_i \leqslant V_i A^{n-i} W_i$ различает $\mathfrak{A}_{q_0}$ и $\mathfrak{B}_{q_0}$.

2) Пусть неразличимость множеством W_i разбивает состояния автомата $\mathfrak{B}$ на классы, число которых меньше $i+1$. Так как $v_i{}^{\mathfrak{A}}{}_{q_0}$ существует, неразличимость множеством W_i разбивает состояния $\mathfrak{A}_{q_0}$ по меньшей мере на $i+1$ класс, т. е. из q_0 достижимо по меньшей мере $i+1$ состояние, попарно различимые множеством W_i. Согласно следствию из леммы 2.5, множество $V_i(A^0 \cup A^1 \cup \ldots \cup A^{n-i-1})$ переводит $\mathfrak{A}_{q_0}$ во все эти состояния. Так как по меньшей мере два из соответствующих состояний $\mathfrak{B}_{q_0}$ не различимы множеством W_i, множество $V_i(A^0 \cup A^1 \cup \ldots \cup A^{n-i-1}) W_i \leqslant V_i A^{n-i} W_i$ различает $\mathfrak{A}_{q_0}$ и $\mathfrak{B}_{q_0}$.

3) Пусть V_i переводит $\mathfrak{B}_{q_0}$ в $i+1$ попарно различимых состояний, и пусть неразличимость множеством W_i разбивает состояния $\mathfrak{A}$ по меньшей мере на $i+1$ класс. Тогда $V_i(A^0 \cup A^1 \cup \ldots \cup A^{n-i-1})$ переводит $\mathfrak{A}_{q_0}$ во все его состояния (лемма 2.5) и $A^{n-i-1}W_i$ различает любую пару различных состояний $\mathfrak{B}$ (лемма 2.7). $V(\mathfrak{A}_{q_0}, 0) = V(\mathfrak{B}_{q_0}, 0) = W(\mathfrak{A}, 0) = W(\mathfrak{B}, 0) = \Lambda$. Поэтому если $V_{i+1} \neq V(\mathfrak{B}_{q_0}, i+1)$, то $\exists j (0 \leqslant j \leqslant i)$ $V_j = L(\mathfrak{B}_{q_0}, j)$, но $V_{j+1} \neq V(\mathfrak{B}_{q_0}, j+1)$. Тогда, согласно утверждению 2, $V_j \cup V_j A$ содержит два слова, переводящие один из рассматриваемых автоматов в различимые (а именно множеством $A^{n-i-1}W_i$) состояния, другой — в одинаковые состояния, и множество $(V_j \cup V_j A) A^{n-i-1} W_i \subseteq (V_i \cup V_i A) A^{n-i-1} W_i \leqslant V_i A^{n-i} W_i$ различает $\mathfrak{A}_{q_0}$, $\mathfrak{B}_{q_0}$. Если же $W_{i+1} \neq W(\mathfrak{B}, \quad i+1)$, то существует такое j, что $W_j = W \quad (\mathfrak{B}\ \ j)$, но $W_{j+1} \neq W(\mathfrak{B}, \quad j+1)$. Тогда, согласно утверждению 3, один из рассматриваемых автоматов имеет состояние, отличимое от всех состояний другого множеством AW_j. Некоторое слово множества $V_i(A^0 \cup A^1 \cup \ldots \cup A^{n-i-1})$ переводит этот автомат в такое состояние, поэтому множество $V_i(A^0 \cup A^1 \cup \ldots \cup A^{n-i-1})\ AW_j \leqslant V_i A^{n-i} W_j$ различает $\mathfrak{A}_q$ и $\mathfrak{B}_q$. Лемма доказана.

Обозначим $|\mathfrak{A}|$ число состояний автомата $\mathfrak{A}$.

Лемма 2.10. Множество входных слов $V(\mathfrak{A}_{q_0}) A^{n-|\mathfrak{A}|-1} W(\mathfrak{A})$ различает $\mathfrak{A}_{q_0}$ и все отличные от $\mathfrak{A}_{q_0}$ автоматы $\mathfrak{B}_{q_0}$ из $\mathcal{K}_{m,n}$.

Доказательство. Пусть $\mathfrak{B}_{q_0} \in \mathcal{K}_{m,n}$; $\mathfrak{B}_{q_0} \neq \mathfrak{A}_{q_0}$. Если $V(\mathfrak{A}_{q_0}, |\mathfrak{A}|) \neq V(\mathfrak{B}_{q_0}, |\mathfrak{A}|)$ либо $W(\mathfrak{A}, |\mathfrak{A}|) \neq W(\mathfrak{B}, |\mathfrak{A}|)$, то $V(\mathfrak{A}_{q_0}) A^{n-|\mathfrak{A}|+1} W(\mathfrak{A})$ различает $\mathfrak{A}_{q_0}$ и $\mathfrak{B}_{q_0}$ в силу леммы 2.9 при $i = |\mathfrak{A}| - 1$ (так как

$\mathfrak{A}_{q_0}$ — приведенный, то $v^{\mathfrak{A}_{q_0}}_{|\mathfrak{A}|-1}$ существует). Если $\mathfrak{A}$ и $\mathfrak{B}$ неотличимы, то $\mathfrak{B}_{q_0}$ неотличим от $\mathfrak{A}_{q_i}$ при некотором $i \neq 0$ и $\mathfrak{B}_{q_0}$ различает с $\mathfrak{A}_{q_0}$ множество

$$W(\mathfrak{A}) = AW(\mathfrak{A}) \leqslant V(\mathfrak{A}_{q_0}) A^{n-|\mathfrak{A}|+1} W(\mathfrak{A}).$$

Пусть, наконец, $V(\mathfrak{A}_{q_0}, |\mathfrak{A}|) = V(\mathfrak{B}_{q_0}, |\mathfrak{A}|)$ и $W(\mathfrak{A}, |\mathfrak{A}|) = W(\mathfrak{B}, |\mathfrak{A}|)$, но $\mathfrak{A}$ и $\mathfrak{B}$ не эквивалентны. Так как $V(\mathfrak{A}_{q_0}, |\mathfrak{A}|) = V(\mathfrak{A}_{q_0}, |\mathfrak{A}|-1)$ и $W(\mathfrak{A}, |\mathfrak{A}|) = W(\mathfrak{A}, |\mathfrak{A}|-1)$, то и $V(\mathfrak{B}_{q_0}, |\mathfrak{A}|) = V(\mathfrak{B}_{q_0}, |\mathfrak{A}|-1)$ и $W(\mathfrak{B}, |\mathfrak{A}|) = W(\mathfrak{B}, |\mathfrak{A}|-1)$, следовательно, автомат $\mathfrak{B}$ имеет ровно $|\mathfrak{A}|$ состояний и все они попарно различимы множеством $W(\mathfrak{A})$. Рассмотрим объединенное множество состояний $\mathfrak{A}$ и $\mathfrak{B}$. Если неразличимость множеством $W(\mathfrak{A})$ разбивает его на более чем $|\mathfrak{A}|$ классов, то в одном из автоматов имеется состояние, различимое со всеми состояниями другого множеством $W(\mathfrak{A})$; он переводится в это состояние множеством $V(\mathfrak{A}_{q_0})$, поэтому $V(\mathfrak{A}_{q_0}) W(\mathfrak{A}) \leqslant V(\mathfrak{A}_{q_0}) A^{n-|\mathfrak{A}|+1} W(\mathfrak{A})$ различает $\mathfrak{A}_{q_0}$ и $\mathfrak{B}_{q_0}$. Если же неразличимость множеством $W(\mathfrak{A})$ разбивает его на $|\mathfrak{A}|$ классов, то в каждом из них находится по одному состоянию из $\mathfrak{A}$ и $\mathfrak{B}$. Так как $\mathfrak{A}$ и $\mathfrak{B}$ не эквивалентны, по меньшей мере одна из этих пар состояний различима. Пользуясь теми же рассуждениями, что и при доказательстве леммы 2.7, можно показать, что одна такая пара различима множеством $AW(\mathfrak{A})$, следовательно, $AW(\mathfrak{A})$ различает некоторое состояние $\mathfrak{A}$ и все состояния $\mathfrak{B}$, $V(\mathfrak{A}_{q_0})$ переводит $\mathfrak{A}_{q_0}$ во все его состояния, поэтому $V(\mathfrak{A}_{q_0}) AW(\mathfrak{A}) \leqslant V(\mathfrak{A}_{q_0}) A^{n-|\mathfrak{A}|+1} W(\mathfrak{A})$ различает $\mathfrak{A}_{q_0}$ и $\mathfrak{B}_{q_0}$. Лемма доказана.

Лемма 2.11. Пусть K — конечное множество; $U_1, \ldots, U_p$ — семейство конечных множеств ($p \geqslant 1$), U^* — множество конечных последовательностей (включая пустую) элементов из $U_1 \cup \ldots \cup U_p$; $\mathscr{P}$ — предикат на $K \times U^*$ и выполнены условия:

1) $\forall v \in U^* \exists i \in \{1, \ldots, p\} \forall a \in K \exists u \in U_i \mathscr{P}(a, vu)$;

2) $\forall a \in K \forall v \in U^* \forall u \in U^* (\mathscr{P}(a, v) \Rightarrow \mathscr{P}(a, vu))$.

Тогда $\exists u_0 \in U^* \forall a \in K \mathscr{P}(a, u_0)$, причем длина слова u_0 не превосходит $\left] \max\limits_{1 \leqslant i \leqslant p} |U_i| \ln |K| \right[$.

Доказательство. Обозначим $b = \max\limits_{1 \leqslant i \leqslant p} |U_i|$; $K = K^{(0)}$. Полагая в 1) $v = \Lambda$, находим такое $i_0 \in \{1, \ldots, p\}$, что $\forall a \in K \exists u \in U_{i_0} \mathscr{P}(a, u)$. Обозначив при $u \in U_{i_0}$ посредством $K_u^{(0)}$ множество $\{a \mid a \in K^{(0)} \& \mathscr{P}(a, u)\}$, получим отсюда, что существует $u_1 \in U_{i_0}$, такое, что $|K^{(0)}_{u_1}| \geqslant \frac{|K^{(0)}|}{|U_{i_0}|}$. Полагаем $K^{(1)} = K^{(0)} \setminus K^{(0)}_{u_1}$. Очевидно, $|K^{(1)}| \leqslant$ $\leqslant |K^{(0)}| - \frac{|K^{(0)}|}{|U_{i_0}|} = |K^{(0)}| \left(1 - \frac{1}{|u_{i_0}|}\right) \leqslant |K| \left(1 - \frac{1}{b}\right)$. Пусть уже построены $u_1, \ldots, u_l$, где $u_j \in U_1 \cup \ldots \cup U_p$, а также множество $K^{(l)} \subseteq K$, такие, что $|K^{(l)}| \leqslant |K| \left(1 - \frac{1}{b}\right)^l$ и $\forall a \in K \setminus K^{(l)} \mathscr{P}(a, u_1 \ldots u_l)$.

Используя 1) при $v=u_1 \dots u_l$, находим такое $i_l \in \{1, \dots, p\}$, что $\forall a \in K \; \exists u \in U_{i_l} \mathscr{P}(a, u_1 \dots u_l u)$; при $u \in U_{i_l}$ полагаем $K_u^{(l)} = \{a \mid a \in \in K^{(l)} \& \mathscr{P}(a, u_1 \dots u_l u)\}$ и находим, что существует $u_{l+1} \in U_{i_l}$, для которого $|K_{u_{l+1}}^{(l)}| \geqslant \frac{|K^{(l)}|}{|U_{i_l}|}$. Полагаем $K^{(l+1)} = K^{(l)} \setminus K_{u_{l+1}}^{(l)}$. Очевидно, $|K^{(l+1)}| \leqslant |K^{(l)}| - \frac{|K^{(l)}|}{|U_{i_l}|} \leqslant |K| \left(1 - \frac{1}{b}\right)^{l+1}$. В силу 2) $\forall a \in K \setminus K^{(l+1)} \mathscr{P}(a, u_1 \dots u_l u_{l+1})$. Очевидно, что если при некотором l $|K^{(l)}| < 1$, то в качестве искомого u_0 можно взять слово $u_1 \dots u_l$. Так как $|K^{(l)}| \leqslant |K| \left(1 - \frac{1}{b}\right)^l < |K| e^{-\frac{l}{b}} = e^{\ln|K| - \frac{l}{b}}$, то длина слова u_0 не будет превосходить величины $]b \ln|K|[$ (здесь $]a[$ обозначает наименьшее целое число, большее или равное a). Лемма доказана.

Лемма 2.12. Для произвольных m, n, s $(s \leqslant n)$ существует входное слово α длины, не превышающей $n(n-s+1)m^{n-s+1} \ln n$, обладающее следующим свойством: если автомат $\mathfrak{A}_{q_0}$ имеет сильно связный подавтомат, содержащий не менее чем s состояний, то α переводит $\mathfrak{A}_{q_0}$ в некоторый его сильно связный подавтомат.

Доказательство. Разбиваем все инициальные автоматы из $\mathscr{K}_{m,n}$ имеющие сильно связные подавтоматы с не менее чем s состояниями на классы, относя к одному классу автоматы, которые можно сделать совпадающими путем изменения функций выходов и переименования состояний. Очевидно, любое входное слово одновременно переводит все автоматы одного класса в сильно связные подавтоматы. Обозначим множество этих классов через $\mathscr{K}'$. Легко видеть, что $|\mathscr{K}'| \leqslant n^{mn}$. Применяем лемму 2.11 для $p=1$, $U_1 = A^{n-s}$, $K = \mathscr{K}'$. При $a \in \mathscr{K}'$ и $x \in U_1^*$ полагаем $\mathscr{P}(a, x)$, если входное слово x переводит все автоматы класса a в сильно связные подавтоматы. Так как для автомата из $\mathscr{K}_{m,n}$, содержащего сильно связный подавтомат с не менее чем s состояниями, при произвольной фиксации начального состояния существует входное слово длины $n-s$, переводящее его в сильно связный подавтомат, то условия 1) и 2) леммы 2.11 выполнены, поэтому существует входное слово, переводящее все автоматы классов множества K в сильно связные подавтоматы, и в этом слове использовано не более $]|U_1| \ln |\mathscr{K}'|[$ отрезков из $U_1 = A^{n-s}$, поэтому длина его не превышает $]|U_1| \ln |\mathscr{K}'|[\; (n-s) \leqslant n(n-s+1)m^{n-s+1} \ln n$. Лемма доказана.

Лемма 2.13. Существует входное слово α длины, не превышающей $(n+1)^2 m^{n+1} \ln(n+1)$, которое переводит каждый автомат $\mathfrak{A}_{q_0}$ из $\mathscr{K}_{m,n}$ в сильно связный подавтомат и проходит по всем ребрам диаграммы этого подавтомата.

Доказательство. Каждый автомат имеет сильно связный подавтомат. Применяем лемму 2.12 при $s=1$ и числе состояний автоматов, равном $n+1$. Построенное слово α с указанной в лемме 2.13 оценкой длины переводит все автоматы из $\mathcal{K}_{m,n+1}$ в сильно связные подавтоматы. Пусть $\mathfrak{A}_{q_0}$ — произвольный автомат из $\mathcal{K}_{m,n}$. Покажем, что α проходит по всем ребрам диаграммы $\mathfrak{A}_{q_0}$, достижимым из $\varphi(q_0, \alpha)$. Действительно, в противном случае добавляем к $\mathfrak{A}_{q_0}$ одно состояние такое, что все выходящие из него ребра в диаграмме ведут к нему же, и проводим к этому состоянию то ребро, которое не проходилось при подаче на вход автомата $\mathfrak{A}_{q_0}$ слова α. Очевидно, α не переводит полученный автомат $\mathfrak{B}_{q_0} \in \mathcal{K}_{m,n+1}$ в сильно связный подавтомат, что противоречит построению α. Лемма доказана.

Лемма 2.14. Если входное слово α есть простой безусловный установочный эксперимент для $\mathcal{K}_{m,n,2}$, то α — простой безусловный установочный эксперимент для $\mathcal{K}_{m,n}$.

Доказательство. Допустим противное, тогда существуют автоматы $\mathfrak{A}_{q_0}$ и $\mathfrak{B}_{q_0}$, принадлежащие $\mathcal{K}_{m,n,l}$ при некотором $l > 2$, такие, что α не различает $\mathfrak{A}_{q_0}$ и $\mathfrak{B}_{q_0}$, но $\mathfrak{A}_{\varphi_{\mathfrak{A}}(q_0,\alpha)}$ и $\mathfrak{B}_{\varphi_{\mathfrak{B}}(q_0,\alpha)}$ — различимы некоторым словом βa_i, где $a_i \in A$ и слово $\alpha\beta$ не различает $\mathfrak{A}_{q_0}$, $\mathfrak{B}_{q_0}$, причем $\psi_{\mathfrak{A}}(\varphi_{\mathfrak{A}}(q_0, \alpha\beta), a_i) = b_1$; $\psi_{\mathfrak{B}}(\varphi_{\mathfrak{B}}(q_0, \alpha\beta), a_i) = b_2 \neq b_1$. Отобразим $b_1, \ldots$ $\ldots, b_l = \{1, \ldots, l\}$ на $\{1, 2\}$ так, чтобы b_1 перешло в 1, а b_2 — в 2. Применяя это отображение к функциям выходов автоматов $\mathfrak{A}_{q_0}$ и $\mathfrak{B}_{q_0}$ получаем автоматы $\mathfrak{A}'_{q_0}$ и $\mathfrak{B}'_{q_0}$ и $\mathcal{K}_{m,n,2}$. Так как α не различает $\mathfrak{A}_{q_0}$ и $\mathfrak{B}_{q_0}$, то α не различает и $\mathfrak{A}'_{q_0}$, $\mathfrak{B}'_{q_0}$. В то же время $\mathfrak{A}_{\varphi_{\mathfrak{A}}(q_0,\alpha)}$ и $\mathfrak{B}_{\varphi_{\mathfrak{B}}(q_0,\alpha)}$, очевидно, различимы словом βa_i, т. е. α не есть установочный эксперимент для $\mathcal{K}_{m,n,2}$. Полученное противоречие и доказывает лемму.

§ 5. ОЦЕНКА СЛОЖНОСТИ ЭКСПЕРИМЕНТОВ ДЛЯ КЛАССОВ $\mathcal{K}_{m,n}$, $\mathcal{K}_{m,n,l}$

В этом параграфе будут установлены оценки наименьших длины, объема и кратности экспериментов различных типов, проводимых с автоматом, принадлежащим множеству $\mathcal{K}_{m,n}$ либо $\mathcal{K}_{m,n,l}$.

Теорема 2.13 [4]. Наименьшая длина кратного (как условного, так и безусловного) эксперимента, диагностического для $\mathcal{K}_{m,n}$, равна $2n-1$.

Доказательство теоремы непосредственно вытекает из теоремы 2.4 и приведенного после теоремы 2.4 примера, показывающего, что оценка $|Q|+|Q'|-1$ длины слова, отличающего $\mathfrak{A}_q$ от $\mathfrak{A}'_{q'}$, в этой теореме не может быть понижена. Отсутствие простых диагностических экспериментов для $\mathcal{K}_{m,n}$ при $n \geqslant 3$ вытекает из теоремы 2.10.

Теорема 2.14 [8]. Для величин $v_\delta(m, n)$ и $k_\delta(m, n)$ наименьших объема и кратности кратного безусловного эксперимента, диагностического для $\mathcal{K}_{m,n}$, имеют место следующие асимптотические (при $n \to \infty$) соотношения:

$$(2n-1)m^{2n-1} \geqslant v_\delta(m, n) \geqslant \begin{cases} \frac{3}{2} n2^{n-1} & \text{при } m = 2, \\ \frac{10}{9} n3^{n-1} & \text{при } m = 3, \\ nm^{n-1} & \text{при } m = 4, 5, 6, \\ \frac{n(m-1)^{2n-4}}{2^{2n-5}} & \text{при нечетном } m \geqslant 7, \\ n\frac{m^{n-2}(m-2)^{n-2}}{2^{2n-5}} & \text{при четном } m \geqslant 8; \end{cases}$$

$$m^{2n-1} \geqslant k_\delta(m, n) \geqslant \begin{cases} \frac{9}{8} 2^{n-1} & \text{при } m = 2, \\ m^{n-1} & \text{при } 3 \leqslant m \leqslant 6, \\ \frac{(m-1)^{2n-4}}{2^{2n-4}} & \text{при нечетном } m \geqslant 7, \\ \frac{m^{n-2}(m-2)^{n-2}}{2^{2n-4}} & \text{при четном } m \geqslant 8. \end{cases}$$

Доказательство. Пусть E — кратный безусловный эксперимент, состоящий из всех слов длины $2n-1$ в алфавите $A=\{1, \ldots, m\}$; если $\mathfrak{A}_q, \mathfrak{A}'_{q'} \in \mathcal{K}_{m,n}$ — различные инициальные автоматы, то, согласно доказательству теоремы 2.4, результаты применения E к $\mathfrak{A}_q$ и $\mathfrak{A}'_{q'}$ различны, и E — диагностический эксперимент для $\mathcal{K}_{m,n}$. Поэтому получаем: $v_\delta(m, n) \leqslant v(E, \mathcal{K}_{m,n}) = (2n-1)m^{2n-1}$; $k_\delta(m, n) \leqslant k(E, \mathcal{K}_{m,n}) = m^{2n-1}$.

Для получения нижних оценок разберем ряд подслучаев.

а) $3 \leqslant m \leqslant 6$. Рассмотрим автоматы $\mathfrak{A}_1$ и $\mathfrak{A}_2(\tilde{\alpha})$, где $\tilde{\alpha}=a(1)\ldots$ $\ldots a(n-1)$ — некоторое слово длины $n-1$ в алфавите $A=\{1, \ldots, m\}$; диаграммы этих автоматов приведены на рис. 2.12 (начальные состояния $\mathfrak{A}_1$ и $\mathfrak{A}_2(\tilde{\alpha})$ отмечены знаком $*$). Очевидно, любой кратный безусловный эксперимент E, отличающий $\mathfrak{A}_1$ от $\mathfrak{A}_2(\tilde{\alpha})$, должен содержать слово, началом которого является слово α, а так как $\mathfrak{A}_1$ и $\mathfrak{A}_2(\tilde{\alpha})$ при любом $\tilde{\alpha}$ указанного вида входят в $\mathcal{K}_{m,n}$, то диагностический для $\mathcal{K}_{m,n}$ кратный эксперимент E должен содержать слова, начинающиеся с любого слова $\tilde{\alpha}$ длины $n-1$. Так как число различных таких слов $\tilde{\alpha}$ есть m^{n-1}, а их суммарная длина — $(n-1)m^{n-1}$, то при $3 \leqslant m \leqslant 6$ получаем оценки: $v_\delta(m, n) \geqslant \geqslant (n-1)m^{n-1} \geqslant nm^{n-1}$; $k_\delta(m, n) \geqslant m^{n-1}$. Первую из этих оценок при $m=3$ можно усилить следующим образом.

Пусть $\mathfrak{A}_3$ — автомат, диаграмма которого приведена на рис. 2.13, и $\mathfrak{A}_4(1\tilde{\alpha}1)$, $\mathfrak{A}_4(1\tilde{\alpha}2)$ ($\tilde{\alpha}=a(1)\ldots a(n-2)$ — слово длины $n-2$ в алфавите A) — автоматы, диаграммы которых приведены на рис. 2.14. Пусть, далее, $\mathfrak{A}_4(2\tilde{\alpha}1)$, $\mathfrak{A}_4(2\tilde{\alpha}2)$, $\mathfrak{A}_4(3\tilde{\alpha}1)$, $\mathfrak{A}_4(3\tilde{\alpha}2)$ ($\tilde{\alpha}=a(1)\ldots a(n-3) \in A^*$) — автоматы, диаграммы которых приве-

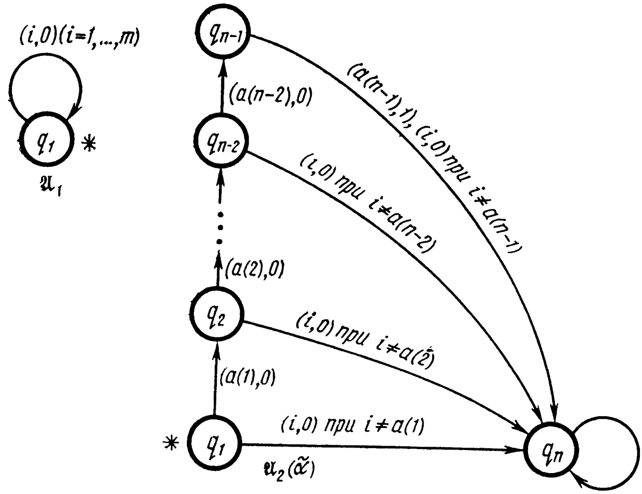

Рис 2 12.

дены на рис. 2.15. Для различения $\mathfrak{A}_3$ с автоматами $\mathfrak{A}_4(1\tilde{\alpha}1)$, $\mathfrak{A}_4(1\tilde{\alpha}2)$, $\mathfrak{A}_4(2\tilde{\alpha}1)$, $\mathfrak{A}_4(2\tilde{\alpha}2)$, $\mathfrak{A}_4(3\tilde{\alpha}1)$, $\mathfrak{A}_4(3\tilde{\alpha}2)$ необходимо пользоваться словами, имеющими соответственно начала вида: $1\tilde{\alpha}(1\tilde{\alpha})^i12$; $1\tilde{\alpha}(\tilde{\alpha})^i2$; $2\tilde{\alpha}(2\tilde{\alpha})^i12$; $2\tilde{\alpha}2$; $3\tilde{\alpha}(3\tilde{\alpha})^i12$; $3\tilde{\alpha}2$ (здесь $i \geqslant 0$). Нетрудно видеть, что при различных α множества таких слов не пересекаются. Если слова $1\tilde{\alpha}(1\tilde{\alpha})^i12$ и $1\tilde{\alpha}(\tilde{\alpha})^j2$ суть начала одного и того же слова p, то случай $i=j=0$ невозможен, и в слове p можно выделить не менее двух непересекающихся вхождений слова $\tilde{\alpha}$. Аналогично, если $2\tilde{\alpha}(2\tilde{\alpha})^i12$ и $2\tilde{\alpha}2$ — начала одного и того же слова p, то в p можно выделить непересекающиеся вхождения слов $\tilde{\alpha}2$ и $\tilde{\alpha}12$; слова $3\tilde{\alpha}(3\tilde{\alpha})^i12$ и $3\tilde{\alpha}2$ не являются началами одного и того же слова ни при каком $i \geqslant 0$.

Таким образом, в каждом кратном диагностическом для $\mathcal{K}_{r,n}$ эксперименте можно выделить $2\cdot 3^{n-2}$ непересекающихся вхождений слова $\tilde{\alpha}$, имеющего длину $n-2$; $2\cdot 3^{n-3}$ непересекающихся друг с другом и с предыдущими вхождениями вхождений слов $\tilde{\alpha}2$, $\tilde{\alpha}12$, где $\tilde{\alpha}$ — слово длины $n-3$, и $2\cdot 3^{n-3}$ непересекающихся друг с другом и с предыдущими вхождениями вхождений слов $3\tilde{\alpha}2$, $3\tilde{\alpha}12$, где $\tilde{\alpha}$ — слово длины $n-3$, откуда и получаем:

$$v_\delta(3, n) \geqslant (n-2)(2\cdot 3^{n-2} + 2\cdot 3^{n-3} + 2\cdot 3^{n-3}) \sim \frac{10}{9}\, n\cdot 3^{n-1}.$$

б) $m=2$. В этом случае рассматриваем автоматы $\mathfrak{A}_5$, $\mathfrak{A}_6(1\tilde{\alpha}1)$, $\mathfrak{A}_6(1\tilde{\alpha}2)$, $\mathfrak{A}_6(2\tilde{\alpha}1)$, $\mathfrak{A}_6(2\tilde{\alpha}2)$, получающиеся из автоматов $\mathfrak{A}_3$, $\mathfrak{A}_4(1\tilde{\alpha}1)$, $\mathfrak{A}_4(1\tilde{\alpha}2)$, $\mathfrak{A}_4(2\tilde{\alpha}1)$, $\mathfrak{A}_4(2\tilde{\alpha}2)$ соответственно удалением входного символа 3. Для отличения $\mathfrak{A}_5$ от автоматов $\mathfrak{A}_6(1\tilde{\alpha}1)$,

$\mathfrak{A}_6(1\tilde{\alpha}2)$, $\mathfrak{A}_6(2\tilde{\alpha}1)$, $\mathfrak{A}_6(2\tilde{\alpha}2)$ необходимо пользоваться словами, имеющими соответственно начала следующих видов: $1\tilde{\alpha}(1\tilde{\alpha})^i12$; $1\tilde{\alpha}(\tilde{\alpha})^i2$; $2\tilde{\alpha}(2\tilde{\alpha})^i12$; $2\tilde{\alpha}2$ (здесь $i \geqslant 0$). При различных α множества таких слов не пересекаются. Если $1\tilde{\alpha}(1\tilde{\alpha})^i12$ и $1\tilde{\alpha}(\tilde{\alpha})^j2$ — начала одного и того же слова, то либо $\tilde{\alpha}=1\ldots1$, либо $\tilde{\alpha}=12a(3)\ldots a(n-2)$. Поэтому $k_\delta(2, n) \geqslant 2(3\cdot 2^{n-4}-1)+2^{n-4}+1+2^{n-3}\sim(9/8)\cdot 2^{n-1}$. Рассуждая далее так же, как и в случае $m=3$, найдем $v_\delta(2, n) \gtrsim (3/2)n\cdot 2^{n-1}$.

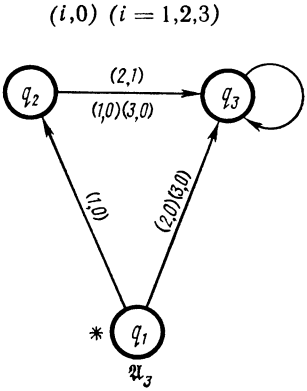

Рис. 2.13.

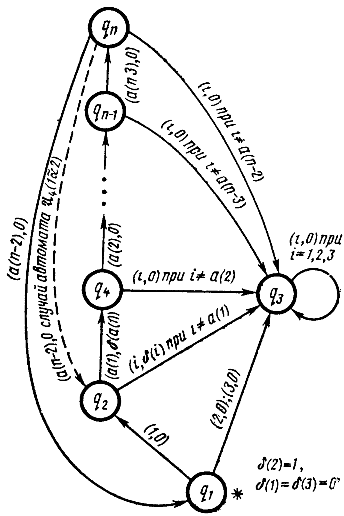

Рис. 2.14.

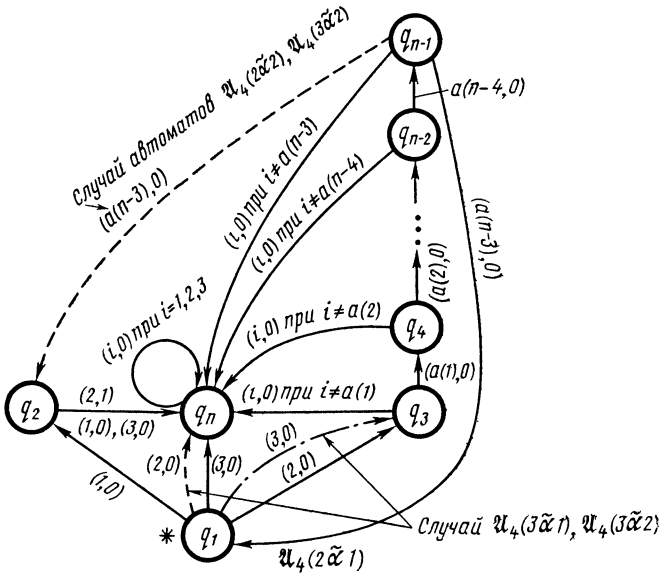

Рис. 2.15.

в) $m>6$. Пусть $m=r+s+1$, где $r\geqslant 1$, $s\geqslant 1$. Произвольной паре слов $\tilde{\alpha}=a(1)\ldots a(n-2)$ и $\tilde{\beta}=b(1)\ldots b(n-2)$, где $a(i)\in\{1, \ldots, r\}$; $b(i)\in\{r+1, \ldots, r+s\}$, сопоставим автоматы $\mathfrak{A}_7(\tilde{\alpha}, \tilde{\beta})$ и $\mathfrak{A}_8(\tilde{\alpha}, \tilde{\beta})$, диаграммы которых приведены на рис. 2.16. Эти автоматы сильно связаны и не эквивалентны.

Чтобы отличить их друг от друга, необходимо сначала перевести каждый из них в состояние q_{n-1}, после чего подать входной символ $b(n-2)$. Тогда $\mathfrak{A}_7(\tilde{\alpha}, \tilde{\beta})$ перейдет в состояние q_{n-2}, а $\mathfrak{A}_8(\tilde{\alpha}, \tilde{\beta})$ — в q_0. Теперь для отличения их друг от друга необходимо перевести $\mathfrak{A}_7(\tilde{\alpha}, \tilde{\beta})$ в q_1, не используя при этом символ m и не проходя через q_0. После этого $\mathfrak{A}_7(\tilde{\alpha}, \tilde{\beta})$ и $\mathfrak{A}_8(\tilde{\alpha}, \tilde{\beta})$ отличаются символом m. Пусть E — произвольный кратный безусловный эксперимент, диагностический для $\mathcal{K}_{m,n}$, и u — произвольное слово из E, причем mvm — отрезок слова u и $v=v(1)\ldots v(l)$ не содержит символа m. Покажем, что следующая за v буква m отличает не более одной пары $\mathfrak{A}_7(\tilde{\alpha}, \tilde{\beta})$; $\mathfrak{A}_8(\tilde{\alpha}, \tilde{\beta})$. Если $l<2(n-2)$, то эта буква не различает ни одну такую пару, так как первый символ m переводит оба автомата в состояние q_1 и v «не успевает» довести их до состояний, отличимых символом m. Пусть $l\geqslant 2(n-2)$. Введем функцию $f_v(i)$, равную разности между количествами букв из алфавитов $\{1, \ldots, r\}$ и $\{r+1, \ldots, r+s\}$ в слове $v(1)\ldots v(i)$; $f_v(0)=0$. Очевидно, если при некотором i $(1\leqslant i\leqslant l)$ $f_v(i)<0$ или $f_v(i)>n-2$, а также если не существует i, при котором $f_v(i)=n-2$ и если $f_v(l)\neq 0$, то vm не различает ни одну из рассматриваемых пар. То же справедливо, если при некоторых i и j $f_v(i)=f_v(j)$ и буквы $v(i+1)$ и $v(j+1)$ различны, но входят одновременно в $\{1, \ldots, r\}$ либо в $\{r+1, \ldots, r+s\}$. Если же перечисленные условия не нарушены, то слово vm различает одну из пар $\mathfrak{A}_7(\tilde{\alpha}, \tilde{\beta})$; $\mathfrak{A}_8(\tilde{\alpha}, \tilde{\beta})$, причем по виду v можно определить $\tilde{\alpha}$ и $\tilde{\beta}$.

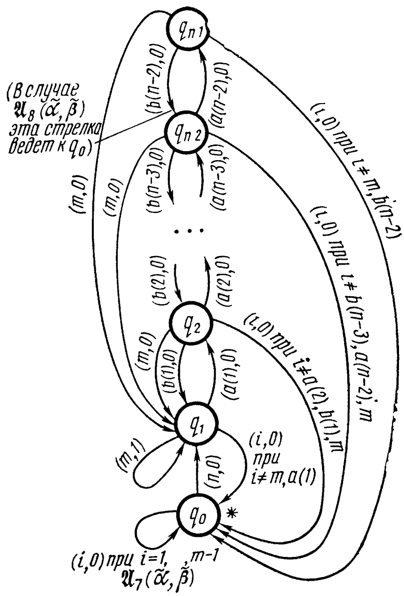

Рис 2 16

Поэтому каждой из описанных пар автоматов соответствует отрезок vm в некотором слове из E, длина которого не менее $2n-3$, откуда $v_6(m, n)\geqslant(2n-3)r^{n-2}s^{n-2}$. Если m нечетно, то при $r=s=(m-1)/2$ имеем:

$$v_6(m, n)\geqslant(2n-3)\frac{(m-1)^{2n-4}}{2^{2n-4}}\geqslant\frac{n(m-1)^{2n-4}}{2^{2n-5}}$$

при $n \to \infty$. Для четных m полагаем $r=m/2$, $s=(m/2)-1$ и

$$v_\delta(m, n) \geqslant (2n-3)\frac{m^{n-2}(m-2)^{n-2}}{2^{2n-4}} \gtrsim \frac{nm^{n-2}(m-2)^{n-2}}{2^{2n-5}}$$

при $n \to \infty$. Для получения нижней оценки кратности изменяем автоматы $\mathfrak{A}_7(\tilde{\alpha}, \tilde{\beta})$ и $\mathfrak{A}_8(\tilde{\alpha}, \tilde{\beta})$, проводя в их диаграммах стрелки от всех состояний q_i, соответствующие входному символу m, к состоянию q_0 и выбирая в качестве начального состояние q_1. Слова, различающие полученные автоматы $\mathfrak{A}'_7(\tilde{\alpha}, \tilde{\beta})$ и $\mathfrak{A}'_8(\tilde{\alpha}, \tilde{\beta})$, различны при разных $\tilde{\alpha}$ и $\tilde{\beta}$, и поэтому $k_\delta(m, n) \geqslant \frac{(m-1)^{2n-4}}{2^{2n-4}}$ при нечетном m и $k_\delta(m, n) \geqslant \frac{m^{n-2}(m-2)^{n-2}}{2^{2n-4}}$ при четном m. Теорема доказана.

Теорема 2.15 [8]. Для величин $k_y(m, n)$ и $v_y(m, n)$ наименьших кратности и объема условного эксперимента, диагностического для $\mathcal{K}_{m,n}$, имеют место оценки (асимптотика берется при $n \to \infty$):

$$\frac{m^{n+1}}{m-1} \geqslant k_y(m, n) \gtrsim \begin{cases} m^{n-1} & \text{при } m \geqslant 3, \\ \frac{9}{8} 2^{n-1} & \text{при } m = 2; \end{cases}$$

$$n\frac{m^{n+1}}{m-1} \gtrsim v_y(m, n) \gtrsim \begin{cases} nm^{n-1} & \text{при } m \geqslant 4, \\ \frac{10}{9} n3^{n-1} & \text{при } m = 3, \\ \frac{3}{2} n2^{n-1} & \text{при } m = 2. \end{cases}$$

Доказательство. Получение нижних оценок происходит точно так же, как в случае функций $v_\delta(m, n)$; $k_\delta(m, n)$ (кроме случая $m>6$, рассматривавшегося особо при получении оценок $v_\delta(m, n)$, $k_\delta(m, n)$). Займемся получением верхних оценок. Для этого опишем кратный условный эксперимент E, диагностический для $\mathcal{K}_{m,n}$. Пусть $\mathfrak{A}_q \in \mathcal{K}_{m,n}$. Введем обозначение $v_i^{\mathfrak{A}_q} = v_i$; $V(\mathfrak{A}_q, i) = V_i$; $w_i^{\mathfrak{A}} = w_i$; $W(\mathfrak{A}, i) = W_i$ при $i=1, 2, \ldots$. Эксперимент проводится по шагам и начинается с шага 0. Перед этим шагом нам известны $V_0 = W_0 = \{\Lambda\}$. Подавая на вход автомата $\mathfrak{A}_q$ множество слов $V_0A^{n-0}W_0 = A^n$, различаем, согласно лемме 2.9, $\mathfrak{A}_q$ и любой автомат $\mathfrak{B}_q \in \mathcal{K}_{m,n}$, для которого $V(\mathfrak{B}_q, 1) \neq V_1$ или $W(\mathfrak{B}, 1) \neq W_1$. Следовательно, для всех автоматов $\mathfrak{B}_q$, не различимых с $\mathfrak{A}_q$ множеством $V_0A^nW_0$, $V(\mathfrak{B}_q, 1) = V_1$ и $W(\mathfrak{B}, 1) = W_1$, поэтому после шага 0 можно найти V_1 и W_1. Если $W_1 = W_0$, то эксперимент E заканчивается, в противном случае переходим к шагу 1.

Шаг i ($i=1, 2, \ldots$). Перед этим шагом нам известны V_i и W_i, а также результаты подачи на вход $\mathfrak{A}_q$ множества $V_{i-1}A^{n-i+1}W_{i-1}$. Установим результат подачи на вход $\mathfrak{A}_q$ множества

$$V_iA^{n-i}W_i = (V_{i-1} \cup \{v_i\}) A^{n-i} (W_{i-1} \cup \{w_i\}) =$$

$$= V_{i-1}A^{n-i}w_i \cup v_iA^{n-i}W_{i-1} \cup V_{i-1}A^{n-i}W_{i-1} \cup v_iA^{n-i}w_i.$$

Так как

$$V_{i-1}A^{n-1}w_i \subseteq V_{i-1}A^{n-i}AW_{i-1} = V_{i-1}A^{n-i+1}W_{i-1};$$
$$v_iA^{n-i}W_{i-1} \subseteq V_{i-1}AA^{n-i}W_{i-1} = V_{i-1}A^{n-i+1}W_{i-1};$$
$$V_{i-1}A^{n-i}W_{i-1} \leqslant V_{i-1}A^{n-i+1}W_{i-1},$$

то достаточно подавать на вход $\mathfrak{A}_q$ множество $v_iA^{n-1}w_i$. В результате подачи на вход $\mathfrak{A}_q$ указанного множества, согласно лемме 2.9, устанавливается различимость $\mathfrak{A}_q$ и любого автомата $\mathfrak{B}_q \in \mathcal{K}_{m,n}$, для которого $V(\mathfrak{B}_q, i+1) \neq V_{i+1}$, либо $W(\mathfrak{B}, i+1) \neq$ $\neq W_{i+1}$, поэтому устанавливаются W_{i+1} и V_{i+1}. Если $W_{i+1} = W_i$, эксперимент E заканчивается, в противном случае переходим к шагу $i+1$.

Очевидно, эксперимент E заканчивается не позднее чем на шаге $|\mathfrak{A}|-1 \leqslant n-1$. Пусть эксперимент E закончился на шаге i $(0 \leqslant i \leqslant |\mathfrak{A}|-1)$. Тогда $W_i = W(\mathfrak{A})$, и нам известны результаты подачи на вход $\mathfrak{A}_q$ множества $V_iA^{n-i}W_i = V_iA^{n-i}W(\mathfrak{A}) \geqslant$ $\geqslant V_{|\mathfrak{A}|-1}A^{n-|\mathfrak{A}|+1}W(\mathfrak{A}) = V(\mathfrak{A}_q)A^{n-|\mathfrak{A}|+1}W(\mathfrak{A})$. Поэтому, согласно лемме 2.10, множество слов использованное для подачи на вход $\mathfrak{A}_q$, отличает $\mathfrak{A}_q$ от всех остальных автоматов из $\mathcal{K}_{m,n}$, т. е. E — диагностический эксперимент для $\mathcal{K}_{m,n}$. На шаге i на вход $\mathfrak{A}_q$ подается множество $v_iA^{n-i}w_i$, содержащее m^{n-i} слов, длина каждого из которых не больше $n+i$. Поэтому кратность эксперимента E не превышает $\sum\limits_{i=0}^{n-1} m^{n-i} \leqslant \frac{m^{n+1}}{m-1}$, а объем его не больше

$$\sum_{i=0}^{n-1} m^{n-1}(n+i) = n\sum_{i=0}^{n-1} m^{n-i} + \sum_{i=0}^{n-1} im^{n-i} \leqslant$$

$$\leqslant \frac{m}{m-1}nm^n + \max_{i=0,1,\ldots} im^{n-i} + \int_0^{n-1} im^{n-i}\,di = \frac{m}{m-1}nm^n +$$

$$+ m^{n-1} - \frac{im^{n-i}}{\ln m}\Bigg|_{i=0}^{i=n+1} - \frac{m^{n-i}}{(\ln m)^2}\Bigg|_{i=0}^{i=n-1} <$$

$$< \frac{m}{m-1}nm^n + m^{n-1} + \frac{m^n}{(\ln m)^2} \leqslant \frac{m}{m-1}nm^n +$$

$$+ m^n\left(\frac{1}{2} + \frac{1}{(\ln 2)^2}\right) < \left(\frac{m}{m+1}n + 3\right)m^n \lesssim n\frac{m^{n+1}}{m-1}$$

при $n \to \infty$. Теорема доказана.

Теорема 2.16 [4, 8, 9]. Наименьшая длина $l_y(m, n)$ простого условного эксперимента, установочного для $\mathcal{K}_{m,n}$, не менее m^n, причем $n \to \infty$:

$$l_y(m, n) \lesssim (5/3)m^{n+1}n^4\ln(mn^2).$$

Доказательство. Для получения нижней оценки величины $l_y(m, n)$ рассмотрим для каждого слова $\tilde{\alpha}=a(1)\ldots a(n)$ $(a(i)\in \in\{1, \ldots, m\})$ автомат $\mathfrak{A}_{q_0}(\tilde{\alpha})$, диаграмма которого указана на рис. 2.17.

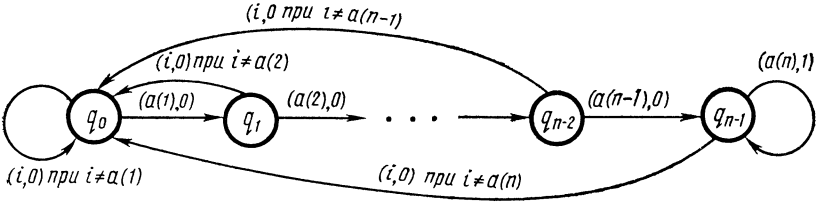

Рис 2.17.

Пусть Φ — простой условный эксперимент, установочный для $\mathcal{K}_{m,n}$. Если длина Φ менее чем m^n, то существуют автоматы $\mathfrak{A}_{q_0}(\tilde{\alpha})$ и $\mathfrak{A}_{q_0}(\tilde{\beta})$, $(\tilde{\alpha}\neq\tilde{\beta})$, такие, что $(\tilde{\gamma}_1, \tilde{\delta}_1)$ и $(\tilde{\gamma}_2, \tilde{\delta}_2)$ — результаты применения к ним эксперимента Φ, причем $\tilde{\delta}_1=\underbrace{0\ldots0}_{i}1\tilde{\delta}_1'$; $\tilde{\delta}_2=$ $=\underbrace{0\ldots0}_{i}1\tilde{\delta}_2'$ (так как, очевидно, для результата $(\tilde{\gamma}, \tilde{\delta})$ применим Φ к автомату вида $\mathfrak{A}_{q_0}(\tilde{\alpha})$, $\tilde{\delta}\neq\tilde{0}$). Но тогда $\tilde{\gamma}_1=\gamma(1)\ldots\gamma(i+1)\tilde{\gamma}_1'$; $\tilde{\gamma}_2=\gamma(1)\ldots\gamma(i+1)\tilde{\gamma}_2'$, т. е. конец слова $\gamma(1)\ldots\gamma(i+1)$ отличен либо от $\tilde{\alpha}$, либо от $\tilde{\beta}$ и одновременное появление 1 на выходе автоматов $\mathfrak{A}_{q_0}(\tilde{\alpha})$ и $\mathfrak{A}_{q_0}(\tilde{\beta})$ при подаче на них слова $\gamma(1)\ldots\gamma(i+1)$ невозможно.

Докажем теперь верхнюю оценку для $l_y(m, n)$. Опишем простой условный эксперимент E, установочный для $\mathcal{K}_{m,n}$. Согласно лемме 2.13 из § 4, существует входное слово α, переводящее любой автомат из $\mathcal{K}_{m,n}$ в сильно связный подавтомат и проходящее по всем ребрам диаграммы этого подавтомата. Эксперимент E проводится по шагам и начинается с предварительного шага.

Предварительный шаг. На автомат $\mathfrak{A}_q\in\mathcal{K}_{m,n}$ подается указанное выше слово α. Составляется список S появившихся при этом выходных букв, и далее выполняется шаг 0, который будет описан ниже. Автомат $\mathfrak{A}_{\varphi(q,\alpha)}$ эквивалентен некоторому сильно связному приведенному автомату $\mathfrak{B}_{q_1}\in\mathcal{K}_{m,n}$. Обозначим $w_i^{\mathfrak{B}}=$ $=w_i$; $W(\mathfrak{M}, i)=W_i$. Полагая известным некоторый класс сильно связных автоматов $\mathfrak{M}_{q'}\in\mathcal{K}_{m,n}$, содержащий $\mathfrak{B}_{q_1}$, для которых $W(\mathfrak{B}, i)=W_i$, будем искать входное слово u_i, различающее $\mathfrak{B}_{q_1}$ и все сильно связные автоматы $\mathfrak{N}_{q_0'}\in\mathcal{K}_{m,n}$, для которых $W(\mathfrak{N}, i+1)\neq W_{i+1}$; если w_{i+1} не существует, потребуем, чтобы u_i при любом q_j отличало $\mathfrak{B}_{q_j}$ от любого автомата $\mathfrak{N}_{q'}\in\mathcal{K}_{m,n}$, такого, что автомат $\mathfrak{B}_{\varphi(q_j,u_i)}$ не эквивалентен автомату $\mathfrak{N}_{\varphi(q',u_i)}$.

Из лемм 2.9 и 2.10 предыдущего параграфа и из соотношений

$$\bigcup_{j=1}^{|\mathfrak{B}|} V(\mathfrak{B}_{q_j}, i)\, A^{n-i}W_i \leqslant A^i A^{n-i}W_i = A^n W_i;$$

$$\bigcup_{j=1}^{|\mathfrak{B}|} V(\mathfrak{B}_{q_j})\, A^{n-|\mathfrak{B}|+1}\, W(\mathfrak{B}) \leqslant A^{|\mathfrak{B}|-1}\, A^{n-|\mathfrak{B}|+1}\, W(\mathfrak{B}) = A^n W(\mathfrak{B})$$

следует, что для любого состояния q_j автомата $\mathfrak{B}$ и любого сильно связного автомата $\mathfrak{N}_{q'} \in \mathcal{K}_{m,n}$, такого, что $W(\mathfrak{N}, \ i+1) \neq W_{i+1}$, в $A^n W_i$ существует слово u, различающее $\mathfrak{B}_{q_j}$ и $\mathfrak{N}_{q'}$. Если же w_{i+1} не существует, то $W(\mathfrak{B}) = W_i$, поэтому указанное слово u найдется в $A^n W_i$ любого автомата $\mathfrak{N}_{q'}$ из $\mathcal{K}_{m,n}$, отличного от $\mathfrak{B}_{q_j}$. Для тех i, для которых существует w_i, построим множество $\mathbf{C}_i = \{\langle \mathfrak{M}_{q'}, \mathfrak{N}_{q''}\rangle\}$, где $\mathfrak{M}_{q'}$ пробегает все сильно связные автоматы из $\mathcal{K}_{m,n}$, для которых $W(\mathfrak{M}, \ i) = W_i$. Если $w_{i+1}^{\mathfrak{M}}$ существует, $\mathfrak{N}_{q''}$ пробегает все сильно связные автоматы из $\mathcal{K}_{m,n}$, для которых $W(\mathfrak{N}, \ i+1) \neq W(\mathfrak{M}, \ i+1)$, в противном случае $\mathfrak{N}_q$ пробегает все сильно связные автоматы из $\mathcal{K}_{m,n}$, отличные от $\mathfrak{M}_{q'}$. Как в $\mathfrak{M}$, так и в $\mathfrak{N}$ разрешается использовать лишь те выходные символы, которые входят в указанный выше список S. Очевидно, $|\mathbf{C}_i| \leqslant (\tilde{p}n)^{2mn}$, где $\tilde{p} = |S|$. Полагаем $\mathcal{P}(\langle \mathfrak{M}_2 \quad \mathfrak{N}_2\rangle, x)$, если входное слово x различает $\mathfrak{M}_q$ и $\mathfrak{N}_q$, либо $\mathfrak{M}_{\varphi(q,x)}$ эквивалентен $\mathfrak{N}_{\varphi(q,x)}$. Подставляем $\mathbf{C}_i$, $A^n W_i$ и $\mathcal{P}$ вместо K, u_i и $\mathcal{P}$ из леммы 2.11 из § 4 (при $p=1$). Условия 1) и 2), очевидно, выполнены, поэтому из этой леммы вытекает существование входного слова (обозначим его через u_i), такого, что для любой пары $\langle \mathfrak{M}_q, \mathfrak{N}_q\rangle \in \mathbf{C}_i$ либо u_i различает $\mathfrak{M}_q$ и $\mathfrak{N}_q$, либо $\mathfrak{M}_{\varphi(q,u_i)}$ эквивалентно $\mathfrak{N}_{\varphi(q,u_i)}$. Закончим описание эксперимента E.

Шаг i (i=0, 1, 2, ...). Перед этим шагом нам известны W_i и некоторый класс сильно связных автоматов $\mathfrak{M}_q \in \mathcal{K}_{m,n}$, содержащий автомат, неотличимый от $\mathfrak{B}_{q'} = \mathfrak{B}_{\varphi(q_1, u_0, \ldots, u_{i-1})}$, для которых $W(\mathfrak{M}, \ i) = W_i$; известно также u_i. На i-м шаге на автомат $\mathfrak{B}_q'$ подается слово u_i; в результате этот автомат отличается от любого сильно связного автомата $\mathfrak{N}_{q''} \in \mathcal{K}_{m,n}$, для которого $W(\mathfrak{N}, \ i+1) \neq W_{i+1}$, поэтому по результату подачи слова u_i можно установить w_{i+1}, а отсюда и u_{i+1}. Если $W_{i+1} = W_i$, эксперимент E заканчивается, в противном случае переходим к шагу $i+1$. Очевидно, эксперимент E заканчивается не позднее чем на шаге $|\mathfrak{B}|-1 \leqslant n-1$. Пусть эксперимент закончился на шаге i $(0 \leqslant i \leqslant |\mathfrak{B}|-1)$. Так как в таком случае w_{i+1} не существует, для любого $\mathfrak{L}_{q''} \in \mathcal{K}_{m,n}$ либо u_i различает $\mathfrak{A}_{\varphi(q, \alpha u_0 \ldots u_{i-1})}$ и $\mathfrak{L}_{q''}$, либо $\mathfrak{A}_{\varphi(q, \alpha u_0 \ldots u_i)}$ эквивалентен $\mathfrak{L}_{\varphi(q'', u_i)}$, т. е. E — установочный для $\mathcal{K}_{m,n}$ эксперимент. Оценим его длину, учитывая, что длина α не больше чем $(n+1)^2 m^{n+1} \ln n$, а длина u_i не больше $(n+i)\,]\, m^n (i+1) \ln (\tilde{p}n)^{2mn}\,[$. Имеем:

$$l_y(m, n) \leqslant l(E, \mathcal{K}_{m,n}) \leqslant (n+1)^2 m^{n+1} \ln n +$$

$$+\sum_{i=0}^{n-1}(n+i)\,m^n(i+1)\,2mn\ln\widetilde{pn}\sim 2m^{n+1}n\ln\widetilde{pn}\sum_{i=0}^{n-1}{}'(n+i)(i+1)\sim$$

$$\sim 2m^{n+1}n\ln\widetilde{pn}\left(\frac{n^3}{2}+\frac{n^3}{3}\right)=\frac{5}{3}m^{n+1}n^4\ln\widetilde{pn}\leqslant\frac{5}{3}m^{n+1}n^4\ln(mn^2).$$

Теорема доказана.

Теорема 2.17 [8]. Наименьшая длина $l_\delta(m, n)$ простого безусловного эксперимента, установочного для $\mathscr{K}_{m,n}$, не превосходит $]4m^{2n}n^2\ln 2n[$, причем при $n\to\infty$:

$$l_\delta(m, n) \gtrsim \begin{cases} m^n \text{ при } m\leqslant 5, \\ n\,\dfrac{m^{n-2}(m-2)^{n-2}}{2^{2n-5}} \text{ при четном } m\geqslant 6, \\ n\,\dfrac{(m-1)^{2n-4}}{2^{2n-5}} \text{ при нечетном } m\geqslant 6. \end{cases}$$

Доказательство. Для получения верхней оценки величины $l_\delta(m, n)$ применим лемму 2.11. Пусть в этой лемме K — множество всех пар $\langle\mathfrak{A}_q, \mathfrak{B}_q\rangle$ (неупорядоченных) элементов $\mathscr{K}_{m,n,l}$; $p=1$; U_1 — множество всех входных слов длины $2n-1$ и $\mathscr{P}(\langle\mathfrak{A}_q, \mathfrak{B}_q\rangle, u_1\ldots u_s)$ означает, что входное слово $u_1\ldots u_s=u$ либо различает $\mathfrak{A}_q$ и $\mathfrak{B}_q$, либо переводит их в неразличимые состояния. Тогда справедливость первого условия леммы 2.11 вытекает из различимости любых двух различных автоматов $\mathfrak{A}_q$ и $\mathfrak{B}_q$ из $\mathscr{K}_{m,n,l}$ словом длины $2n-1$; справедливость второго условия очевидна, и, согласно лемме, существует слово u_0 в алфавите U_1^* длины, не большей $]\,|U_1|\ln|K|\,[$, такое, что $\mathscr{P}(\langle\mathfrak{A}_q, \mathfrak{B}_q\rangle, u_0)$ для любых различных $\mathfrak{A}_q$, $\mathfrak{B}_q\in\mathscr{K}_{m,n,l}$. Очевидно, это и означает, что u_0 (рассматриваемое уже как слово в алфавите A) является простым. безусловным экспериментом, установочным для $\mathscr{K}_{m,n,l}$. Длина u_0 (как слова в алфавите A) не превосходит $(2n-1)\,]m^{2n-1}\times\times\ln C^2_{nl}mn\,[\leqslant]\,4m^{2n}n^2\ln(ln)[$. Но по лемме 2,14 слово u_0, являющееся простым безусловным установочным экспериментом для $\mathscr{K}_{m,n,2}$, является в то же время простым безусловным установочным экспериментом и для $\mathscr{K}_{m,n}$; поэтому подставляем $l=2$ и получаем искомую верхнюю оценку. При $m\leqslant 5$ нижняя оценка $l_\delta(m, n)$ есть следствие соотношения $l_\delta(m, n)\geqslant l_y(m, n)$ и доказанного ранее неравенства $l_y(m, n)\geqslant m^n$. При $m>5$ нижние оценки для $l_\delta(m, n)$ устанавливаются с использованием тех же вспомогательных автоматов, что и оценки для $v_\delta(m, n)$. Теорема доказана. Пусть $l_\text{т}(m, n, t)$ (соответственно $k_\text{т}(m, n, t)$, $v_\text{т}(m, n, t)$) — наименьшее число, такое, что для любого автомата $\mathfrak{A}_q\in\mathscr{K}_{m,n}$ с t состояниями существует кратный эксперимент, тестовый для $\mathfrak{A}_q$ относительно $\mathscr{K}_{m,n}$, длина (соответственно кратность, объем) которого не превосходит $l_\text{т}(m, n, t)$ (соответственно $k_\text{т}(m, n, t)$, $v_\text{т}(m, n, t)$). Имеет место следующая теорема:

Теорема 2.18 [7]. $l_т(m, n, t) = n+t-1$; если $t\to\infty$, $n\to\infty$, $t\leqslant n$ то

$$k_т(m, n, t) \sim t^2(m-1)m^{n-t};$$

$$v_т(m, n, t) \sim t^2 n(m-1)m^{n-t}.$$

Доказательство. Для получения верхних оценок опишем кратный эксперимент E, тестовый относительно $\mathcal{K}_{m,n}$ для автомата $\mathfrak{A}_q \in \mathcal{K}_{m,n}$, имеющего t состояния. На вход автомата $\mathfrak{A}_q$ подадим множество $[V(\mathfrak{A}_q)A]A^{n-t}(W(\mathfrak{A})\setminus\{\Lambda\})$, если $t>1$, и множество $[V(\mathfrak{A}_q)A]A^{n-t}W(\mathfrak{A})$, если $t=1$. Так как $V(\mathfrak{A}_q)\ A^{n-t+1}W(\mathfrak{A}) \leqslant [V(\mathfrak{A}_q)A]A^{n-t}W(\mathfrak{A})$ (лемма 2.8 из § 4) и при $t>1$ $W(\mathfrak{A})\neq\{\Lambda\}$; $\Lambda\leqslant W(\mathfrak{A})\setminus\{\Lambda\}$, то использованное множество, согласно лемме 2.10, различает $\mathfrak{A}_q$ и все не эквивалентные ему автоматы из $\mathcal{K}_{m,n}$, т. е. эксперимент E — тестовый для $\mathfrak{A}_q$ относительно $\mathcal{K}_{m,n}$. Длина слов из $[V(\mathfrak{A}_q)A]$ не больше t; длина слов из A^{n-t} равна $n-t$; длина слов из $W(\mathfrak{A})$ не больше $t-1$, поэтому $l_т(m, n, t)\leqslant n+t-1$. Легко видеть, что объем использованного множества принимает максимальное значение, если существуют такие слова v и w длины $t-1$, что:

$$V(\mathfrak{A}_q) = \{\Lambda,\ v(1),\ v(1)v(2),\ldots, v(1)\ldots v(t-1)\},$$

$$W(\mathfrak{A}) = \{\Lambda,\ w(t-1),\ w(t-2)w(t-1),\ldots, w(1)\ldots w(t-1)\}.$$

Тогда

$$[V(\mathfrak{A}_q)A]A^{n-t}W(\mathfrak{A}) = (vA \cup \bigcup_{i=1}^{t-1} v(1)\ldots v(i-1)\{1,\ldots$$

$$\ldots, v(i)-1,\ v(i)+1,\ldots, m\})A^{n-t}\bigcup_{j=1}^{t-1} w(t-j)\ldots$$

$$\ldots w(t-1) = \bigcup_{j=1}^{t-1} vAA^{n-t}w(t-j)\ldots w(t-1) \cup \bigcup_{i=1}^{t-1}\bigcup_{j=1}^{t-1} v(1)\ldots$$

$$\ldots v(i-1)\{1,\ldots, v(i)-1,\ v(i)+1,\ldots, m\}A^{n-t}w(t-j)\ldots w(t-1).$$

Объем первого из этих множеств равен

$$\sum_{j=1}^{t-1}(t-1+1+n-t+j)m^{n-t+1} = m^{n-t+1}\sum_{j=1}^{t-1}(n+j) =$$

$$= m^{n-t+1}(t-1)\left(n+\frac{t}{2}\right) = o(t^2 n(m-1)m^{n-t}).$$

Объем второго множества равен

$$\sum_{i=1}^{t-1}\sum_{j=1}^{t-1}(i+n-t+j)(m-1)m^{n-t} =$$

$$= (m-1)m^{n-t}(t-1)\sum_{i=1}^{t-1}\left(i+n-t+\frac{t}{2}\right) \sim t^2 n(m-1)m^{n-t}.$$

Аналогично, число слов в рассматриваемом множестве асимптотически не более чем $t^2(m-1)m^{n-t}$, что и завершает получение верхних оценок. Для получения нижних оценок построим ряд вспомогательных автоматов. Пусть $\alpha=\alpha(1)\ldots\alpha(t-1)$ — входное слово, содержащее любой отрезок длины $]\log_m t[$ не более одного раза. В качестве α можно, например, брать начальный отрезок слова, содержащего точно один раз каждый отрезок длины $]\log_m t[$; известно [10], что такое слово существует и длина его равна $m^{]\log_m t[}+]\log_m t[-1\geqslant t$. Пусть $\mathfrak{A}^1$ — автомат, диаграмма которого приведена на рис. 2.18.

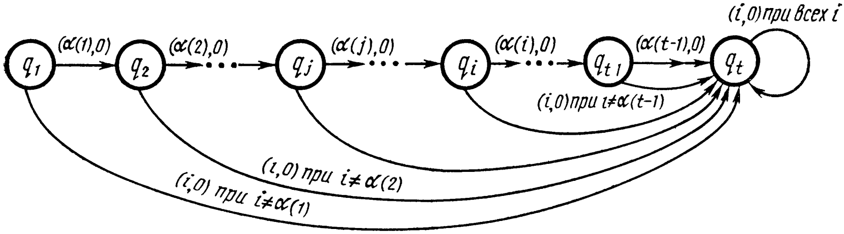

Рис. 2 18.

Очевидно, $\mathfrak{A}^1$ — приведенный. Пусть далее, $i\in\{1, \ldots, t-1\}$; $j\in 1, \ldots, i-]\log_m t[, i+1, \ldots, t-]\log_m t[\}$; $z\in\{1, \ldots, \alpha(i)-1, \alpha(i)+1, \ldots, m\}$; $a\in A^{n-t}$. Определяем автомат $\mathfrak{A}^2(i, j, z, a)$ при помощи диаграммы, приведенной на рис. 2.19.

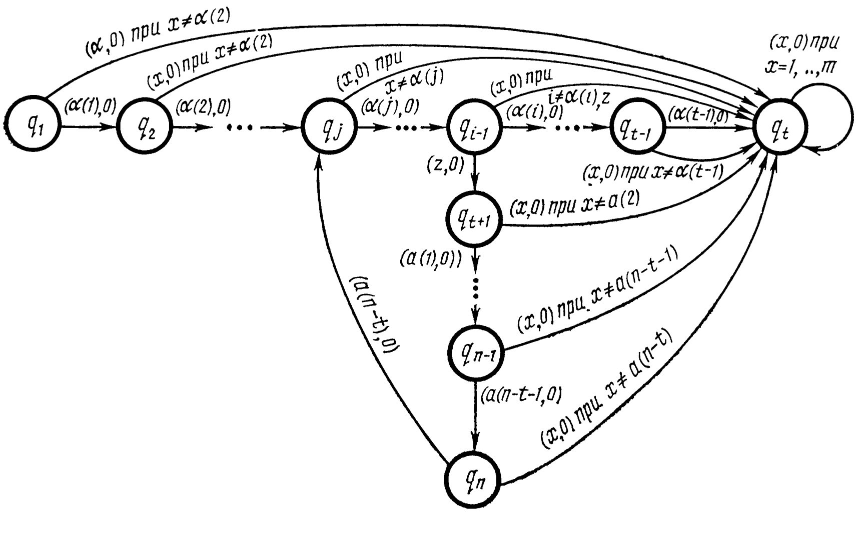

Рис. 2.19.

Для различения $\mathfrak{A}^1_{q_1}$ и $\mathfrak{A}^2_{q_1}(i, j, z, a)$ при $i<j$ необходимо слово, началом которого является $\alpha(1)\ldots\alpha(i-1)za(1)\ldots a(n-t)\alpha(j)\ldots\ldots\alpha(t-1)$. Для различения их при $i>j$ необходимо слово, началом которого при некотором $c\geqslant 0$ является $\alpha(1)\ldots\alpha(i-1)za(\alpha(j)\ldots\ldots\alpha(i-1)za)^c\alpha(j)\ldots\alpha(i-1)\alpha(i)\ldots\alpha(t-1)$. Легко убедиться, что эти слова различны при различных значениях i, z, a. Но, так как длина слова $\alpha(j)\ldots\alpha(t-1)$ в случае $i<j$ и слова $\alpha(j)\ldots\alpha(i-1)$ в случае $j<i$ не меньше $]\log_m t[$ и α не содержит двух равных отрезков длины $]\log_m t[$, не могут совпадать и отличающие $\mathfrak{A}^1_{q_1}$ от $\mathfrak{A}^2_{q_1}(i, j, z, a)$ слова при одинаковых i, z, a, но разных j. Поэтому наименьшим по объему и кратности множеством M, различающим $\mathfrak{A}^1_{q_1}$ и все $\mathfrak{A}^2_{q_1}(i, j, z, a)$, является множество, состоящее из всех слов вида $\alpha(1)\ldots\alpha(i-1)za\alpha(j)\ldots\alpha(t-1)$ при всех указанных i, j, z, a.

При фиксированном i величина j может принимать не менее $t-2]\log_m t[$ значений, z — $(m-1)$ значение, a — m^{n-t} значений, поэтому при каждом i соответствующая часть множества M содержит не менее $(t-2]\log_m t[)(m-1)m^{n-t}\sim t(m-1)m^{n-t}$ слов, сумма длин которых не менее

$$\sum_{j=2]\log_m t[}^{t-1}(m-1)m^{n-t}(i+n-t+t-j)\sim$$

$$\sim t\left(i+n-\frac{t}{2}\right)(m-1)m^{n-t}.$$

Величина i может принимать $t-1$ значение, поэтому:

$$k_T(m, n, t)\geqslant t^2(m-1)m^{n-t};$$

$$v_T(m, n, t)\geqslant\sum_{i=1}^{t-1}t\left(i+n-\frac{t}{2}\right)(m-1)m^{n-t}\sim t^2n(m-1)m^{n-t}.$$

Для оценки $l_T(m, n, t)$ рассматриваем автоматы $\mathfrak{A}^3$ и $\mathfrak{A}^4(i, j, z, a)$, отличающиеся от $\mathfrak{A}^1$ и $\mathfrak{A}^2(i, j, z, a)$ лишь тем, что стрелки, ведущие от состояния q_i, где $i<t$, к состоянию q_t и отмеченные парой $(x, 0)$, перебрасываются к состоянию q_1. Кратчайшим словом, отличающим $\mathfrak{A}^3_{q_1}$ и $\mathfrak{A}^4_{q_1}(t, 1, z, a)$, является слово $\alpha(1)\ldots\alpha(t-1)$ $za(1)\ldots a(n-t)\alpha(1)\ldots\alpha(t-1)$. Его длина равна $t-1+1+n-t+t-1=n+t-1$, откуда и вытекает $l_T(m, n, t)\geqslant n+t-1$. Теорема доказана.

Глава III
АВТОМАТЫ КАК АКЦЕПТОРЫ

§ 1. ПРЕДСТАВЛЕНИЕ СОБЫТИЙ АВТОМАТАМИ. ТЕОРЕМА КЛИНИ

Здесь мы рассмотрим ставшую классической для теории автоматов задачу о представлении событий автоматами.

Пусть заданы инициальный абстрактный конечный автомат $\mathfrak{A}_q = (A, Q, B, \varphi, \psi, q)$ и подмножество $B' \subseteq B$. Будем говорить, что автомат $\mathfrak{A}_q$ представляет подмножество E, $E \subseteq A^*$ с помощью выделенного подмножества B', если для любого слова α из A^* вхождение α в E эквивалентно соотношению $\psi(q, \alpha) \in B'$. Автомат $\mathfrak{A}_q$ с выделенным подмножеством B' будем обозначать через $(\mathfrak{A}_q, B')$ или через $(A, Q, B, \varphi, \psi, q, B')$. Подмножества множества A^* в дальнейшем будем называть событиями. Событие, E, $E \subseteq A^*$, назовем **представимым автоматом** $\mathfrak{A}_q$ **с помощью** B' (т. е. парой $(\mathfrak{A}_q, B')$, или объектом $(A, Q, B, \varphi, \psi, q, B')$. Главной нашей задачей будет описание всех представимых событий. Введем некоторые операции над событиями.

Объединением событий E_1 и E_2 называется множество $E_1 \cup E_2$, состоящее в точности из всех тех слов α, которые входят хотя бы в одно из множеств E_1 и E_2.

Произведением событий E_1 и E_2 называется множество $E_1 \cdot E_2$, состоящее в точности из всех таких слов α, что для некоторых слов α_1 из E_1 и α_2 из E_2 имеет место $\alpha = \alpha_1\alpha_2$.

Итерацией события E называется множество E^*, состоящее при $E \neq \varnothing$ в точности из всех таких слов α, что для некоторых слов $\alpha_1, \alpha_2, \ldots, \alpha_n$ из E имеет место $\alpha = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n$. Если $E = \varnothing$, то $E^* = \varnothing$.

Нетрудно видеть, что операции объединения и произведения событий ассоциативны. Это позволяет использовать сокращенные обозначения $\bigcup_{i=1}^{n} E_i$ и $\prod_{i=1}^{n} E_i$ для выражений $E_1 \cup \ldots \cup E_n$ и $E_1 \cdot \ldots \cdot E_n$ соответственно. Операция объединения коммутативна, т. е. для любых событий E_1 и E_2 справедливо равенство $E_1 \cup E_2 = E_2 \cup E_1$, а операция произведения не является коммутативной. Далее, для любого события E справедливо соотношение $(E^*)^* = E^*$; кроме того, полагая $E^1 = E$ и $E^n = \prod_{i=1}^{n} E_i$, где $E_i = E$, очевидно, имеем

$E^* = \bigcup_{j=1}^{\infty} E^j$. Отметим, наконец, что введенное нами ранее обозначение A^* согласуется с только что введенной операцией итерации.

Введем индуктивно **понятие регулярного события над алфавитом** $A=\{a_1, \dots, a_m\}$. Для краткости мы будем опускать слова «над алфавитом А» и говорить просто о регулярных событиях или о регулярных множествах.

а) Каждое из множеств $\{a_i\}$; $i=1, \dots, m$, а также пустое множество являются регулярными.

б) Если множества E_1 и E_2 регулярные, то каждое из множеств $E_1 \cup E_2$, $E_1 \cdot E_2$, $E_1{}^*$ также является регулярным.

Следующая теорема Клини [11] дает исчерпывающее описание представимых событий.

Теорема 3.1. Для заданного конечного алфавита A событие $E \subseteq A^*$ является представимым тогда и только тогда, когда оно регулярно.

Доказательство. Докажем сначала, что каждое регулярное множество является представимым.

Нетрудно видеть, что каждое из множеств $\{a_i\}$; $i=1, \dots, m$ и пустое множество являются представимыми. В самом деле, объект $(A, \{q^1, q^2\}, \{0, 1\}, \varphi, \psi, q^1, \{1\})$, где $\varphi(q, a)=q^2$; $q \in \{q^1, q^2\}$, $a \in A$, а $\psi(q^1, a_i)=1$ и $\psi(q, a)=0$ при $(q, a) \neq (q^1, a_i)$, очевидно, представляет множество $\{a_i\}$, а объект $(A, \{1\}, \{0, 1\}, 1, 0, \{1\})$ представляет пустое множество.

Доказательство представимости множеств $E_1 \cup E_2$, $E_1 \cdot E_2$ и $\overset{*}{E_1}$ для представимых множеств E_1 и E_2 вынесем в ряд отдельных утверждений.

Лемма 3.1. Если события E_1 и E_2, E_1, $E_2 \subseteq A^*$, представимые, то событие $E_1 \cup E_2$ также представимое.

Доказательство. Пусть события E_1 и E_2 представляются автоматами $\mathfrak{A}_q = (A, Q, B, \varphi, \psi, q)$ и $\mathfrak{A}_{q'} = (A, Q', B', \varphi', \psi', q')$ с помощью подмножеств B_1, $B_1 \subseteq B$, и B_1', $B_1' \subseteq B'$, соответственно.

Рассмотрим автомат $\mathfrak{A}_q \times \mathfrak{A}_{q'} = (A, Q \times Q', B \times B', (\varphi, \varphi'), (\psi, \psi'), (q, q'))$ и обозначим через $\overline{B}$ множество таких пар (b, b') из $B \times B'$, что или $b \in B_1$, или $b' \in B_1'$. Нетрудно видеть, что событие, представимое объектом $(\mathfrak{A}_q \times \mathfrak{A}_{q'}, B)$ совпадает с событием $E_1 \cup E_2$. Лемма доказана.

Лемма 3.2. Если события E_1 и E_2; E_1, $E_2 \subseteq A^*$, представимые, то событие $E_1 \cdot E_2$ также представимое.

Доказательство. Пусть события E_1 и E_2 представляются автоматами $\mathfrak{A}_q = (A, Q, B, \varphi, \psi, q)$ и $\mathfrak{A}_{q'} = (A, Q', B', \varphi', \psi', q')$ с помощью подмножеств B_1, $B_1 \subseteq B$; B_1', $B_1' \subseteq B'$, соответственно. Обозначим через $2^{Q'}$ множество всех подмножеств T множества Q' и рассмотрим инициальный автомат $\widetilde{\mathfrak{A}}_{(q, \varnothing)} = (A, Q \times 2^{Q'}, \{0, 1\}, \widetilde{\varphi}, \widetilde{\psi}, (q, \varnothing))$. Определим функцию $\widetilde{\varphi}$ этого автомата следующим образом:

$$\widetilde{\varphi}((q^i, T), a) = (\varphi(q^i, a), \{\varphi'(t, a) : t \in T\} \cup U),$$

где $q^i \in Q$; запись $\{\varphi'(t, a) : t \in T\}$ означает, что берется множество всех таких $\varphi'(t, a)$, для которых существует t из T, а U равно $\varnothing$, если $\psi(q^i, a) \in B \setminus B_1$, и U равно $\{q'\}$, если $\psi(q^i, a) \in B_1$; $\widetilde{\psi}((q^i, T), a) = 1$ тогда и только тогда, когда существует такое t из T, что $\psi'(t, a) \in B_1'$.

Покажем, что $(\widetilde{\mathfrak{A}}_{(q,\varnothing)}, \{1\})$ представляет множество $E_1 \cdot E_2$. В самом деле, пусть сначала имеется слово α^p из A^*, никакое собственное начало которого не является словом из E_1. Тогда каждое значение $\widetilde{\varphi}((q, \varnothing), \underset{r}{\underline{\alpha|}})$, где $r < p$, имеет вид $(q_j, \varnothing)$ и, значит, $\widetilde{\psi}((q, \varnothing), \alpha^p) = 0$, т. е. α^p не входит в то множество, которое представляется объектом $(\widetilde{\mathfrak{A}}_{(q,\varnothing)}, \{1\})$. Пусть теперь α^p имеет вид $\alpha^r \cdot \gamma^s$, где $\alpha^r \in E_1$ и $s \geqslant 1$, и пусть $(r_1, s_1), \ldots, (r_l, s_l)$ — всевозможные пары таких значений для r и s. Тогда, как нетрудно видеть, из определения автомата $\widetilde{\mathfrak{A}}_{(q,\varnothing)}$ вытекает, что

$$\widetilde{\varphi}((q, \varnothing), \underset{p-1}{\underline{\overline{\alpha^p}|}}) = (\varphi(q, \underset{p-1}{\underline{\overline{\alpha^p}|}}, \{\varphi'(q', \underset{s_1-1}{\underline{\overline{\gamma^{s_1}}|}}), \varphi'(q', \underset{s_2-1}{\underline{\overline{\gamma^{s_2}}|}}), \ldots, \varphi'(q', \underset{s_l-1}{\underline{\overline{\gamma^{s_l}}|}})\}),$$

и так как вычисление $\widetilde{\psi}((q, \varnothing), \alpha^p)$, очевидно, сводится к установлению существования в последовательности

$$\psi'(\varphi'(q', \underset{s_1-1}{\underline{\overline{\gamma^{s_1}}|}}), \delta_{s_1}), \psi'(\varphi'(q', \underset{s_2-1}{\underline{\overline{\gamma^{s_2}}|}}), \delta_{s_2}), \ldots, \psi'(\varphi'(q', \underset{s_l-1}{\underline{\overline{\gamma^{s_l}}|}}), \delta_{s_l}),$$

где δ_{s_i} — последняя буква в слове γ^{s_i} $(i = 1, 2, \ldots, l)$ хотя бы одного значения из B_1', то обращение выражения $\widetilde{\psi}((q, \varnothing), \alpha^p)$ в единицу эквивалентно возможности записать α^p в виде $\alpha^r \gamma^s$, где $\alpha^r \in E_1$ и $\gamma^s \in E_2$. Тем самым объект $(\widetilde{\mathfrak{A}}_{(q,\varnothing)}, \{1\})$ представляет событие $E_1 \cdot E_2$, и лемма доказана.

Лемма 3.3. Если событие E, $E \subseteq A^*$, представимое, то событие E^* также представимое.

Доказательство. Пусть событие E представимо автоматом $\mathfrak{A}_q = (A, Q, B, \varphi, \psi, q)$ с помощью подмножества B_1, $B_1 \subseteq B$. Вновь обозначим через 2^Q множество всех подмножеств T множества Q и рассмотрим инициальный автомат $\widetilde{\mathfrak{A}}_{\{q\}} = (A, 2^Q, \{0, 1\}, \widetilde{\varphi}, \widetilde{\psi}, \{q\})$. Определим функции $\widetilde{\varphi}$ и $\widetilde{\psi}$ этого автомата следующим образом:

$$\widetilde{\varphi}(T, a) = \{\varphi(t, a) : t \in T\} \cup U,$$

где U равно $\{q\}$, если существует такое t из T, что $\varphi(t, a) \in B_1$, в противном случае U равно $\varnothing$, функция $\widetilde{\psi}(T, a)$ равна 1 тогда и только тогда, когда существует такое t из T, что $\psi(t, a) \in B_1$. Покажем, что $(\widetilde{\mathfrak{A}}_{\{q\}}, \{1\})$ представляет событие E^*. В самом деле, пусть сначала имеется слово $\alpha^p \in A^*$, никакое начало которого не является словом из E. Тогда, как нетрудно, видеть, $\widetilde{\varphi}(\{q\},$

$\overline{\underset{p-1}{\alpha^p}|}) = \{\varphi(q, \overline{\underset{p-1}{\alpha^p}|})\}$, и, значит, $\tilde{\psi}(\{q\}, \alpha^p) = \tilde{\psi}(\{\varphi(q, \overline{\underset{p-1}{\alpha^p}|})\}, \delta_p)$, где δ_p — последняя буква слова α_p. Так как $\psi(q, \alpha^p) = \psi(\varphi(q, \overline{\underset{p-1}{\alpha^p}|}), \delta_p)$ и, очевидно, $\alpha^p \notin E^*$, то $\psi(q, \alpha^p) \notin B_1$, а отсюда следует, что $\psi(\{\varphi(q, \overline{\underset{p-1}{\alpha^p}|})\}, \delta_p) = 0$. Тем самым слово α^p не входит в событие, представимое объектом $(\tilde{\mathfrak{A}}_{\{q\}}, \{1\})$. Пусть теперь α^p имеет вид $\alpha^{r_1}\alpha^{r_2}\ldots\alpha^{r_l}\gamma^s$, где слово α^{r_i} содержится в E; γ^s или пустое, или ни одно его начало не содержится в E, а $i=1, 2, \ldots, l$. Ясно, что такое разложение слова α^p, вообще говоря, не однозначно. Зафиксируем какое-нибудь из них.

Как нетрудно видеть, из определения автомата $\tilde{\mathfrak{A}}_{\{q\}}$ вытекает, что множество $\tilde{\varphi}(\{q\}, \overline{\underset{p-1}{\alpha^p}|})$ содержит каждое из состояний

$$\varphi(q, \overline{\underset{p-1}{\alpha^{r_1}\alpha^{r_2}\ldots\alpha^{r_l}\gamma^s}|}),\ \varphi(q, \overline{\underset{p-r_1-1}{\alpha^{r_2}\alpha^{r_3}\ldots\alpha^{r_l}\gamma^s}|}), \ldots,$$

$$\varphi(q, \overline{\underset{p-(r_1+\ldots+r_{l-1})-1}{\alpha^{r_l}\gamma^s}|}),\ \varphi(q, \overline{\underset{p-(r_1+\ldots+r_l)-1}{\gamma^s}|})$$

и всякое состояние множества $\tilde{\varphi}(\{q\}, \overline{\underset{p-1}{\alpha^p}|})$ получается указанным образом из соответствующего представления слова α^p в виде $\alpha^{r_1}\alpha^{r_2}\ldots\alpha^{r_l}\gamma^s$. Заметим теперь, что вычисление значения $\tilde{\psi}(q, \alpha^p)$ сводится к установлению существования такого разложения слова α^p в виде $\alpha^{r_1}\alpha^{r_2}\ldots\alpha^{r_l}\gamma^s$, что γ^s пусто. Если такое представление возможно, то $\tilde{\psi}(q, \alpha^p)=1$; если оно невозможно, то $\tilde{\psi}(q, \alpha^p)=0$. Тем самым $(\tilde{\mathfrak{A}}_{\{q\}}, \{1\})$ представляет событие E^*, и лемма доказана.

Из доказанных утверждений вытекает представимость каждого регулярного множества.

Покажем, что имеет место и обратное утверждение.

Для этого нам понадобится ряд понятий и вспомогательных утверждений. Пусть на $A=\{a_1, \ldots, a_m\}$ задано некоторое бинарное отношение R, т. е. для каждой упорядоченной пары (a, b) имеет место aRb или не имеет места aRb, последнее мы обозначим через $\overline{aRb}$. Слово $\alpha=a(1)a(2)\ldots a(t)$ из A^* назовем при $t>1$ R-словом, если для любого j; $j=1, 2, \ldots t-1$ имеет место $a(j)Ra(j+1)$. При $t=1$ слово α является по определению R-словом.

Лемма 3.4. Пусть заданы алфавит A и бинарное отношение R на нем, тогда для любых фиксированных элементов a и b из A множество T всех R-слов из A^*, начинающихся с a и кончающихся на b, является регулярным.

Доказательство. Рассуждение будем вести с помощью индукции по числу m элементов в A.

Пусть $m=1$, $A=\{a_1\}$. Тогда искомое множество всех R-слов совпадает, очевидно, с $\{a_1\}^*$ при условии, что R не пусто, то есть a_1Ra_1. Если же бинарное отношение R пустое, то искомое множество равно $\{a_1\}$.

Пусть теперь $m>1$, и наше утверждение доказано для всех n, $n<m$. Докажем его справедливость для алфавита A, состоящего из m букв. Рассмотрим два случая.

1) Пусть $a=b$. Тогда любое R-слово из T длины, большей чем единица, выделением в нем всех вхождений буквы a может быть записано в виде $a\alpha_1 a\alpha_2 a \ldots a\alpha_r a$, где слово α_i может быть пустым, если справедливо aRa и в любом случае не содержит буквы a, $i=1, 2, \ldots, n$. Пусть $e_1, e_2, \ldots, e_t$; $t\geqslant 0$ — все такие буквы из A, отличные от a, что имеет место aRe_j, $j=1, 2, \ldots, t$, и $f_1, f_2, \ldots, f_s$; $s\geqslant 0$ — все такие буквы из A, отличные от a, что справедливо f_kRa, $k=1, 2, \ldots, s$. Тогда любое непустое слово α_i является R-словом, начинающимся с e, $e\in\{e_1, e_2, \ldots, e_t\}$, кончающимся на f, $f\in\{f_1, \ldots$ $\ldots, f_s\}$ и не содержащим буквы a, т. е. является R-словом в алфавите $A\setminus\{a\}$. По предположению индукции для каждой пары (e, f) множество Bef всех таких слов является регулярным.

Указанных множеств — конечное число l, не превосходящее t_s; пусть $B_1, B_2, \ldots, B_l$ — все эти множества. Тогда если справедливо aRa, то множество C всех R-слов вида $a\alpha_i$, очевидно, совпадает с множеством $\{a\}\cup\{a\}(B_1\cup B_2\cup\ldots\cup B_l)$. Если же выполнено $\overline{aRa}$, то множество C совпадает с множеством $\{a\}\cdot(B_1\cup B_2\cup\ldots\cup B_l)$. Таким образом, множество C регулярно. Нетрудно видеть, что в обоих случаях $T=\{a\}\cup(C^*\cdot\{a\})$, т. е. T является регулярным.

2) Пусть $a\neq b$. Так как пустое множество является регулярным, то можно считать, что $T\neq\varnothing$. Тогда любое слово из T может быть представлено в виде $a\alpha a\gamma b$ или $a\gamma b$, где γ не содержит буквы a. Пусть $\mathscr{D}$ — множество всех R-слов, начинающихся и оканчивающихся на букву a. Как показано в пункте 1), это множество регулярно. Пусть $e_1, e_2, \ldots, e_t$; $t\geqslant 0$, — все такие буквы из A, отличные от a, что имеет место aRe_j, $j=1, 2, \ldots, t$. Пусть $\mathscr{F}_{eb}$ — множество всех таких R-слов, которые не содержат буквы a, начинаются на некоторую букву e из множества $\{e_1, \ldots, e_t\}$ и оканчиваются на букву b. Этих множеств, очевидно, конечное число l, $l\geqslant m$, и каждое из них, по предположению индукции, регулярно. Пусть $\mathscr{F}_1, \mathscr{F}_2, \ldots, \mathscr{F}_l$ — все эти множества. Тогда, как нетрудно видеть, $T=\mathscr{D}\cdot(\mathscr{F}_1\cup\mathscr{F}_2\cup\ldots\cup\mathscr{F}_l)$, т. е. T — регулярное множество. Лемма доказана.

Пусть для конечного алфавита A выполнено $A=A_1\times A_2$ и $\alpha=(a^1(1), a^2(1))\ldots(a^1(t), a^2(t))$ — некоторое слово в алфавите A, где $a^1(j)\in A_1$, $a^2(j)\in A_2$; $j=1, 2, \ldots, t$. Обозначим через $\mathrm{pr}^i\alpha$ слово $a^i(1)a^i(2)\ldots a^i(t)$, $i=1, 2$, и назовем его **проекцией слова α на i-ю координату.**

Пусть имеется множество $\mathscr{D}$, $\mathscr{D}\subseteq A^*$, тогда через $\mathrm{pr}^i\mathscr{D}$ обозначим множество всех проекций слов из $\mathscr{D}$ на i-ю координату.

Лемма 3.5. Если множество E, $E\subseteq A^*$, регулярно, то при $A=$ $=A_1\times A_2$ множество $\mathrm{pr}^i E$ также регулярно.

Доказательство этого утверждения вытекает из того, что отдельные буквы из A_i обозначают регулярные множества и из следующих легко проверяемых соотношений:

$$\mathrm{pr}^i(E_1 \cup E_2) = (\mathrm{pr}^i E_1) \cup (\mathrm{pr}^i E_2),$$
$$\mathrm{pr}^i(E_1 E_2) = (\mathrm{pr}^i E_1) \cdot (\mathrm{pr}^i E_2),$$
$$\mathrm{pr}^i(E_1^*) = (\mathrm{pr}^i E_1)^*, \text{ где } E_1, E_2 \subseteq A_-^*, \ i = 1, 2.$$

Используя доказанные вспомогательные утверждения, установим теперь регулярность каждого представимого множества.

Пусть имеется объект $(A, Q, B, \varphi, \psi, q^1, B_1)$, который представляет множество E, $E \subseteq A^*$. Обозначим через T множество $Q \times A$ и через T' — множество всех пар (q, a) из $Q \times A$, таких, что $\psi(q, a) \in B_1$. На множестве T определим бинарное отношение R: $(q, a) R (q', a')$ справедливо тогда и только тогда, когда $q' = \varphi(q, a)$.

Для фиксированных пар (q^1, a) и (q', a') из множеств T и T' соответственно рассмотрим множество $E_{(q^1,a),(q',a')}$ всех R-слов из T^*, начинающихся с пары (q^1, a) и оканчивающихся парой (q', a'). По лемме 3.4 множество $E_{(q^1,a),(q',a')}$ регулярно. Варьируя пары (q^1, a) и (q', a'), получим все такие множества E_1, E_2, ..., E_l, где $l \leqslant |A|^2 |Q|$. Далее, нетрудно видеть, что $E = \bigcup_{i=1}^{l} \mathrm{pr}^2 E_i = \mathrm{pr}^2 (\bigcup_{i=1}^{l} E_i)$, и так как, очевидно, множество $\bigcup_{i=1}^{l} E_i$ регулярно, то по лемме 3.5 множество E также регулярно, что и требовалось доказать. Теорема 3.1, таким образом, полностью доказана.

Отметим, что в приведенном здесь доказательстве теоремы Клини использованы построения работ [12, 13].

Ясно, что не всякое событие является представимым. Так как всего событий имеется континуум, а представимых событий, очевидно, только счетное множество, то замеченное выше следует уже из мощностных соображений. На самом деле, можно указать эффективные примеры событий довольно простой логической природы, которые не являются представимыми. В качестве такого примера рассмотрим множество E_0 всех слов из $\{0, 1\}^*$, длина которых равна точным квадратам натуральных чисел. Покажем, что оно не является представимым. В самом деле, рассмотрим произвольный объект $(\mathfrak{A}_{q_1}, B_1) = (\{0, 1\}, Q, B, \varphi, \psi, q_1, B_1)$, в котором без ограничения общности можно считать, что $B = \{0, 1\}$ и $B_1 = \{1\}$. Если бы объект $(\mathfrak{A}_q, B_1)$ представлял множество E_0, то, применяя автомат $\mathfrak{A}_q$ к входному сверхслову 000..., мы, очевидно, получили бы выходное сверхслово, у которого на местах под номерами, соответствующими точным квадратам натуральных чисел, стоят единицы, а на остальных местах стоят нули, тем самым выходная последовательность была бы непериодической. С другой стороны, так как сверхслово 000... — периодическое, то, в силу теоремы 2.1, указанное выходное сверхслово должно быть периодическим. Полученное противоречие доказывает наше утверждение.

В заключение опишем некоторые способы задания регулярных событий.

Пусть $A=\{a_1, \ldots, a_m\}$ — конечный алфавит. **Регулярными выражениями над** A будем называть слова в алфавите $\{a_1, \ldots, a_m, \varnothing, \vee, \cdot, *, (,)\}$, определяемые индуктивно следующим образом:

1) Каждая буква a_i алфавита A, а также символ $\varnothing$ суть регулярные выражения над A.

2) Если R_1 и R_2 — регулярные выражения над A, то $(R_1 \vee R_2)$, $(R_1 \cdot R_2)$, $(*R_1)$ — также регулярные выражения над A. Говорим, что $(R_1 \vee R_2)$ есть **дизъюнкция**, $(R_1 \cdot R_2)$ — **конъюнкция**, $(*R_1)$ — **итерация выражений** R_1 и R_2.

Вместо $(*R)$ далее используем обозначение R^* или $\langle R \rangle$, где скобки $\langle, \rangle$ называем итерационными скобками.

С каждым регулярным выражением R над алфавитом A связано соответствующее регулярное событие $|R|$. А именно:

1) если R есть буква a_i, то $|R|=\{a_i\}$, $i \in \{1, 2, \ldots, m\}$;

2) если R есть $\varnothing$, то $|R|=\varnothing$;

3) $|(R_1 \vee R_2)| = |R_1| \cup |R_2|$, $|(R_1 \cdot R_2)| = |R_1| \cdot |R_2|$ $|(*R_1)| = |R_1|^*$.

Другим способом задания регулярных событий, как следует из теоремы 3.1, служит задание при помощи представляющих их автоматов. Если регулярное событие задано своим регулярным выражением, то рассуждения использованные при доказательстве этой теоремы, позволяют построить автомат, представляющий то же событие, и, наоборот, от задания события посредством представляющего это событие автомата перейти к заданию его регулярным выражением. Покажем, что для любого регулярного события α существует автомат с выходным алфавитом $\{0, 1\}$, представляющий это событие посредством множества $\{1\}$. Действительно, если $\mathfrak{A}=(A, Q, B, \varphi, \psi, q_0)$ — некоторый автомат, представляющий α посредством $B' \subseteq B$, то рассмотрим автомат $\mathfrak{A}'=(A, Q, \{0, 1\}, \varphi, \psi', q_0)$, такой, что $\psi'(q, a)=1$ тогда и только тогда, когда $\psi(q, a) \in B'$; очевидно, он и будет искомым автоматом.

Пусть автоматы $\mathfrak{A}=(A, Q, \{0, 1\}, \varphi, \psi, q_0)$ и $\mathfrak{A}'=(A, Q', \{0, 1\}, \varphi', \psi', q_0')$ представляют события α и α' соответственно посредством множества $B'=\{1\}$. Если $\alpha \neq \alpha'$, рассмотрим слово p, входящее в одно из этих событий и не входящее в другое; пусть для определенности $p \in \alpha$, $p \notin \alpha'$. Тогда $\psi(q_0, p)=1$, $\psi'(q_0', p)=0$ и слово p отличает состояния q_0 и q_0'. Обратно, пусть состояния q_0 и q_0' отличимы и p — кратчайшее, отличающее их слово. Тогда слова $\overline{\psi}(q_0, p)$ и $\overline{\psi}'(q_0', p)$ должны отличаться своими последними буквами, т. е. $\psi(q_0, p) \neq \psi'(q_0', p)$, откуда получаем, что p входит в одно из событий α, α' и не входит в другое, т. е. $\alpha \neq \alpha'$. Равенство событий α и α' эквивалентно, таким образом, неотличимости состояний q_0 и q_0', а так как последняя устанавливается на словах длины $|Q|+|Q'|-1$, получаем также эффективную процедуру проверки равенства регулярных событий, заданных указанным способом. Если события α и α' заданы каким-либо иным образом (при помощи регулярных выражений и т. д.), то для проверки их равенства достаточно перейти к их заданию автоматами $\mathfrak{A}$ и $\mathfrak{A}'$ указанного вида и затем выяснить, отличимы ли состояния q_0 и q_0'.

Опишем способ задания регулярных событий из A^* при помощи так называемых источников.

Источник над алфавитом A представляет собой конечный ориентированный граф G, каждому ребру которого сопоставлен символ алфавита A и у которого выделена вершина v_0, называемая начальной; выделено подмножество $F \neq \varnothing$ вершин, называемых финальными, причем выполнены условия:

1) различным ребрам, выходящим из одной вершины, сопоставлены различные символы алфавита A;

2) для каждой вершины v существует путь π_1, ведущий к v от v_0, и путь π_2, ведущий от v к некоторой финальной вершине.

Каждый источник G над алфавитом A задает событие $|G|$ — множество всех слов $p = a_{i1} \ldots a_{ik}$ в алфавите A, таких, что существует ведущий от v_0 к финальной вершине v_{ik} путь $\pi = v_0 \rho_{i1} v_{i1} \ldots$ $\ldots \rho_{ik} v_{ik}$ в источнике G, у которого ребру ρ_{ij} $(1 \leqslant j \leqslant k)$ сопоставлен символ a_{ij}. Будем говорить, что слово $a_{i1} \ldots a_{ik}$ соответствует пути π и обозначать это слово $[\pi]$. Заметим, что $|G|$ может содержать пустое слово.

Покажем, что произвольное непустое регулярное событие может быть задано некоторым источником и, наоборот, каждый источник задает регулярное при отбрасывании пустого слова событие.

Пусть автомат $\mathfrak{A}_{q_0} = (A, Q, B, \varphi, \psi, q_0)$ представляет непустое событие E, $E \subset A^*$, с помощью множества B', $B' \subseteq B$. Построим граф G, вершинами которого являются элементы множества $\{q_0\} \cup \{(q_i, b_j) \mid q_i \in Q, b_j \in B\}$. Из каждой вершины графа G выходят ребра, отмеченные всеми различными буквами $a_i \in A$, причем из вершины q_0 ребро с отметкой a_i ведет к вершине $(\varphi(q_0, a_i), \psi(q_0, a_i))$, а из каждой вершины (q_i, b_j) ребро с отметкой a_l ведет к вершине $(\varphi(q_i, a_l), \psi(q_i, a_l))$. Если в графе G выделить в качестве начальной вершину q_0, а в качестве множества F — финальных вершин — все такие пары (q_i, b_j), что $b_j \in B'$, после чего отбросить все вершины графа G, не лежащие на путях, ведущих от q_0 к вершинам из F, то, как легко заметить, получается источник G', задающий то же событие, что и пара $(\mathfrak{A}_{q_0}, B')$.

Обратно, если задан источник G над алфавитом A с начальной вершиной v_0 и множеством F финальных вершин, то рассмотрим автомат $\mathfrak{A}_{v_0}(A, Q, \{0, 1\}, \varphi, \psi, v_0)$, такой, что Q есть объединение множества вершин источника G с некоторым вспомогательным элементом v', а функции φ и ψ определяются так:

$$\varphi(v, a) = \begin{cases} v', & \text{если } v = v' \text{ либо из } v \text{ не выходит} \\ & \text{ребро с отметкой } a, \\ w, & \text{если в источнике } G \text{ от вершины } v \\ & \text{к вершине } w \text{ ведет ребро с отметкой } a; \end{cases}$$

$$\psi(v, a) = \begin{cases} 1, & \text{если } \varphi(v, a) \in F, \\ 0, & \text{если } \varphi(v, a) \notin F. \end{cases}$$

Нетрудно видеть, что $|G| \setminus \{\Lambda\}$ совпадает с событием, представимым парой $(\mathfrak{A}_{v_0}, \{1\})$.

Число вершин источника G далее обозначаем $\|G\|$.

Для описания регулярных событий можно использовать также понятие **квазиисточника над алфавитом** A, определение которого получается из определения источника отбрасыванием условий 1) и 2). Квазиисточник G определяет событие $|G|$, образованное всеми словами в алфавите A, соответствующими путям в G, ведущим от v_0 к вершинам из F.

Очевидно, любое регулярное событие определяется некоторым квазиисточником. Пусть, обратно, G — квазиисточник над алфавитом A, имеющий начальную вершину v_0 и множество F финальных вершин. Для установления регулярности события $|G|$ достаточно рассмотреть автомат $\mathfrak{A} = (A, Q, \{0, 1\}, \varphi, \psi, \{v_0\})$, состояниями которого служат всевозможные подмножества вершин квазиисточника (включая пустое множество); $\varphi(q, a)$ есть множество всех вершин, к которым от вершин множества q ведут стрелки, отмеченные буквой a, а $\psi(q, a) = 1$ тогда и только тогда, когда $\varphi(q, a) \cap F \neq \varnothing$. Нетрудно проверить, что $\varphi(\{v_0\}, \alpha)$ есть множество всех вершин квазиисточника, к которым от v_0 ведет путь, отметки ребер которого образуют слово α, так что $\mathfrak{A}$ представляет событие $|G|$ посредством множества $\{1\}$.

УПРАЖНЕНИЯ

1. Доказать нерегулярность события над алфавитом $\{0, 1\}$, состоящего из всех симметричных слов. (Слово $\alpha = a(1)a(2)\ldots a(n)$ называется симметричным, если $a(1)a(2)\ldots a(n) = a(n)\ldots$ $\ldots a(2)a(1)$.)
2. Является ли регулярным событие над алфавитом $\{0, 1\}$, состоящее из всех слов $\alpha = a(1)a(2)\ldots a(n)$, являющихся двоичными записями простых чисел?
3. Доказать регулярность события над алфавитом $\{0, 1\}$, состоящее из всех слов, имеющих четное число единиц.
4. Доказать, что если события $E_1, E_2 \subseteq A^*$ регулярны, то регулярны также события $E_1 \cap E_2$; $E_1 \setminus E_2$.
5. Существует ли нерегулярное событие E такое, что событие $E \cdot E$ регулярно?
6. Найти все решения уравнения $X = A \cdot X \cup B$, где A, B — заданные регулярные события.
7. Квазиисточник G над алфавитом $\{0, 1, 2\}$ имеет 4 вершины: v_0, v_1, v_2, v_3. Для любых $i, j \in \{0, 1, 2\}$ из вершины v_i к вершине v_j ведет ребро с отметкой $i \pmod 3$. Начальная вершина квазиисточника G есть v_0, множество финальных вершин — $\{v_0, v_1, v_3\}$. Построить источник, представляющий то же событие, что и G.

8. Пусть Q_n — число слов, определяемых регулярным выражением $(0,10^*1\vee 111)^*$ и имеющих длину, не превосходящую n. Найти величину $\lambda = \lim\limits_{n\to\infty} \frac{\log_2 Q_n}{n}$.

§ 2. АЛГОРИТМЫ АНАЛИЗА И СИНТЕЗА АВТОМАТОВ

В теоретических и прикладных аспектах автоматов важную роль играют так называемые задачи анализа и синтеза автоматов. Многообразие способов, описывающих функционирование автоматов, может быть разбито условно на две группы: группу языков, т. е. алгебро-логических описаний, и группу способов, описывающих внутренние процессы реальных автоматов, примером которых могут служить диаграммы Мура, источники и др. Переход от способа первого типа ко второму называется синтезом автоматов, а от второго к первому — анализом автоматов. В качестве способа первого типа в этом параграфе будет рассматриваться язык регулярных выражений; в качестве способов второго типа — диаграммы Мура и источники.

Пусть инициальный автомат $\mathfrak{A}_q=(A, Q, B, \varphi, \psi, q)$ задан диаграммой Мура и $B'\subseteq B$. При решении задачи анализа (т. е. задачи нахождения регулярного выражения, определяющего событие, представимое парой $(\mathfrak{A}_q, B')$) в этом случае можно перейти сначала от пары $(\mathfrak{A}_q, B')$ к источнику G, как это показано в предыдущем параграфе, и далее решать задачу анализа для источника G. Аналогично, при решении задачи синтеза по заданному регулярному выражению пары $(\mathfrak{A}_q, B')$, определяющей то же событие, что и рассматриваемое выражение, можно сначала решить задачу синтеза соответствующего источника, от которого и перейти к искомой паре $(\mathfrak{A}_p, B')$. В силу сказанного, будем далее рассматривать в качестве способа второго типа описания функционирования автоматов только язык источников. При этом оказывается удобным расширить язык регулярных выражений, используя наряду с символами $a_1, \ldots, a_n$ основного алфавита A также символ e, обозначающий событие $\{\Lambda\}$. Далее будем считать, что $\Lambda\in|\langle R\rangle|$.

Пусть задан источник G. Задачу построения регулярного выражения R, такого, что $|G|=|R|$, будем называть **задачей анализа источника** G.

Опишем способ **А** анализа источников. Обозначим $G^v_{v_0v_1\ldots v_s}$ $(s\geqslant 0)$ источник, получающийся из источника G удалением вершин $v_0, v_1, \ldots, v_s$ и всех других вершин источника G, которые оказываются недостижимыми из вершины v после удаления $v_0, v_1, \ldots$ $\ldots, v_s$ вместе с инцидентными им ребрами, у которого v есть начальная и единственная финальная вершина. То регулярное выражение, которое получается в результате анализа источника G, будем обозначать $\mathbf{A}(G)$.

Пусть источник G состоит только из одной вершины v и не имеет ребер. Тогда по определению $\mathbf{A}(G)=e$.

Теперь определим $\mathbf{A}(G)$ для источников, имеющих единственную финальную вершину, совпадающую с начальной. Множество всех таких источников специального вида обозначим через M. Пусть $G \in M$, $\|G\| = 1$, т. е. G имеет вид, изображенный на рис. 3.1. Тогда полагаем

$$\mathbf{A}(G) = \langle a_{i1} \vee \dots \vee a_{ik} \rangle.$$

Пусть для всех $G \in M$, таких, что $\|G\| \leqslant n$, уже определено $\mathbf{A}(G)$, и пусть $\|G\| = n+1$; v_0 — начальная вершина G. Рассмотрим некоторый простой цикл π в источнике G, проходящий через вершину v_0 (рис. 3.2). Если $k=0$, то положим $R(\pi) = a_{i1}$. Если $k > 0$, то рассмотрим источники $G_1 = G^{v_1}, \dots, G_{k-1} = G^{v_{k-1}}_{v_0 v_1 \dots v_{k-2}}, G_k = G^{v_k}_{v_0 v_1 \dots v_{k-1}}$.

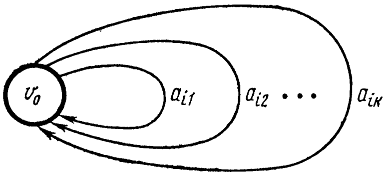

Рис. 3.1.

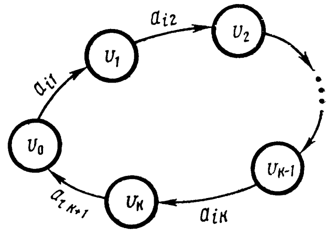

Рис. 3.2.

По предположению индукции уже определены выражения $R_1 = \mathbf{A}(G_1)$, ..., $R_k = \mathbf{A}(G_k)$. Положим $R(\pi) = a_{i1} R_1 a_{i2} R_2 \dots a_{ik} R_k a_{i\,k+1}$. Определим теперь $\mathbf{A}(G)$ как $\mathbf{A}(G) = \langle \bigvee_{\pi \in C} R(\pi) \rangle$, где C — множество всех простых циклов, проходящих через v_0. Таким образом, при $G \in M$ мы уже определили $\mathbf{A}(G)$.

Пусть G — произвольный источник с начальной вершиной v_0 и множеством F финальных вершин. Рассмотрим некоторый простой путь π, ведущий из вершины v_0 к финальной вершине v_k (см. рис. 3.3). Пусть $G_0 = G^{v_0}$, $G_1 = G^{v_1}_{v_0}, \dots, G_k = G^{v_k}_{v_0 v_1 \dots v_{k-1}}$, причем

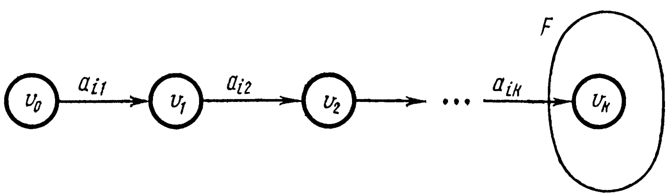

Рис 3 3.

$R_0 = \mathbf{A}(G_0)$, $R_1 = \mathbf{A}(G_1)$, ..., $R_k = \mathbf{A}(G_k)$. Положим $R(\pi) = R_0 a_{i1} R_1 \dots \dots a_{ik} R_k$. Если $v_0 \notin F$, то определим

$$\mathbf{A}(G) = \bigvee_{\pi \in P} R(\pi),$$

где P — множество всех простых путей от v_0 к F. Если же $v_0 \in F$, то полагаем

$$\mathbf{A}(G) = \bigvee_{\pi \in P} R(\pi) \vee R_0.$$

Корректность описанного способа анализа **А** доказывается в следующей теореме.

Теорема 3.2. Для любого источника G имеет место равенство $|G| = |\mathbf{A}(G)|$.

Доказательство. Сначала докажем, что теорема верна для любого источника $G \in M$.

Пусть $G \in M$, $\|M\| = 1$, т. е. G имеет вид, изображенный на рис. 3.1, и пусть $p \in |G|$. Слову p соответствует путь $\pi \in G$ вида $\pi_1 \pi_2 \dots \pi_s$, где π_t — петля, проходящая через вершину v_0, отмеченная буквой a_{ij_t} $(1 \leqslant t \leqslant s)$. Ясно, что каждая буква $a_{ij} \in \{a_{i1}, \dots, a_{ik}\}$ принадлежит событию $|\mathscr{P}|$, где $\mathscr{P} = a_{i1} \vee a_{i2} \vee \dots \vee a_{ik}$ и, согласно определению итерации событий, очевидно, что $p \in |\langle \mathscr{P} \rangle| = A(G)$. Предположим теперь, что $p = a_{ij_1} a_{ij_2} \dots a_{ij_s}$, $p \in |\mathbf{A}(G)|$. Тогда каждой букве a_{ij_t} $(1 \leqslant t \leqslant s)$ соответствует член в выражении $\mathscr{P} = a_{i1} \vee \dots \vee a_{ik}$, а каждому члену — петля в источнике G, проходящая через вершину v_0, отмеченная этой буквой. Таким образом, слову p можно сопоставить путь π в источнике G, ребра которого последовательно отмечены буквами этого слова, что и показывает, что $p \in |G|$.

Предположим, что для всех $G \in M$, таких, что $\|G\| \leqslant n$, уже показано, что $|G| = |\mathbf{A}(G)|$, и пусть $\|G\| = n+1$; v_0 — начальная вершина G. Пусть p — любое слово, $p \in |G|$. Для него в источнике G существует путь π, выходящий из вершины v_0 и ведущий в вершину v_0. Путь π можно изобразить в виде $\pi = \pi_1 \dots \pi_s$ $(s \geqslant 1)$, где π_i $(1 \leqslant i \leqslant s)$ есть цикл, проходящий через v_0 ровно один раз. Поэтому $p = p_1 \dots p_s$, где p_i — слово, соответствующее циклу π_i. Известно, что циклу π_i соответствует простой цикл $\pi'_i = v_0 \rho_{i1} v_{i1} \dots \rho_{ik} v_{ik} \rho_{i\,k+1} v_0$, для которого способом **А** анализа источников строим выражение $R(\pi'_i)$, являющееся одним из членов дизъюнкции $\bigvee_{\pi'_i \in C} R(\pi'_i)$ (C — множество всех простых циклов, проходящих через v_0); $R(\pi'_i) = a_{i1} R_{i1} \dots a_{ik} R_{ik} a_{i\,k+1}$, где a_{ij} $(1 \leqslant j \leqslant k+1)$ — буква, являющаяся отметкой ребра ρ_{ij}, и R_{it} $(1 \leqslant t \leqslant k)$ — регулярное выражение, представляющее по предположению индукции регулярное событие, заданное источником $G^{v_{it}}_{v_0 v_{i1} \dots v_{it-1}}$. Если через p_{it} обозначим слово, принадлежащее $|R_{it}|$, то $p_i = a_{i1} p_{i1} a_{i2} \dots a_{ik} p_{ik} a_{i\,k+1}$ и $p_i \in |R(\pi'_i)|$. Отсюда $p = p_1 \dots p_s$, согласно определению итерации, принадлежит $|\langle \bigvee_{\pi'_i \in C} R(\pi'_i) \rangle| = |\mathbf{A}(G)|$.

Обратно, пусть слово $p \in \mathbf{A}(G) = |\langle \bigvee_{\pi'_i \in C} R(\pi'_i) \rangle|$. Его можно записать в виде $p = p_1 \dots p_n$, где p_i $(1 \leqslant i \leqslant n)$ — слово, принадлежащее хотя бы одному из членов дизъюнкции $\bigvee\limits_{\pi'_i \in C} R(\pi'_i)$. Предположим, что $p_i \in |R(\pi'_i)|$. Согласно способу **A** анализа источников, $R(\pi'_i)$ соответствует простой цикл $\pi'_i = v_0\rho_{i1}v_{i1} \ldots$ $\ldots \rho_{ik}v_{ik}\rho_{i\,k+1}v_0$; $R(\pi'_i) = a_{i1}R_{i1}a_{i2}R_{i2} \ldots a_{ik}R_{ik}a_{i\,k+1}$, где a_{il} $(1 \leqslant l \leqslant k+$ $+1)$ — отметка ребра ρ_{il}; R_{im} $(1 \leqslant m \leqslant k)$ — регулярное выражение, соответствующее источнику $G^{v_{im}}_{v_0v_{i1} \ldots v_{i\,m-1}}$, причем по предположению индукции $|R_{im}| = |G^{v_{im}}_{v_0v_{i1} \ldots v_{i\,m-1}}|$. Поэтому слову p_i можем сопоставить некоторый цикл $\tilde{\pi}_i$, проходящий через v_0, ребра которого отмечены последовательно его буквами. Тогда, очевидно, слову $p = p_1 \ldots p_n$ (n — произвольное) соответствует путь в источнике G, ведущий от вершины v_0 к v, у которого ребрам сопоставлены символы в том же самом порядке, что и в слове p, и поэтому $p \in G$.

Покажем теперь, что теорема верна и для любого источника G, с начальной вершиной v_0 и множеством F финальных вершин. Пусть сначала $v_0 \notin F$. Пусть $p \in |G|$. Слову p соответствует в источнике G путь π, выходящий из начальной вершины v_0 и ведущий в некоторую финальную вершину v_{ik}. Для пути π существует простой путь $\pi' = v_0\rho_{i1}v_{i1} \ldots \rho_{ik}v_{ik}$, $v_{ik} \in F$, которому соответствует член $R(\pi')$ в выражении $\mathbf{A}(G) = \bigvee\limits_{\pi' \in P} R(\pi')$, где P—множество всех простых путей из v_0 в некоторую финальную вершину; $R(\pi') =$ $= R_0a_{i1}R_{i1} \ldots a_{ik}R_{ik}$, причем $R_0 = \mathbf{A}(G_0)$, $R_{i1} = \mathbf{A}(G_{i1})$, ..., $R_{ik} = \mathbf{A}(G_{ik})$; $G_0 = G^{v_0}$, $G_{i1} = G^{v_{i1}}_{v_0}$, ..., $G_{ik} = G^{v_{ik}}_{v_0v_{i1} \ldots v_{i\,k-1}}$. Каждый из источников G_0, G_{i1}, ..., G_{ik} принадлежит множеству M источников специального вида, для которых уже показано, что $|G_0| = |\mathbf{A}(G_0)|$, $|G_{i1}| = |\mathbf{A}(G_{i1})|$, ..., $G_{ik} = |\mathbf{A}(G_{ik})|$. Слово p принадлежит хотя бы одному из $|R(\pi'_i)|$ и может быть записано в виде $p = p_0a_{i1}p_{i1} \ldots$ $\ldots a_{ik}p_{ik}$, где $p_0 \in |G_0|$; $p_{im} \in |G_{im}|$ $(1 \leqslant m \leqslant k)$, и поэтому $p \in$ $\in |\mathbf{A}(G)|$. Если $p \in |\mathbf{A}(G)|$, то можно, аналогично тому, как это делалось для источников специального вида, показать, что $p \in |G|$.

Для завершения доказательства теоремы заметим, что в случае $v_0 \in F$ рассуждения совершенно аналогичны. Теорема доказана.

Теперь опишем способ $\mathbf{A}_1$ анализа источников, представляющий собой некоторую модификацию способа **A**.

Если G — источник с начальной вершиной v_0 и $\pi = v_0\rho_1v_1 \ldots$ ρ_sv_s — простой путь в источнике G, то будем говорить, что источник $G(\pi) = G^{v_s}_{v_0v_1 \ldots v_{s-1}}$ соответствует пути π.

Пусть $\mathfrak{M}$— конечное множество слов в алфавите $\mathscr{A}$. Дерево $T(\mathfrak{M})$, вершинам которого сопоставлены взаимно-однозначно всевозможные начала слов из $\mathfrak{M}$, включая пустое слово e (причем если v — вершина, сопоставленная слову p; w — вершина, сопоставленная слову pa $(a \in \mathscr{A})$, то от v к w проводится ребро с отметкой a) будем называть **деревом, соответствующим множеству слов** $\mathfrak{M}$.

Способ $\mathbf{A}_1$ анализа источников определим индуктивно следующим образом.

Если источник G состоит только из одной вершины v и не имеет ребер, то по определению $\mathbf{A}_1(G)=e$.

Пусть $G\in M$, $\|G\|=1$. Тогда $\mathbf{A}_1(G)=\mathbf{A}(G)$.

Предположим, что для всех $G\in M$, таких, что $\|G\|\leqslant n$, уже определено $\mathbf{A}_1(G)$, и пусть $|G|=n+1$; v_0 — начальная вершина G. Рассмотрим множество $\mathfrak{M}$ всех слов, соответствующих простым циклам источника G (проходящим через v_0), и построим дерево $T(\mathfrak{M})$. Слово, сопоставленное вершине v дерева $T(\mathfrak{M})$ обозначим через p_v. Каждой вершине v дерева $T(\mathfrak{M})$ сопоставим также путь π_v в источнике G, соответствующий слову p_v. Легко заметить, что если v — неконцевая вершина дерева $T(\mathfrak{M})$, то путь π_v простой. Сопоставим каждой вершине v дерева $T(\mathfrak{M})$ регулярное выражение R_v следующим образом. Если v — концевая вершина дерева $T(\mathfrak{M})$, причем к ней ведет ребро с отметкой a, то полагаем $R_v=a$. Пусть v — вершина $T(\mathfrak{M})$, отличная от корня, причем к v ведет ребро с отметкой a, из v выходят ребра к вершинам $v_1, \ldots, v_k$ и $R_{v_1}, \ldots, R_{v_k}$ уже определены. Тогда полагаем $R_v= = a\mathbf{A}_1(G(\pi_v))(R_{v_1}\vee\ldots\vee R_{v_k})$. Если v_0 — корень дерева $T(\mathfrak{M}$, причем от v ведут ребра к вершинам $v_1, \ldots, v_s$ и $R_{v_1}, \ldots, R_{v_s}$ уже определены, то полагаем $R_{v_0}=R_{v_1}\vee\ldots\vee R_{v_s}$. Полагаем

$$\mathbf{A}_1(G)=\langle R_{v_0}\rangle.$$

Пусть G — произвольный источник с начальной вершиной v_0 и множеством F финальных вершин. Рассмотрим множество $\mathfrak{M}$ всех слов, соответствующих простым путям от v_0 к вершинам из F, и построим дерево $T(\mathfrak{M})$. Как и выше, обозначим p_v слово, сопоставленное вершине v, и π_v — путь в G, соответствующий слову p. Обозначим также w_v последнюю вершину пути π_v. Очевидно, π_v — простой. Каждой вершине v дерева $T(\mathfrak{M})$ сопоставим регулярное выражение R_v следующим образом. Если v — концевая вершина дерева $T(\mathfrak{M})$, причем к v ведет ребро с отметкой a, то полагаем $R_v=a\mathbf{A}_1(G(\pi_v))$. Пусть v—вершина $T(\mathfrak{M})$, отличная от корня, причем к v ведет ребро с отметкой a $(a\in\mathscr{A})$, из v выходят ребра к вершинам $v_1, \ldots, v_r$ и $R_{v_1}, \ldots, R_{v_r}$ уже определены. Тогда если $w_v\in F$, то полагаем $R_v=a\mathbf{A}_1(G(\pi_v))(e\vee R_{v_1}\vee\ldots\vee R_{v_r})$; если $w_v\notin F$, то $R_v=a\mathbf{A}_1(G(\pi_v)(R_{v_1}\vee\ldots\vee R_{v_r})$. Если v_0 — корень дерева $T(\mathfrak{M})$, причем от v_0' ведут ребра к вершинам $v_1, \ldots, v_t$ и $R_{v_1}, \ldots, R_{v_t}$ уже определены, то полагаем

$$R_{v_0}=\begin{cases}\mathbf{A}_1(G(\pi_{v_0}))(R_{v_1}\vee\ldots\vee R_{v_t}) \text{ при } w_{v_0'}\notin F,\\ \mathbf{A}_1(G(\pi_{v_0}))(e\vee R_{v_1}\vee\ldots\vee R_{v_t}) \text{ при } w_{v_0'}\in F.\end{cases}$$

Полагаем

$$\mathbf{A}_1(G)=R_{v_0}.$$

Теорема 3.3. Для любого источника G $|G|=\mathbf{A}_1(G)$.

Доказательство теоремы 3.3 аналогично доказательству теоремы 3.2.

Теперь рассмотрим задачу, обратную задаче анализа источников, т. е. **задачу синтеза источников.**

Пусть регулярное событие задано выражением R. Задачу построения источника G, такого, что $|G|=|R|$, будем называть **задачей синтеза источника** G.

Для описания в несколько модифицированной форме алгоритма S синтеза источников, предложенного В. М. Глушковым [14], введем ряд понятий.

Если регулярное выражение R имеет вид $R_1 \vee \dots \vee R_k$, где R_i $(1 \leqslant i \leqslant k)$ — регулярные выражения, не являющиеся дизъюнкциями, то $R_1, \dots, R_k$ называются **членами выражения** R. Если выражение R не является дизъюнкцией, то оно само является своим членом.

Разделяющими местами в регулярном выражении R называем специально вводимые знаки раздела (вертикальные линии), вставляемые между любыми двумя знаками этого выражения (включая скобки). Место, расположенное слева от самого левого символа выражения R, называется **начальным местом,** а место, которое расположено справа от самого правого символа выражения R, — **конечным.**

Вводятся следующие **правила подчиненности мест.**

1. Начальные места всех членов выражения R, заключенного в обычные или итерационные скобки, подчинены месту, находящемуся непосредственно слева от открывающей скобки.

2. Место, находящееся непосредственно справа от закрывающей скобки (обычной или итерационной), подчинено конечным местам всех членов выражения, заключенного в соответствующие скобки, а в случае итерационных скобок — также и месту, расположенному непосредственно слева от соответствующей открывающей скобки.

3. Начальные места всех членов выражения, заключенного в итерационные скобки, подчинены месту, расположенному непосредственно справа от соответствующей закрывающей скобки.

4. Место, находящееся непосредственно справа от символа пустого слова e, подчинено месту, расположенному непосредственно слева от этого символа.

5. Если место γ подчинено месту β, а место β подчинено месту α, то место γ подчинено месту α.

6. Каждое место подчинено самому себе.

7. Других случаев подчиненности мест нет.

Пусть p — слово в алфавите $\mathcal{A}$, над которым задано регулярное выражение R. Дадим индуктивное определение места выражения R, p-**следующего** за местом α этого выражения.

1) Место β e-следует за местом α тогда и только тогда, когда β подчинено месту α.

2) Пусть β p-следует за α, место γ подчинено месту β, причем

непосредственно справа от места γ расположена буква a. Тогда место δ, находящееся непосредственно справа от этой буквы a, pa-следует за местом α.

Основным местом в регулярном выражении R, заданном над алфавитом $\mathscr{A}$, называем место, непосредственно слева от которого стоит буква алфавита $\mathscr{A}$, а также начальное место. Основное место выражения R будем называть **финальным**, если ему подчинено конечное место этого выражения. Место в выражении R, непосредственно справа от которого стоит буква a алфавита $\mathscr{A}$, назовем **предосновным.**

Построим теперь источник $G=S(R)$ над алфавитом, совпадающим с алфавитом $\mathscr{A}$ заданного выражения R, такой, что $|G|=|R|$.

В качестве начальной вершины $\mathfrak{M}_0$ источника $G=S(R)$ берем начальное место выражения R. Пусть a — произвольная буква алфавита $\mathscr{A}$. Определим множество всех основных место выражения R, a-следующих за его начальным местом. Если $\mathfrak{M}_a\neq\varnothing$, то $\mathfrak{M}_a$ есть вершина источника G, в которую входит ребро, выходящее из вершины v_0, отметкой которого является буква a. Предположим, что v — уже построенная вершина источника G, представляющая собой непустое множество основных мест выражения R. Для произвольной буквы b алфавита $\mathscr{A}$ найдем множество $\mathfrak{M}_b$ всех основных мест выражения R, b-следующих хотя бы за одним местом множества основных мест v. Если $\mathfrak{M}_b=\varnothing$, то ребро с отметкой b из вершины v не проводится. Если $\mathfrak{M}_b\neq\varnothing$ совпадает с некоторой, уже построенной, вершиной w источника G, то проводим ребро из вершины v в вершину w, отмечая его буквой b. Если $\mathfrak{M}_b\neq\varnothing$ не совпадает ни с одной из уже построенных вершин, то строим новую вершину $\mathfrak{M}_b$ и ребро ρ, ведущее из v к $\mathfrak{M}_b$, отмечая это ребро буквой b. Вершина v построенного источника G является финальной, если она содержит хотя бы одно финальное место выражения R. (Финальные вершины источника G отмечаем некоторым способом, например, двойными кружками.) Заметим, что если k — общее число вхождений букв алфавита $\mathscr{A}$ в данное выражение R, то число вершин источника G не превосходит 2^{k+1}.

Корректность описанного способа синтеза S докажем в следующей теореме.

Теорема 3.4. Для любого регулярного выражения R имеет место $|R|=|S(R)|$.

Для доказательства теоремы введем понятие p-спектра регулярного выражения и докажем одно вспомогательное утверждение.

Пусть R — регулярное выражение и p — слово, заданное в алфавите $\mathscr{A}$. Множество основных мест выражения R, p-следующих за его начальным местом, будем называть **p-спектром** этого выражения и обозначать R_p. (В частности, R_e состоит из начального места выражения R.)

Лемма 3.6. Пусть R — регулярное выражение и $\mathfrak{M}$ — его основное место. Тогда существует слово p, такое, что множество мест выражения R, p-следующих за местом $\mathfrak{M}$, содержит хотя бы одно его финальное место.

Доказательство. Доказательство поведем индукцией по сложности n регулярного выражения R.

Если $n=1$, то R — буква, и утверждение, очевидно, верно.

Пусть лемма верна для всех регулярных выражений сложности $n\leqslant k$; рассмотрим выражение R сложности $k+1$. Предположим, что $R=\langle\mathscr{P}\rangle$. Пусть $\mathfrak{M}$ — любое основное место выражения R. Легко заметить, что либо $\mathfrak{M}$ — начальное место, либо $\mathfrak{M}$ есть основное место выражения $\mathscr{P}$. В первом случае обозначим $\mathfrak{M}'$ начальное место выражения $\mathscr{P}$, во втором — $\mathfrak{M}'=\mathfrak{M}$. По предположению индукции для $\mathfrak{M}'$ существует слово p', такое, что множество мест, p'-следующих за $\mathfrak{M}'$, содержит хотя бы одно финальное место выражения $\mathscr{P}$. Но в силу правил 2 и 5 о подчиненности мест регулярного выражения R, финальные места выражения $\mathscr{P}$ являются финальными местами выражения $R=\langle\mathscr{P}\rangle$, и в качестве слова p можно взять слово p'.

Пусть $R=(R_1\vee\ldots\vee R_s)$ $(s\geqslant 2)$ и $\mathfrak{M}$ — его основное место. Либо $\mathfrak{M}$ есть основное место некоторого выражения R_i $(1\leqslant i\leqslant s)$ сложности $n\leqslant k$, для которого по предположению индукции лемма верна, либо $\mathfrak{M}$ — начальное место выражения R, и тогда предположение индукции применяем для начального места выражения R_1. И снова, используя правила 2 и 5 о подчиненности мест регулярного выражения R, получаем, что лемма верна.

Предположим, что $R=R_1\ldots R_t$ $(t\geqslant 2)$ и $\mathfrak{M}$ — его основное место. Либо $\mathfrak{M}$ есть основное место некоторого сомножителя R_j $(1\leqslant j\leqslant t)$ выражения R, либо $\mathfrak{M}$ — начальное место выражения R. В первом случае обозначаем $\mathfrak{M}'=\mathfrak{M}$, во втором $\mathfrak{M}'$ — начальное место выражения R_j, $j=1$. По предположению индукции существует слово p_j, такое, что множество мест, p_j-следующих за $\mathfrak{M}'$ в R_j, содержит хотя бы одно финальное место выражения R_j. Обозначим $R'=R_{j+1}R_{j+2}\ldots R_s$. По предположению индукции существует слово p', такое, что множество мест, p'-следующих за начальным местом выражения R', содержит финальное место $\mathfrak{M}_f$ выражения R'. Очевидно, что множество мест, p_jp'-следующих за основным местом $\mathfrak{M}$ выражения R, содержит финальное место $\mathfrak{M}_f$. Поэтому в качестве слова p берем слово p_jp'. Лемма доказана.

Доказательство теоремы 3.4. Сначала докажем, что ориентированный граф $G=S(R)$ является источником. Из способа построения графа G следует, что различные ребра, выходящие из любой вершины (множество основных мест выражения R), отмечены различными буквами алфавита A. В силу предыдущей леммы из любой вершины графа G достижима финальная вершина G и граф $G=S(R)$ является источником.

Теперь покажем, что $|R|=|S(R)|$. Пусть p — слово, $p\in|R|$. Тогда, очевидно, R_p содержит хотя бы одно финальное место выражения R. Поэтому в источнике $S(R)$ существует ведущий к финальной вершине путь π, такой, что $[\pi]=p$, так что $p\in|S(R)|$. Предположим, что слово $p\in|S(R)|$. Тогда в источнике G существует путь π, $[\pi]=p$, по которому из начальной вершины достижима некоторая финальная вершина v. Так как начальная вершина источника G есть начальное место выражения R, а финальная вершина v — подмножество основных мест выражения R, содержащее хотя бы одно финальное место $\mathfrak{M}_f$, то $\mathfrak{M}_f \in R_p$ и $p \in |R|$. Теорема доказана.

Исходя из способа S синтеза источников, В. М. Глушков предложил ряд его уточнений и изменений, которые позволяют строить источники с меньшим числом вершин. Эти уточнения и изменения опишем в несколько модифицированном виде, более удобном для исследования качественных характеристик получаемых источников.

Введем несколько новых понятий.

Основные места регулярного выражения R, заданного над алфавитом $\mathscr{A}$, назовем **соответственными**, если множества слов алфавита $\mathscr{A}$, связывающих начальное место выражения R с каждым из этих мест, одинаковы.

Основные места $\mathfrak{M}_1, \dots, \mathfrak{M}_k$ выражения R называются **подобными**, если они одновременно финальные либо нефинальные, причем для любой буквы a из алфавита $\mathscr{A}$ множества $M_1, \dots, M_k$ основных мест выражения, a-следующих за местами $\mathfrak{M}_1, \dots, \mathfrak{M}_k$, одинаковы, либо становятся одинаковыми при замене входящих в них мест $\mathfrak{M}_2, \dots, \mathfrak{M}_k$ местом $\mathfrak{M}_1$.

К регулярному выражению R применяем так называемую **операцию отождествления мест.** Она состоит в отождествлении некоторых групп соответственных мест либо подобных мест. Заметим, что после отождествления по одному признаку места, которые было возможно отождествить по другому признаку, могут оказываться неотождествимыми.

Пусть π — последовательность отождествлений соответственных и подобных мест выражения R. Множества мест выражения R, оказавшихся отождествленными в результате применения последовательности π, будем называть **обобщенными местами** выражения R, соответствующими последовательности отождествлений π.

Пусть p — слово алфавита $\mathscr{A}$, над которым задано регулярное выражение R. Обобщенное место β выражения R **p-следует за** обобщенным местом α этого выражения, если некоторое основное место $\mathfrak{M}_\beta$ из β p-следует хотя бы за одним местом $\mathfrak{M}_\alpha$ из α. Будем также говорить, что β достижимо из α по слову p или что слово p связывает обобщенное место α с обобщенным местом β.

Пусть R — регулярное выражение и π — произвольная последовательность отождествлений соответственных и подобных мест этого выражения. Построим источник $G=S(\pi, R)$ над алфавитом $\mathscr{A}$ заданного выражения R, такой, что $|R|=|S(\pi, R)|$. Этот способ построения будем называть **улучшенным способом синтеза источников** В. М. Глушкова, соответствующим последовательности π отождествлений соответственных и подобных мест выражения R.

В качестве начальной вершины $\mathfrak{M}_0$ источника $G=S(\pi, R)$

берем обобщенное место выражения R, содержащее его начальное место. (Нетрудно заметить, что такое обобщенное место единственное для выражения R.) Пусть a — произвольная буква алфавита $\mathscr{A}$. Определим множество $\mathfrak{M}_a$ всех обобщенных мест выражения R, a-следующих за его начальным местом. Если $\mathfrak{M}_a \neq \varnothing$, то $\mathfrak{M}_a$ есть вершина источника $G=S(\pi, R)$, в которую входит ребро, выходящее из вершины $\mathfrak{M}_0$ и отмеченное буквой a. Предположим, что v — уже построенная вершина источника G, представляющая собой непустое множество обобщенных мест выражения R. Для произвольной буквы b в алфавите $\mathscr{A}$ найдем множество $\mathfrak{M}_b$ всех обобщенных мест выражения R, b-следующих хотя бы за одним обобщенным местом множества обобщенных мест v. Если $\mathfrak{M}_b = \varnothing$, то ребро с отметкой b из вершины v не проводится. Если $\mathfrak{M}_b \neq \varnothing$ и совпадает с некоторой уже построенной вершиной w источника $G=S(\pi, R)$, то проводим ребро из вершины v в вершину w, отмечая его буквой b. Если $\mathfrak{M}_b \neq \varnothing$ и не совпадает ни с одной из уже построенных вершин, то строим новую вершину $\mathfrak{M}_b$ и ребро ρ, ведущее из v к $\mathfrak{M}_b$, отмечая это ребро буквой b. Вершина построенного источника $G=S(\pi, R)$ является финальной, если она содержит хотя бы одно из обобщенных финальных мест выражения R. (Обобщенное место $\mathfrak{M}$ выражения R является финальным обобщенным местом этого выражения, если содержит хотя бы одно финальное место выражения R.)

Аналогично теореме 3.4, можно доказать, что для любого регулярного выражения R и любой последовательности π отождествлений соответственных и подобных мест выражения R имеет место $|R| = |S(\pi, R)|$.

УПРАЖНЕНИЯ

1. Источник G над алфавитом $\{0, 1\}$ имеет три вершины v_0, v_1, v_2. Из каждой вершины v_i этого источника $(i=0, 1, 2)$ выходят два ребра, одно из которых отмечено символом 0 и ведет к вершине v_i, а другое отмечено символом 1 и ведет к вершине $v_{i+1}(\mathrm{mod}\,3)$. Начальная вершина источника G_1 есть v_0, финальные вершины суть v_1, v_2. Найти регулярные выражения $\mathbf{A}(G)$ и $\mathbf{A}_1(G)$.
2. Источник G имеет 4 вершины. Каково наибольшее возможное число регулярных событий, представимых источниками вида $G^{v}_{v_0 v_1\;\; v_s}$?
3. Пусть R — регулярное выражение вида: $\langle b \vee a \langle a \rangle b \rangle a \langle a \rangle (a \vee b)$. Построить источник $S(R)$.
4. Найти все пары соответственных подобных мест в регулярном выражении $a\langle b \rangle \vee (c \vee a)(\langle c \rangle \vee \langle b \rangle)$. Построить источник $S(\pi, R)$ с наименьшим возможным числом вершин.
5. Существует ли регулярное выражение R, такое, что $S(R)$ есть источник G из упражнения 1?

§ 3. КАЧЕСТВЕННЫЕ ХАРАКТЕРИСТИКИ ОСНОВНЫХ АЛГОРИТМОВ АНАЛИЗА И СИНТЕЗА АВТОМАТОВ

В этом параграфе мы рассмотрим качественные характеристики алгоритмов анализа и синтеза автоматов, предложенных В. М. Глушковым и играющих важную роль в теории автоматов.

Мы исходим из задания автоматов при помощи источников. По этим источникам с помощью описанного алгоритма Глушкова **А** строится регулярное выражение. На этом этапе (т. е. при решении задачи анализа с помощью алгоритма **А**) возникает задача описания множества $\tilde{R}$ всех соответствующих регулярных выражений. Ее решение позволяет установить точное соответствие между классами источников J и соответствующими регулярными выражениями, восстанавливаемыми по источнику с помощью алгоритма **А**. Полученное описание позволяет перейти к задаче синтеза, т. е. задаче описания всех источников J', получаемых из регулярных выражений множества $\tilde{R}$ с помощью алгоритма Глушкова. На этом этапе основной задачей является описание класса всех источников, возникающих указанным образом. При этом представляется важным соотношение как классов J и J', так и их частей. Здесь приведем точное конструктивное описание класса $\tilde{R}$ и класса J', а также покажем, в каких случаях $G \in J$ и соответствующий $G' \in J'$ изоморфны, т. е. практически совпадают.

Определим некоторые понятия, связанные с регулярными выражениями.

Дадим индуктивное определение **ветви регулярного выражения** над алфавитом $\mathscr{A}$.

1°. Ветвью пустого слова e является само это слово.

2°. Для каждой буквы a алфавита A ее ветвями являются пустое слово и сама буква a.

3°. Если $P_1 \vee \ldots \vee P_n$ — регулярное выражение, то его ветвями являются ветви выражений $P_1, \ldots, P_n$.

4°. Ветвями регулярного выражения $R = P_1 \ldots P_k$ являются всевозможные выражения вида $P_1 \ldots P_l P$, где P — ветвь выражения P_{l+1} $(0 \leqslant l \leqslant k-1)$.

5°. Ветвями регулярного выражения $R = \langle P \rangle$ служат слово e и всевозможные выражения вида $\langle P \rangle L$, где L — ветвь выражения P.

Пусть $R < P$ означает, что регулярное выражение R является ветвью регулярного выражения P.

Лемма 3.7. Для любых регулярных выражений A, B и C, если $A < B$ и $B < C$, то $A < C$.

Доказательство. Доказательство поведем индукцией по сложности n регулярного выражения C.

Если $n = 1$, то C есть e либо буква, и утверждение очевидно.

Пусть лемма верна для всех $n \leqslant k$; рассмотрим выражение C сложности $k+1$. Пусть $C = \langle P \rangle$. Если $A = e$ либо $B = e$, то утверждение очевидно; пусть $A \neq e$, $B \neq e$. По определению ветви регулярного выражения ветвь B выражения C есть выражение $B =$

$=\langle P\rangle P'$, где $P'<P$, а ветвь A выражения B есть $A=\langle P\rangle P''$, где $P''<P$ либо $P''<P'$. В первом случае очевидно, что $A<C$, а в последнем случае, согласно предположению индукции, $P''<P$, откуда и вытекает, что $A<C$.

Пусть $C=C_1\vee\ldots\vee C_r$. Если $B<C_i$ $(1\leqslant i\leqslant r)$ и $A<B$, то по предположению индукции $A<C_i$ и поэтому $A<C$.

Предположим, что $C=C_1\ldots C_s$. По определению ветви, если $B<C$, то $B=C_1\ldots C_m C'_{m+1}$ $(1\leqslant m\leqslant s-1)$, где $C'_{m+1}<C_{m+1}$, и если $A<B$ то либо $A=C_1\ldots C_n C''_{n+1}$, где $C''_{n+1}<C_{n+1}$ $(0\leqslant n\leqslant m+1)$, либо $A=C_1\ldots C_m C''_{m+1}$, где $C''_{m+1}<C'_{m+1}$, и поэтому $A<C$. Лемма доказана.

Лемма 3.8. Если $R_1=\tilde{P}_0\langle\tilde{Q}_1\rangle L_1\tilde{P}_1\langle\tilde{Q}_2\rangle L_2\tilde{P}_2\ldots\langle\tilde{Q}_i\rangle$, $R_2=\tilde{P}_0\langle\tilde{Q}_1\rangle L_1\tilde{P}_1\langle\tilde{Q}_2\rangle\ldots\langle\tilde{Q}_j\rangle T$, где $i>j$, $L_k<\tilde{Q}_k$ $(1\leqslant k\leqslant i-1)$, $\tilde{P}_l$ — непустое слово $(1\leqslant l\leqslant i-1)$, $T<L_j\tilde{P}_j$, либо $T<\tilde{Q}_j$, причем $L_k a_k \nless Q_k$, где a_k — первая буква слова $\tilde{P}_k$ $(1\leqslant k\leqslant i-1)$, то $R_1\nless R_2$.

Доказательство. Доказательство поведем индукцией по i.

Если $i=1$, то $R_1=\tilde{P}_0\langle\tilde{Q}_1\rangle$, а $R_r=T<\tilde{P}_0$. Очевидно, что в этом случае $R_1\nless R_2$.

Предположим, что утверждение верно для каждого $i\leqslant n$. Докажем, что оно верно для $i=n+1$. Предположим, что оно неверно, т. е. что $R_1<R_2$. Рассмотрим сначала случай, когда $T<L_j\tilde{P}_j$. Последний сомножитель R_1 есть $\langle\tilde{Q}_i\rangle$, так что R_1 нельзя представить в виде $\tilde{P}_0\langle\tilde{Q}_1\rangle L_1\tilde{P}_1\ldots\langle\tilde{Q}_j\rangle L_j\tilde{P}'_j$, где $\tilde{P}'_j<P_j$ и $P_j\neq e$. Поэтому R_1 должно быть ветвью выражения $\tilde{P}_0\langle\tilde{Q}_1\rangle L_1\tilde{P}_1\ldots\langle\tilde{Q}_j\rangle L_j$, а вместе с тем, в силу леммы 3.7, и выражения $R'_2=\tilde{P}_0\langle\tilde{Q}_1\rangle L_1\tilde{P}_1\ldots$ $\ldots\langle\tilde{Q}_j\rangle$ (ибо $L_j<\tilde{Q}_j$). Если $T<\tilde{Q}_j$, то снова, в силу леммы 3.7, $R_1<R'_2$. Рассмотрим ветвь $R'_1<R_1$, имеющую вид $R'_1=\tilde{P}_0\langle\tilde{Q}_1\rangle L_1\tilde{P}_1\ldots\langle\tilde{Q}_i\rangle L_j a_j$, где a_j — первая буква слова $\tilde{P}_j$. По лемме 3.7 $R'_1<R'_2$. Но $L_j a_j\nless\tilde{Q}_j$, так что R'_1 представимо в виде $\tilde{P}_0\langle\tilde{Q}_1\rangle L_1\tilde{P}_1\ldots\langle\tilde{Q}_s\rangle T'$, где либо $T'<L_s\tilde{P}_s$, либо $T'<Q_s\,(s<j)$. Но $\tilde{P}_0\langle Q_1\rangle L_1\tilde{P}_1\ldots\langle\tilde{Q}_i\rangle<R'_1$, т. е. $\tilde{P}_0\langle\tilde{Q}_1\rangle L_1\tilde{P}_1\ldots\langle\tilde{Q}_i\rangle<\tilde{P}_0\langle\tilde{Q}_1\rangle L_1\tilde{P}_1\ldots\langle Q_s\rangle T'$, что невозможно по предположению индукции. Лемма доказана.

Регулярное выражение P будем называть **отделимым** от регулярного выражения Q (и обозначать $P\perp Q$), если P представимо в виде LaM, где $La\nless Q$ и существует b, такое, что $Lb<\tilde{Q}$. P **слабо отделимо** от Q $(P\pm Q)$, если $P\neq Q$ и либо $P<Q$, либо $Q<P$, либо $P\perp Q$ (L, M — регулярные выражения, a, b — буквы).

Пусть регулярное выражение R имеет вид

$$P_0\langle Q_1\rangle P_1\ldots P_{m-1}\langle Q_m\rangle P_m\quad(m\geqslant 0),$$

где P_i $(1\leqslant i\leqslant m)$ — слова алфавита A, $P_i\neq e$ $(1\leqslant i\leqslant m-1)$. Если для любого $i\in\{1, 2, \ldots, m\}$ выражение $R_i=P_i\langle Q_{i+1}\rangle P_{i+1}\ldots\langle Q_m\rangle P_m$ слабо отделимо от выражения Q_i, то назовем R **членом 1-го типа.** Если, кроме того, $P_0\neq e$, $P_m\neq e$ и для любого $i\in\{1, \ldots, m\}$ выражение R_i отделимо от выражения Q_i, то назовем R **членом 2-го типа.**

Следующая теорема позволяет описать множество $\tilde{R}$ всех регулярных выражений, получающихся способом **А** анализа источников.

Теорема 3.5 [15]. Регулярное выражение R принадлежит множеству $\tilde{R}$ тогда и только тогда, когда выполняются условия:

1) каждый член выражения R есть член 1-го типа, слабо отделимый от любого другого члена R;

2) если в R входит выражение вида $\langle P\rangle$, то каждый член P есть член 2-го типа, отделимый от любого другого члена P.

Для доказательства теоремы 3.5 нам понадобится ввести ряд новых понятий и доказать два вспомогательных утверждения.

Путь $\pi=v_0\rho_1v_1\ldots\rho_lv_l$ в источнике G с начальной вершиной v_0, где $v_j\neq v_r$, $j\neq r$; j, $r\in\{1, 2, \ldots, l-1\}$, $v_j\neq v_0$, $j\in\{1, 2, \ldots, l-1\}$, $l\geqslant 0$, будем называть **полупростым путем.**

Пусть $\pi=v_0\rho_1v_1\ldots\rho_sv_s$ — полупростой путь в источнике G; ρ — ребро выходящее из v_s и ведущее к некоторой вершине v. **Приведенный путь** $\overline{\pi\rho}$ пути $\pi\rho$ определим следующим образом:

а) если $v_s\neq v_i$ при всех i $(0\leqslant i\leqslant s-1)$, то $\overline{\pi\rho}=\pi\rho$;

в) если $v_s=v_i$ $(0\leqslant i\leqslant s-1)$, то $\overline{\pi\rho}=v_0\rho_1v_1\ldots\rho_iv_i\rho v$.

Очевидно, что $\overline{\pi\rho}$ — снова полупростой путь.

Лемма 3.9. Для любого регулярного выражения R вида $\langle P\rangle$, удовлетворяющего условиям теоремы 3.5, существует источник G, такой, что $\langle P\rangle=\mathbf{A}(G)$, причем

(1) источник G имеет единственную финальную вершину, совпадающую с начальной вершиной;

(2) если $\{a_{i_1}, \ldots, a_{i_k}\}$ — множество всех букв алфавита A, для которых выражение Sa_{i_j} является ветвью P $(1\leqslant j\leqslant k)$, — непусто, то в источнике G существует вершина v, такая, что источник G', получающийся из источника G выбором вершины v в качестве финальной, удовлетворяет условию $\mathbf{A}(G')=\langle P\rangle S$, и отметками ребер, ведущих из v, служат только буквы $a_{i_1}, \ldots, a_{i_k}$;

(3) для каждой вершины $v\in G$ существует единственный простой путь, ведущий из начальной вершины в эту вершину.

Доказательство. Доказательство поведем индукцией по числу d пар итерационных скобок регулярного выражения R.

Если $d=1$, тогда $R=\langle P_1\vee\ldots\vee P_s\rangle$, где каждое P_i $(1\leqslant i\leqslant s)$ есть слово алфавита A. Для каждого $P_i=a_i^{(1)}\ldots a_i^{(m_i)}$ $(1\leqslant i\leqslant s)$ построим цепочку ребер, выходящих из вершины v_0 (см. рис. 3.4, *а*). Склеим одинаково отмеченные ребра 1-го яруса, потом одинаково отмеченные ребра 2-го яруса, выходящие из одной и той же вершины и т д. В конце концов получаем дерево $\mathscr{D}$ с начальной вершиной v_0 и финальными вершинами $v_{f_1}, \ldots, v_{f_s}$ (рис. 3.4, *б*), представляющее событие $|P_1\vee\ldots\vee P_s|$. Легко заметить, что каждая вершина дерева по единственному пути достижима из начальной вершины v_0. Кроме того, пусть $Sa<P'$, $P'=P_1\vee\ldots\vee P_s$, где a — буква алфавита A, и пусть $\{a_{i1}, \ldots, a_{it}\}$ — все буквы алфавита A, для которых в P' найдется ветвь Sa_{ij} $(1\leqslant j\leqslant t)$.

Тогда легко показать, что в дереве существует вершина v, такая, что дерево, получающееся из дерева $\mathscr{D}$ выбором вершины v в качестве финальной, представляет событие $|S|$, причем отметками ребер, выходящих из v, служат только $a_{i1}, \ldots, a_{it}$.

Склеиваем все финальные вершины дерева $\mathscr{D}$ с его начальной вершиной. Получается источник G, который, как легко заметить, удовлетворяет условиям леммы.

Пусть лемма имеет место для всех $d \leqslant k$. Рассмотрим выражение $R = \langle P \rangle$ с $k+1$ парой итерационных скобок. В силу условий теоремы 3.5 P можно представить в виде

(1) $$P_1 \vee \ldots \vee P_l,$$

где P_i $(1 \leqslant i \leqslant l)$ есть член 2-го типа, т. е.

$$P_j = P_0^{(i)} \langle Q_1^{(i)} \rangle P_1^{(i)} \ldots P_{m_i-1}^{(i)} \langle Q_{m_i}^{(i)} \rangle P_{m_i}^{(i)} \quad (m_i \geqslant 0),$$

где $P_j^{(i)}$ — непустое слово $(0 \leqslant j \leqslant m_i)$. Заметим, что выражение P_i можно представить в виде

$$P_i = \widetilde{P}_0^{(i)} \langle \widetilde{Q}_1^{(i)} \rangle L_1^{(i)} \widetilde{P}^{(i)} \ldots \langle \widetilde{Q}_{n_i}^{(i)} \rangle L_{n_i}^{(i)} \widetilde{P}_{n_i}^{(i)} \quad (1 \leqslant i \leqslant n_l),$$

где $\widetilde{P}_s^{(i)}$ — непустое слово $(0 \leqslant s \leqslant n_i)$, $\widetilde{P}_0^{(i)} = P_0^{(i)}$, $\widetilde{Q}_1^{(i)} = Q_1^{(i)}$; $\widetilde{Q}_s^{(i)} = Q_{q_s}^{(i)}$ $(2 \leqslant s \leqslant n_i)$, $q_s \in \{2, 3, \ldots, m_i\}$, $L_j^{(i)} < \widetilde{Q}_j^{(i)}$, $L_j^{(i)} a_{j_i}^{(0)} < \widetilde{Q}_j^{(i)}$, где $a_{j_i}^{(0)}$ — первая буква слова $\widetilde{P}_j^{(i)}$.

Возьмем $P_1 = \widetilde{P}_0^{(1)} \langle \widetilde{Q}_1^{(1)} \rangle L_1^{(1)} \widetilde{P}_1^{(1)} \ldots \langle \widetilde{Q}_{n_1}^{(1)} \rangle L_{n_1}^{(1)} \widetilde{P}_{n_1}^{(1)}$. Для каждого слова $\widetilde{P}_j^{(1)} = a_j^{(0)} a_j^{(1)} \ldots a_j^{(s_j)}$ построим цепочку ребер, выходящих из вершины v_j $(1 \leqslant j \leqslant n_j)$; рис. 3.5. По предположению индукции для каждого сомножителя $\langle \widetilde{Q}_j^{(1)} \rangle$ мы уже умеем строить источник G_j^1, который удовлетворяет условиям леммы (см. рис. 3.6), т. е. $\mathbf{A}(G_j^1) = \langle \widetilde{Q}_j^{(1)} \rangle$. Источник G_j^1 имеет единственную финальную вершину, совпадающую с начальной v_j^1. Кроме того, в нем существует вершина $v_{g_j}^1$ такая, что источник, получающийся из источника

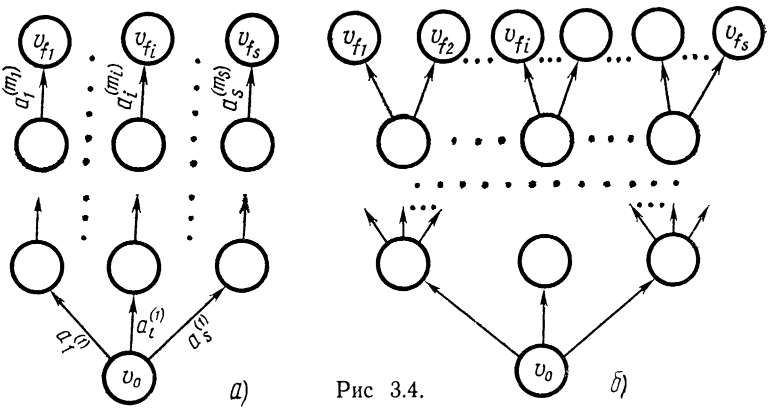

Рис 3.4.

G_j^1 выбором ее в качестве финальной, представляет событие $|\langle \widetilde{Q}_j^{(1)} \rangle L_j^{(1)}|$, причем из нее не выходит ребро с отметкой $a_j^{(0)}$. Если последнюю вершину цепочки, соответствующей слову $\widetilde{P}_0^{(1)}$, склеим с начальной вершиной источника G_j^1, а потом последовательно начальную вершину цепочки, соответствующей слову $\widetilde{P}_j^{(1)}$ с вершиной $v_{g_j}^{(1)}$ источника G_j^1, а последнюю — с начальной v_{j+1}^1 источника G_{j+1}^1, то получаем некоторый источник $\mathfrak{A}_1$, с начальной вершиной v_0 и финальной вершиной v_{f_1} (см. рис. 3.7), который, очевидно, представляет событие $|P_1|$, и $\mathbf{A}(\mathfrak{A}_1) = P_1$. Из способа построения этого источника $\mathfrak{A}_1$ очевидным образом следует, что в v_0 не ведут ребра и из v_f не выходят ребра.

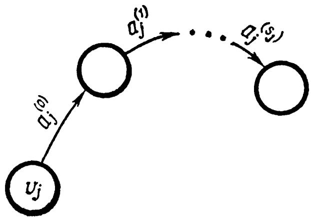

Рис. 3.5.

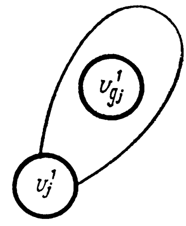

Рис. 3.6.

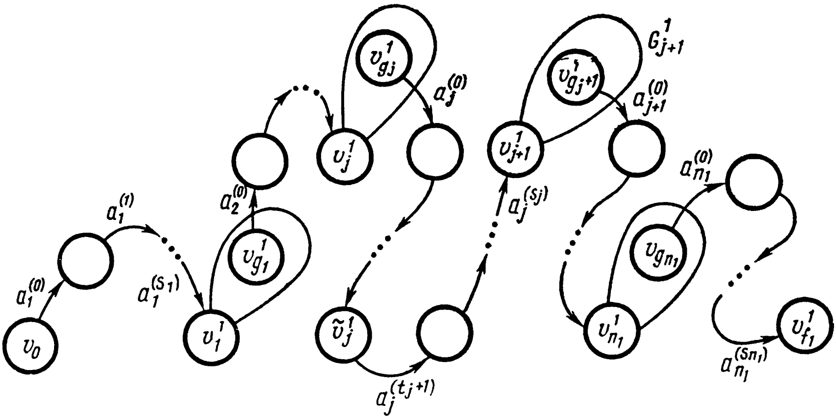

Рис. 3.7.

Пусть имеется ветвь Sa выражения P_1, где a — буква алфавита A, и пусть $\{a_{i1}, \ldots, a_{ir}\}$ — все буквы алфавита A, для которых у P_1 найдется ветвь Sa_{ij} $(1 \leqslant j \leqslant r)$. Покажем, что в источнике $\mathfrak{A}_1$ существует такая вершина v, что источник $\mathfrak{A}_1'$, получающийся из источника $\mathfrak{A}_1$ выбором вершины v в качестве финальной, удовлетворяет условию $\mathbf{A}(\mathfrak{A}_1') = S$, причем отметками ребер, ведущих из v, служат только буквы $a_{i1}, \ldots, a_{ir}$.

Если Sa — ветвь $\widetilde{P}_0^{(1)}$, то последнее утверждение очевидно. Пусть выражение Sa содержит хотя бы одну итерацию выражения

P_1. Очевидно, что Sa имеет вид $\widetilde{P}_0^{(1)} \langle \widetilde{Q}_1^{(1)} \rangle L_1^{(1)} \widetilde{P}_1^{(1)} \ldots \langle \widetilde{Q}_i^{(1)} \rangle T$, где либо $T < \widetilde{Q}_i^{(1)}$, либо $T < L_i^{(1)} \widetilde{P}_i^{(1)}$, причем T непусто $(1 \leqslant i \leqslant n_1)$ Пусть $Sb < P_1$. Тогда Sb представимо в виде $\widetilde{P}_0^{(1)} \langle \widetilde{Q}_1^{(1)} \rangle L_1^{(1)} \widetilde{P}_1^{(1)} \ldots \langle \widetilde{Q}_j^{(1)} \rangle T'$, где либо $T' < \widetilde{Q}_j^{(1)}$, либо $T' < L_j^{(1)} \widetilde{P}_j^{(1)}$, причем T' непусто $(1 \leqslant j \leqslant n_1)$. При $j < i$ получаем $\widetilde{P}_0^{(1)} \langle \widetilde{Q}_1^{(1)} \rangle L_1^{(1)} \widetilde{P}_1^{(1)} \ldots \langle \widetilde{Q}_i^{(1)} \rangle < Sb$, что невозможно в силу леммы 3.8. Так как T' непусто, то $\widetilde{P}_0^{(1)} \langle \widetilde{Q}_1^{(1)} \rangle L_1^{(1)} \widetilde{P}_1^{(1)} \ldots \langle \widetilde{Q}_j^{(1)} \rangle < S$, и при $j > i$ снова по лемме 3.8 приходим к противоречию. Поэтому $j = i$. Таким образом, каждое Sb, являющееся ветвью P_1, представимо в виде $Sb = NS'b$, где $N = \widetilde{P}_0^{(1)} \langle \widetilde{Q}_1^{(1)} \rangle L_1^{(1)} \widetilde{P}_1^{(1)} \ldots \langle \widetilde{Q}_j^{(1)} \rangle$, причем либо $S'b < \widetilde{Q}_j^{(1)}$, либо $S'b < L_j^{(1)} \widetilde{P}_j^{(1)}$. Обозначим через B множество всех b, таких, что $S'b < \widetilde{Q}_j^{(1)}$.

Рассмотрим три случая:

(1) $S' = L_j^{(1)}$. Тогда множество всех b, таких, что Sb — ветвь P_1, есть $\{a_j^{(0)}\} \cup B$. Легко заметить, что в этом случае в качестве вершины v достаточно взять $v_{g_j}^1$ (рис. 3.7).

(2) $S' \neq L_j^{(1)}$, причем существует такое b, что $S'b < \widetilde{Q}_j^{(1)}$. Тогда множество всех b, таких, что $Sb < P_1$, есть B. В качестве вершины v выберем вершину источника G_j^1, такую, что $\mathbf{A}(G_j^v) = \langle \widetilde{Q}_j^{(1)} \rangle S'$, где G_j^v — источник, получающийся из источника выбором вершины v в качестве финальной.

(3) $S' \neq L_j^{(1)}$, причем ни для одного b $S'b$ не является ветвью $\widetilde{Q}_j^{(1)}$. Тогда, если $\widetilde{P}_j^{(1)} = a_j^{(0)} \ldots a_j^{(s_j)}$, то $S' = L_j^{(1)} a_j^{(0)} a_j^{(1)} \ldots a_j^{(t_j)}$ $(1 \leqslant t_j \leqslant s_j)$, $Sb < P_1$ только при $b = a_j^{t_j+1}$, и в качестве вершины v достаточно взять вершину $\tilde{v}_j$ цепочки, отвечающей слову $\widetilde{P}_j^{(1)}$ $(1 \leqslant j \leqslant n_1)$, которая, очевидно, отлична от $v_{g_j}^1$ и v_{j+1}^1 (рис. 3.7).

Таким образом, в каждом из случаев искомая вершина v существует.

Так как для каждой вершины v по предположению индукции в источнике G_j^1 $(1 \leqslant j \leqslant n_1)$ существует единственный простой путь, ведущий из его начальной вершины v_j^1 в эту вершину, то, очевидно, этим свойством обладает и каждая вершина источника $\mathfrak{A}_1$.

Пусть уже построен источник $\mathfrak{A}_i$ $(2 \leqslant i \leqslant l)$, представляющий событие $|P_1 \vee \ldots \vee P_i|$ с начальной вершиной v_0 и финальными вершинами $v_{f_1}, \ldots, v_{f_i}$. Пусть также источник $\mathfrak{A}_i$ обладает следующим свойством. Если $R^{(i)}b$, где b — буква алфавита A, является ветвью выражения

$$P_1 \vee \ldots \vee P_i \tag{2}$$

и $\{b_{j1}, \ldots, b_{jk}\}$ — все буквы алфавита A, для которых выражение $R^{(i)}b_{it}$ $(1 \leqslant t \leqslant k)$ является ветвью выражения (2), то в источнике $\mathfrak{A}_i$ существует вершина v, такая, что источник $\mathfrak{A}_i'$, получающийся из источника $\mathfrak{A}_i$ выбором вершины v в качестве финальной, удовлетворяет условию $\mathbf{A}(\mathfrak{A}'_i)=R^{(i)}$, и отметками ребер, ведущих из v, служат только буквы $b_{j1},\ldots,b_{jk}$.

Пусть, далее, для каждой вершины v источника $\mathfrak{A}_i$ существует единственный простой путь, ведущий из начальной вершины v_0 **в эту** вершину. Возьмем P_{i+1} — член выражения (1), который, как уже заметили, можно представить в виде

$$P_{i+1}=\widetilde{P}_0^{(i+1)}\langle\widetilde{Q}_1^{(i+1)}\rangle L_1^{(i+1)}\widetilde{P}_1^{(i+1)}\ldots\langle\widetilde{Q}_{n_{i+1}}^{(i+1)}\rangle L_{n_{i+1}}^{(i+1)}\widetilde{P}_{n_{i+1}}^{(i+1)},$$

где $n_{i+1}\geqslant 0$, $\widetilde{P}_s^{(i+1)}$ — непустые слова алфавита A $(0\leqslant s\leqslant n_{i+1})$; $L_t^{(i+1)}<\widetilde{Q}_t^{(i+1)}$ $(1\leqslant t\leqslant n_{i+1})$, причем $L_t^{(i+1)}a_t^{(0)}\not< \widetilde{Q}_t^{(i+1)}$, где $a_t^{(0)}$ — первая буква слова $\widetilde{P}_t^{(i+1)}$. Из условия 2 теоремы 3.5 следует, что выражение P_{i+1} отделимо от каждого члена P_t $(1\leqslant t\leqslant i)$, т. е. представимо в виде $R_t^{(i+1)}a_t\mathfrak{M}_t^{(i+1)}$, где $R_t^{(i+1)}a_t\not< P_t$, но имеется буква b_t, такая, что $R_t^{(i+1)}b_t< P_t$.

Обозначим через $R_{\max}^{(i+1)}a$ выражение, содержащее максимальное число сомножителей и не являющееся ветвью ни одного выражения P_t, причем такое, что имеется хотя бы одна буква b, для которой $R_{\max}^{(i+1)}$ b является ветвью хотя бы одного члена P_t. По предположению индукции в источнике $\mathfrak{A}_i$ существует вершина v, такая, что источник $\mathfrak{A}'_i$ получающийся из источника $\mathfrak{A}_i$ выбором вершины v в качестве финальной, удовлетворяет условию $\mathbf{A}(\mathfrak{A}'_i)=R_{\max}^{(i+1)}$, и отметками ребер, ведущих из нее, служат только буквы b, для которых $R_{\max}^{(i+1)}b<P_1\vee\ldots\vee P_i$. Очевидно, из вершины v не выходит ребро с отметкой a. Пусть $P_{i+1}=R_{\max}^{(i+1)}$ $a\mathfrak{M}^{(i+1)}$, где $a\mathfrak{M}^{(i+1)}=S\langle\widetilde{Q}_{j+1}^{(i+1)}\rangle L_{j+1}^{(i+1)}\widetilde{P}_{j+1}^{(i+1)}\ldots\langle\widetilde{Q}_{n_{i+1}}^{(i+1)}\rangle L_{n_{i+1}}^{(i+1)}\widetilde{P}_{n_{i+1}}^{(i+1)}$ $(0\leqslant j\leqslant n_{i+1})$, S — выражение вида aS'. Тогда проведем из вершины v ребро с отметкой a и, поступая далее с выражением $S'\langle\widetilde{Q}_{j+1}^{(i+1)}\rangle L_{j+1}^{(i+1)}\widetilde{P}_{j+1}^{(i+1)}\ldots\langle\widetilde{Q}_{n_{i+1}}^{(i+1)}\rangle L_{n_{i-1}}^{(i+1)}\widetilde{P}_{n_{i+1}}^{(i+1)}$ так, как поступали с выражением P_1 при построении источника $\mathfrak{A}_1$, в конце концов получим источник $\mathfrak{A}_{i+1}$ с начальной вершиной v_0 и финальными вершинами $v_{f_1},\ldots,v_{f_{i+1}}$. Очевидно, что в вершину v_0 не входят ребра и из вершин $v_{f_j}(1\leqslant j\leqslant i+1)$ не выходят ребра.

Пусть имеется ветвь Sa выражения $P_1\vee\ldots\vee P_{i+1}$, где a — буква алфавита A, и пусть $\{a_{i1},\ldots,a_{it}\}$ — все буквы алфавита A, для которых $Sa_{ij}<P_1\vee\ldots\vee P_{i+1}$. Покажем, что в источнике $\mathfrak{A}_{i+1}$ существует вершина v, такая, что источник $\mathfrak{A}'_{i+1}$, получающийся из источника $\mathfrak{A}_{i+1}$ выбором вершины v в качестве финальной, удовлетворяет условию $\mathbf{A}(\mathfrak{A}'_{i+1})=S$, причем отметками ребер, ведущих из v, служат только буквы $a_{i_1},\ldots,a_{i_t}$.

Предположим сначала, что $Sa_{ir}<P_1\vee\ldots\vee P_i$ для каждого r $(1\leqslant r\leqslant t)$. Тогда, очевидно, в качестве финальной вершины v достаточно взять ту самую вершину, которую уже взяли для представления S в источнике $\mathfrak{A}_i$. Пусть теперь существует a, такое, что $Sa<P_{i+1}$, но $Sa\not<P_1\vee\ldots\vee P_i$. Рассмотрим два случая:

1) Пусть существует $r\,(1\leqslant r\leqslant t)$, такое, что $Sa_{i_r}<P_1\vee\ldots\vee P_i$. Тогда $S=R^{(i+1)}_{\max}$ либо $S=R^{(i+1)}_{\max}aT$ (T, быть может, пусто). Если $S=R^{(i+1)}_{\max}aT$, то $Sa_{i_r}=R^{(i+1)}_{\max}aTa_{i_r}<P_1\vee\ldots\vee P_i$, и по лемме 3.7 $R^{(i+1)}_{\max}a<P_1\vee\ldots\vee P_i$, что противоречит предположению о том, что $R^{(i+1)}_{\max}a\nless P_1\vee\ldots\vee P_i$. Отсюда $S=R^{(i+1)}_{\max}$, и в качестве вершины v достаточно взять указанную выше вершину источника $\mathfrak{A}_i$.

2) Для каждого a_{in} имеем $Sa_{i_r}<P_{i+1}$, но $Sa_{i_r}\nless P_1\vee\ldots\vee P_i$. В качестве вершины v нетрудно выбрать тогда одну из вершин источника $\mathfrak{A}_{i+1}$, построенных для выражения $S'\,\langle\widetilde{Q}^{(i+1)}_{j+1}\rangle\,L^{(i+1)}_{j+1}\,\widetilde{P}^{(i+1)}_{j+1}\ldots\langle\widetilde{Q}^{(i+1)}_{n_{i+1}}\rangle\,L^{(i+1)}_{n_{i+1}}\,\widetilde{P}^{(i+1)}_{n_{i+1}}$. Таким образом, мы показали, что в каждом случае вершина v существует.

Отметим еще одно свойство источника $\mathfrak{A}_{i+1}$: для каждой его вершины v существует единственный простой путь, связывающий начальную вершину v_0 с этой вершиной.

Аналогично тому, как был построен источник $\mathfrak{A}_{i+1}$, для выражения $P_1\vee\ldots\vee P_{i+1}$ строим, далее, источник $\mathfrak{A}_{i+2}$ для $P_1\vee\ldots\vee P_{i+2}$; $\mathfrak{A}_{i+3}$ — для выражения $P_1\vee\ldots\vee P_{i+3}$ $(i+3\leqslant l)$, и т. д. В конце концов построим источник $\mathfrak{A}_l$ с начальной вершиной v_0 и с различными финальными вершинами $v_{f_1},\ldots,v_{f_l}$, из которых не выходят ребра, представляющий событие $|P_1\vee\ldots\vee P_l|$, а $\mathbf{A}(\mathfrak{A}_l)=P_1\vee\ldots\vee P_l$.

Склеиванием всех финальных вершин источника $\mathfrak{A}_l$ с его начальной вершиной получается источник G, который удовлетворяет всем условиям леммы. Лемма доказана.

Полупростому пути $\pi=v_0\rho_1v_1\ldots\rho_sv_s$, принадлежащему источнику G, сопоставим выражения $R_1(\pi)=R_0a_1R_1\ldots R_{s-1}a_s$ и $R_2(\pi)=R_0a_1R_1\ldots R_{s-1}a_sR_s$, причем $[\pi]=a_1\ldots a_s$; $R_0=A(G^{v_0}),\ldots,R_i=A(G^{v_i}_{v_0v_1\ldots v_{i-1}})\,(1\leqslant i\leqslant s)$. Если путь π пустой, то $R_1(\pi)=e$, $R_2(\pi)=R_0$.

Лемма 3.10. Пусть G — источник и $R=\mathbf{A}(G)$. Тогда

1) для любого полупростого пути π в G имеем $R_1(\pi)<R$ и $R_2(\pi)<R$;

2) для любой ветви R' выражения R в источнике G существует полупростой путь π, такой, что R' есть либо $R_1(\pi)$, либо $R_2(\pi)$.

Доказательство. Пусть $G\in M$, $\|G\|=1$; см, рис. 3.1 (M — множество всех источников, имеющих единственную финальную вершину, совпадающую с начальной). Тогда утверждение очевидно.

Пусть для всех $G\in M$, таких, что $\|G\|\leqslant n$, лемма уже доказана. Докажем, что она верна, если $\|G\|\leqslant n+1$. Заметим сначала, что регулярное выражение $R=\mathbf{A}(G)$ имеет вид итерации, т. е.

$$R=\langle P_1\vee\ldots\vee P_k\rangle,\quad k\geqslant 1,$$

где P_i $(1\leqslant i\leqslant k)$ — члены, соответствующие простым циклам, проходящим через начальную вершину источника G.

(1). Пусть $\pi=v_0\rho_1v_1\ldots\rho_sv_s$ — любой полупростой путь в источнике G. Если π — пустой путь, то $R_1(\pi)=e$, $R_2(\pi)=R_0$ — ветви выражения R. Пусть π непустой. Покажем, что $R_1(\pi)=R_0a_1R_1\ldots$

$\dots R_{s-1}a_s$ и $R_2(\pi)=R_0a_1R_1\dots R_{s-1}a_sR_s$ суть ветви выражения R. В силу определения источника G существует простой путь π', ведущий от v_s к v_0 (возможно, пустой, если $v_0=v_s$). Если π' не проходит через вершины $v_0, v_1, \dots, v_{s-1}$, то получаем простой цикл $\pi\pi'$, которому соответствует некоторое выражение $P_i=aR_1\dots$ $\dots a_{s-1}R_{s-1}a_sR_s\dots R_{l_i}a_{l_i}$ $(l_i\geqslant s)$. Но $R=R_0$, так что $R_1(\pi)<RP_i<R$; $R_2(\pi)<RP_i<R$. Пусть теперь путь π' проходит через некоторые из вершин $v_0, v_1, \dots, v_{s-1}$. Пусть v_i $(1\leqslant i\leqslant s-1)$ — вершина с наименьшим номером i, принадлежащая π'. Пусть $\pi=\pi_1\pi_2$; $\pi'=\pi_1'\pi_2'$; $\tilde{\pi}=\pi_1\pi_2'$, где π_2' — конец пути π', начинающийся с вершины v_i, а π_1 — отрезок пути π от v_0 до v_i. Тогда $\pi_1\pi_2'$ — простой цикл, проходящий через вершину v_0. Ему соответствует некоторое выражение $P_j=a_1R_1a_2R_2\dots a_iR_iT$, где T — регулярное выражение, соответствующее пути π_2'. Легко заметить, что π_2 — полупростой путь, принадлежащий источнику $G^{v_i}_{v_0v_1\dots v_{i-1}}$. По предположению индукции $R_1(\pi_2)<R_i$, $R_2(\pi_2)<R_i$. Но $R_m(\pi)=R_0a_1R_1\dots a_iR_m(\pi_2)<$ $<R_0P_j<R$; $m=1, 2$. Таким образом, утверждение доказано для всех источников $G\in M$.

Пусть теперь G — произвольный источник с начальной вершиной v_0 и множеством F финальных вершин. Тогда выражение $R=$ $=\mathbf{A}(G)$ имеет вид

$$R=P_1\vee\dots\vee P_r\quad(r\geqslant 1).$$

Рассмотрим произвольный полупростой путь $\pi=v_0\rho_1v_1\dots\rho_sv_s$ в источнике G. Пусть π' — простой путь (возможно, пустой), ведущий от v_s к некоторой финальной вершине v_f. Если $v_f=v_0$, то доказательство того, что $R_1(\pi)<R$, $R_2(\pi)<R$ дословно воспроизводит рассуждения при рассмотрении источников из M; при $v_f\neq v_0$ эти рассуждения сохраняются с очевидными изменениями.

(2). Сначала пусть $R=\mathbf{A}(G)=\langle P\rangle$. Если $R'=e$ либо $R_1=\langle P\rangle=$ $=R$, то в качестве π достаточно выбрать пустой путь. Поэтому пусть $R'=\langle P\rangle S$, где $S\neq e$. Покажем, что существует путь π, принадлежащий источнику G, такой, что R' есть либо $R_1(\pi)$, либо $R_2(\pi)$. Выражение P представимо в виде $P=P_1\vee\dots\vee P_k$ $(k\geqslant 1)$, причем для каждого P_i в источнике G существует простой цикл $\pi_i=v_0\rho_{i1}v_{i1}\dots\rho_{il}v_{il}$, такой, что $P_i=a_{i1}R_1a_{i2}R_2\dots R_{l-1}a_{il}$, где $[\pi_i]=$ $=a_{i1}\dots a_{il}$, $R_j=\mathbf{A}(G^{v_j}_{v_0v_1\dots v_{j-1}})$ $(1\leqslant j\leqslant l-1)$. Так как $S\neq e$ и для любого подходящего i имеем $S<P_i$, то $S=a_{i1}R_1a_{i2}R_2\dots a_{im}S'$, где $m\geqslant 1$, $S'<R_m$. По предположению индукции, для ветви S' выражения $R_m=\mathbf{A}(G^{v_m}_{v_0v_1\dots v_{m-1}})$ в источнике $G^{v_m}_{v_0v_1\dots v_{m-1}}$ существует полупростой путь $\tilde{\pi}$, такой, что S' есть либо $R_1(\tilde{\pi})$, либо $R_2(\tilde{\pi})$. Обозначим $\pi'=v_0\rho_{i1}v_{i1}\dots\rho_{im}v_{im}$; тогда легко видеть, что искомый путь π есть $\pi'\tilde{\pi}$.

Пусть теперь $R=\mathbf{A}(G)=P_1\vee\dots\vee P_r$ $(r\geqslant 1)$, $R'<R$. Тогда для некоторого i $(1\leqslant i\leqslant r)$ имеем $R'<P_i$, и доказательство существования полупростого пути π, $\pi\in G$, такого, что R есть либо $R_1(\pi)$,

либо $R_2(\pi)$, совершенно аналогично проведенному в рассмотренном выше случае. Лемма доказана.

Доказательство теоремы 3.5.

1°. Пусть регулярное выражение R удовлетворяет условиям 1) и 2) теоремы, так что $R=R_1\vee\ldots\vee R_l$ $(l\geqslant 1)$, где каждое R_i $(1\leqslant i\leqslant l)$ есть член 1-го типа. Без ограничения общности можно считать, что при $i<j$ либо $R_j\perp R_i$, либо $R_j<R_i$. Тогда для R строится источник G аналогично тому, как это делалось для выражения (1) в лемме 3.9.

2°. Пусть $R\in\tilde{R}$. Покажем, что R удовлетворяет условиям 1) и 2) теоремы. Для выражения $R=\mathbf{A}(G)$ предположим, что G принадлежит множеству M источников специального вида. Пусть $G\in M$, $\|G\|=1$ (рис. 3.1). Тогда, очевидно, $\mathbf{A}(G)=\langle a_{i1}\vee\ldots\vee a_{ir}\rangle$, причем $\mathbf{A}(G)$ удовлетворяет условиям 1) и 2).

Пусть любое регулярное выражение $R\in\tilde{R}$; $R=A(G)$; $G\in M$ $\|M\|\leqslant n$ удовлетворяет условиям 1) и 2). Пусть $R\in\tilde{R}$, $R=A(G)$, $G\in M$, $\|G\|=n+1$. Согласно способу $\mathbf{A}$ анализа источников, выражение $R=\mathrm{A}(G)$ имеет вид

$$R=\langle\bigvee_{\pi_i\in C}P(\pi_i)\rangle,$$

где C — множество всех простых циклов, проходящих через v_0, а $P(\pi_i)$ — регулярное выражение, соответствующее циклу π_i.

Выражение R является членом и ветвью самого себя, причем членом 1-го типа, и поэтому удовлетворяет условию 1) теоремы.

Покажем, что каждый член выражения $\bigvee\limits_{\pi_i\in C}P(\pi_i)$ есть член 2-го типа. Возьмем произвольное $P(\pi_i)$, которое можно записать в виде

$$P(\pi_i)=a_1R_1a_2R_2\ldots a_{k-1}R_ka_k\quad(k\geqslant 1),$$

где $[\pi_i]=a_1\ldots a_k$.

Пусть $R_j=\langle Q_j\rangle$ $(1\leqslant j\leqslant k)$. Рассмотрим выражение $K=a_{j+1}R_{j+1}\ldots R_ka_k$ и покажем, что $K\perp Q_j$, т. е. что оно имеет вид LaM, где $La\nless Q_j$, но существует b такое, что $Lb<Q_j$. Пусть π_i' — отрезок пути π_i от вершины v_j до такой вершины v_{j+s} в источнике $G^{v_j}_{v_0v_1\ldots v_{j-1}}$, в которой π_i впервые выходит из $G^{v_j}_{v_0v_1\ldots v_{j-1}}$. Тогда, в силу леммы 3.10, $R_2(\pi_i')=\langle Q_j\rangle\,a_{j+1}R_{j+1}\ldots a_{j+s}R_{j+s}<\langle Q_j\rangle$. Согласно определению, ветви регулярного выражения $a_{j+1}R_{j+1}\ldots\ldots a_{j+s}R_{j+s}<Q_j$. Пусть $L=a_{j+1}R_{j+1}\ldots a_{j+s}R_{j+s}$, тогда $K=La_{j+s+1}M$. Предположим, что $La_{j+s+1}<Q_j$, тогда $\langle Q_j\rangle La_{j+s+1}<\langle Q_j\rangle$ и по лемме 3.10 существует полупростой путь $\tilde{\pi}$ в $G^{v_j}_{v_0v_1\ldots v_{j-1}}$, такой, что $\langle Q_j\rangle La_{j+s+1}$ есть либо $R_1(\tilde{\pi})$, либо $R_2(\tilde{\pi})$. Легко заметить, что слово $[\tilde{\pi}]$, соответствующее пути $\tilde{\pi}$, есть кратчайшее слово, входящее в $|R_q(\pi)|$ $(q=1,\ 2)$. Но кратчайшее слово в $|\langle Q_j\rangle La_{j+s+1}|$ есть $a_{j+1}a_{j+2}\ldots a_{j+s+1}$, в то время как путь, соответствующий этому слову, выходит из источника $G^{v_j}_{v_1v_1\ldots v_{j-1}}$. Получено противоречие.

С другой стороны, из вершины v_{j+s} в источнике $G^{v_j}_{v_0 v_1 \dots v_{j-1}}$ выходит хотя бы одно ребро, так как из v_{j+s} достижимо v_j и источник $G^{v_j}_{v_0 v_1 \dots v_{j-1}}$ невырожденный. Взяв любое такое ребро ρ, и рассмотрев путь $\pi'_i\rho$ (полупростой в силу простоты пути π'_i), получаем, что $R_1(\pi'_i\rho) = \langle Q_j \rangle Lb < \langle Q_j \rangle$, где b — отметка ребра ρ, откуда и вытекает $Lb < Q_j$. Таким образом, мы показали, что любой член выражения $\bigvee\limits_{\pi_i \in C} P(\pi_i)$ есть член 2-го типа.

Пусть $P_1 = P(\pi_1)$ и $P_2 = P(\pi_2)$ — любые члены выражения $\bigvee\limits_{\pi_i \in C} P(\pi_i)$, соответствующие путям π_1 и π_2, $\pi_1 \neq \pi_2$. Покажем, что P_1 отделимо от P_2, т. е., что P_2 представимо в виде LaM, где $La \nless P_1$, но имеется буква b, такая, что $Lb < P_1$. Так как P_1 — член 2-го типа, то его можно представить в виде $P_1 = \widetilde{P}_0^{(1)} \langle \widetilde{Q}_1^{(1)} \rangle L_1^{(1)} \widetilde{P}_1^{(1)} \dots \langle \widetilde{Q}_{k_1}^{(1)} \rangle L_{k_1}^{(1)} \widetilde{P}_{k_1}^{(1)}$, где $\widetilde{P}_i^{(1)} = a_i^{(0)} a_i^{(1)} \dots a_i^{(s_i)}$ $(0 \leqslant i \leqslant k_1)$ — непустое слово; $L_i^{(1)} < \widetilde{Q}_i^{(1)}$, причем $L_i^{(1)} a_i^{(0)} \nless \widetilde{Q}_i^{(1)}$. Тогда в π_1 выделяется последовательность вершин $v_{i_1}, \dots, v_{i_{k_1}}$, таких, что $\langle Q_j^{(1)} \rangle = R_j = \mathbf{A}(G_j), G_j = G^{v_{i_j}}_{v_0 v_1 \dots v_{i_j - 1}}$, и в источнике G для пути π_1 выделяем некоторый источник G^* вида, изображенного на рис. 3.8. Пусть $\widetilde{G}$ — источник, получающийся из G^* удалением ребра с отметкой $a_{k_1}^{(s_{k_1})}$, ведущего к вершине v_0, и проведением этого ребра к новой вершине v_0'.

Аналогично тому, как это делали в лемме 3.9 для выражения P_1, построим источник $\widetilde{G}'$, такой, что $\mathbf{A}(\widetilde{G}') = P_1$, причем $\widetilde{G}'$ обладает свойствами, которыми обладал источник $\mathfrak{A}_1$ в лемме 3.9.

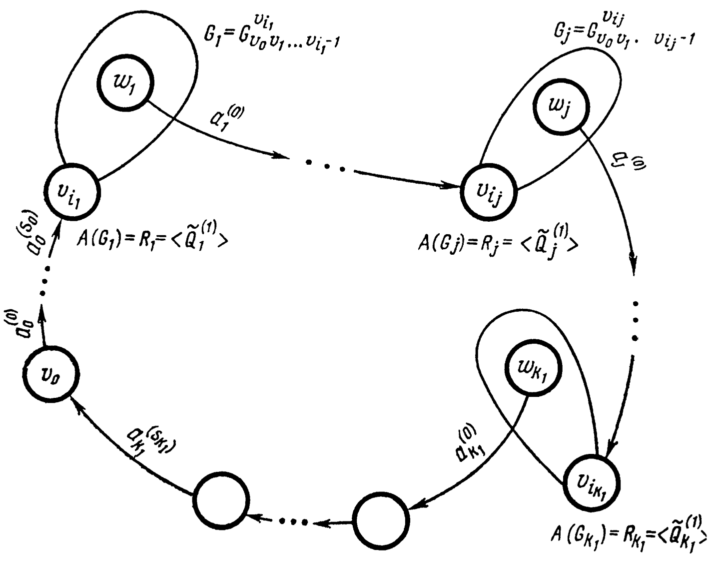

Рис. 3.8.

Пусть π_2' — отрезок пути π_2 в источнике G до некоторой вершины v, в которой впервые π_2 и π_1 расходятся. Тогда, очевидно, возможны два случая:

(а) Вершина v лежит в $\tilde{G}$ на цепочке ребер, соединяющей G_j с G_{j+1}. Тогда в $\tilde{G}'$ пути π_2' соответствует путь π_2'', такой, что $R_2(\pi_2'') < P_2$, причем из вершины v' (соответствующей v в $\tilde{G}'$) не выходит ребро с отметкой a, где a — отметка ребра пути π_2, ведущего из v. Таким образом, $P_2 = R_2(\pi_2'')aM$, где $R_2(\pi_2'')a \not< P_1$, причем, очевидно, существует $b = a_j^{(t)}$ ($a_j^{(t)}$ — отметка ребра, выходящего из v), такое, что $R_2(\pi_2'')\, b < P_1$, т. е. P_2 отделимо от P_1.

(б) Вершина v лежит внутри источника G_j. Тогда рассмотрим отрезок π_2'' пути π_2 от вершины v_{i_j} до выхода пути π_2 из G_j. По лемме 3.4 $R_2(\pi_2'') < R_j$, т. е. в источнике $\tilde{G}_j'$ существует путь π_2''', ведущий от v_{i_j}' к некоторой вершине $\hat{v}$, такой, что $R_2(\pi'') = R_2(\pi''')$. Если $\widehat{\pi}_1$ — начало пути π_1 в источнике G от v_0 до v_{ij}, $\widehat{\pi}_2$ — начало пути π_1' (π_1' — путь в источнике $\tilde{G}'$, соответствующий π_1) от v_0' до v_{ij}', то $R_2(\widehat{\pi}_2, \pi_2''') = R_2(\widehat{\pi}_1, \pi_2'') < P_2$, причем $P_2 = R_2(\widehat{\pi}_1, \pi_2'')aM$, где a — отметка ребра, ведущего в π_2 от последней вершины π_2'', и можно заметить, что в $\tilde{G}'$ из вершины $\hat{v}$ не выходит ребро с отметкой a, т. е. $R_2(\widehat{\pi}_1, \pi_2)a = La$, $La \not< P_1$. В силу определения источника, вершина v_{ij} достижима из v, т. е. существует b, такое, что $Lb < P_1$. Таким образом, для $\langle P \rangle = R$ условие 2) теоремы доказано; если $\langle P \rangle$ — собственная часть R, то это условие справедливо по предположению индукции. Итак, при $G \in M$ выражение $\mathbf{A}(G)$ удовлетворяет условиям 1) и 2) теоремы.

Пусть теперь $R \in \tilde{R}$, $R = \mathbf{A}(G)$; G — любой источник с начальной вершиной v_0 и множеством F финальных вершин. Согласно способу $\mathbf{A}$ анализа источников, выражение $R = \mathbf{A}(G)$ имеет вид $\bigvee_{\pi_i \in C} R(\pi_i)$, где C — множество всех простых путей, ведущих из v_0 в некоторую вершину $v_f \in F$; $R(\pi_i)$ — регулярное выражение, соответствующее пути π_i. Рассуждая аналогично доказательству того, что члены выражения P, входящего в итерацию $\langle P \rangle$, суть члены 2-го типа, можно показать, что члены $R(\pi_i)$ суть члены 1-го типа. Применяя, далее (с очевидными изменениями), рассуждения, проведенные при доказательстве того, что любой член выражения P отделим от каждого другого члена P, можно показать, что член $R(\pi_i)$, $\pi_i \in G$, слабо отделим от любого другого члена выражения R. Таким образом, теорема полностью доказана.

Пусть G — источник над алфавитом A; $R = \mathbf{A}(G)$ — регулярное выражение, построенное способом $\mathbf{A}$ анализа источника G; $G' = S(\mathbf{A}(G))$ — источник, построенный способом S синтеза источников по выражению $R = \mathbf{A}(G)$. В связи с теоремой 3.5, дающей описание множества $\tilde{R}$, естественным образом возникают вопросы об описании множества источников, получающихся в результате применения алгоритма синтеза S В. М. Глушкова к выражениям из $\tilde{R}$, а также взаимосвязи источников G и $S(\mathbf{A}(G))$. Прежде чем привести теоремы, отвечающие на эти вопросы, докажем ряд вспомогательных утверждений о регулярных выражениях и источниках.

Лемма 3.11. Пусть R — регулярное выражение и p — слово. Тогда R_p пусто тогда и только тогда, когда p не есть начало никакого слова из $|R|$.

Доказательство. 1°. Пусть $p=a_1 \dots a_l$ — слово и $R_p \neq \varnothing$. Покажем, что p есть начало некоторого слова $w \in |R|$. В источнике $G=S(R)$ существует вершина v, для которой найдется путь π_1, ведущий из начальной вершины v_0 к вершине v, такой, что $[\pi_1]=$ $=a_1 \dots a_l$. В источнике G существует путь π_2, ведущий из вершины v в некоторую финальную вершину v_f. Пути π_2 соответствует слово q, т. е. $[\pi_2]=q$. Очевидно, слово $pq=w \in R$ и p есть его начало.

2°. Пусть p — начало некоторого слова $w \in |R|$. Слово w представимо в виде $w=p \cdot q$ (q, быть может, пусто). Тогда в источнике $G=S(R)$ существует вершина $v \neq v_0$, достижимая из начальной вершины по пути π, причем $[\pi]=p$. Так как вершина $v \neq v_0$ источника $G=S(R)$ является непустым подмножеством множества основных мест выражения R, то отсюда следует, что $R_p \neq \varnothing$. Лемма доказана.

Очевидны следующие леммы 3 12 и 3.13.

Лемма 3.12. Если P — часть регулярного выражения R и $\mathfrak{M}$ — нефинальное основное место выражения P, то для любой буквы a, $a \in A$, каждое место, a-следующее за $\mathfrak{M}$, принадлежит P.

Лемма 3.13. Если $\mathfrak{M}$ — нефинальное место регулярного выражения P, являющегося частью регулярного выражения R, то $\mathfrak{M}$ — нефинальное место выражения R.

Лемма 3.14. Пусть $R=P_1 \vee \dots \vee P_n$ — регулярное выражение и p — слово. Тогда

$$R_p = \bigcup_{i=1}^{n} (P_i)_p,$$

где $(P_i)_p$ — p-спектр выражения P_i.

Доказательство проведем индукцией по длине $d(p)$ слова p.

Если $d(p)=1$, то $p=a$ — буква. Из правила 1 о подчиненности мест за начальным местом регулярного выражения R e-следуют начальные места его членов P_i $(1 \leqslant i \leqslant n)$. Легко заметить, что множество мест e-следующих за начальным местом $\mathfrak{M}_{i0}$ выражения P_i состоит из некоторого подмножества множества неосновных мест P_i. Берем любой член P_i и рассматриваем $\widetilde{\mathfrak{M}}_i$ — множество его неосновных мест, e-следующих за начальным местом выражения R. В силу того, что R — дизъюнкция, конечному месту члена P_i $(1 \leqslant i \leqslant n)$ не подчинено начальное место ни одного члена P_j $(1 \leqslant j \leqslant n)$, $i \neq j$. Поэтому, если $\mu_i \in \widetilde{\mathfrak{M}}_i$, то каждое a-следующее за местом μ_i место в выражении R принадлежит члену P_i и очевидно, что

$$R_a = \bigcup_{i=1}^{n} (P_i)_a.$$

Предположим, что утверждение доказано для каждого слова p' длины $d(p')=l$, рассмотрим слово $p=p'a$ длины $l+1$; $a\in A$. По предположению индукции $R_{p'}=\bigcup\limits_{i=1}^{n}(P_i)_{p'}$. Берем любое место $\mu_i'\in(P_i)_{p'}$. Если оно нефинальное, то, в силу леммы 3.12 множество a-следующих за ним мест принадлежит P_i. Если μ_i' — финальное место члена P_i, то в силу того, что R — дизъюнкция, согласно правилам о подчиненности мест, a-следующие за ним места тоже принадлежат P_i. Поэтому для любого $\mu_i'\in(P_i)_{p_i'}$ каждое a-следующее за μ_i' место принадлежит члену P_i, а отсюда и вытекает, что $R_p=\bigcup\limits_{i=1}^{n}(P_i)_p$. Лемма доказана.

Лемма 3.15. Пусть $R=\langle P\rangle$ — регулярное выражение и p — слово. Если для любого начала p' слова p $(p'\neq p)$ $P_p{}'$ не содержит финальных мест P, то $R_p=P_p$.

Доказательство поведем индукцией по длине $d(p)$ слова p.

Если $d(p)=1$, то $p=a$ — буква. В силу правил 1, 2 и 3 о подчиненности мест регулярного выражения множество предосновных мест, e-следующих за начальным местом выражения R, совпадает с множеством предосновных мест, e-следующих за начальным местом выражения P. Так как по предположению леммы множество мест, e-следующих за начальным местом выражения P, не содержит финальных мест выражения P, то в силу леммы 3.12 $R_a=P_a$.

Предположим, что утверждение доказано для каждого слова p' длины $d(p')=l$. Рассмотрим слово $p'=pa$, $a\in A$, длины $d(p)=$ $=l+1$. По предположению индукции $R_{p'}=P_{p'}$, а по предположению леммы $P_{p'}$ не содержит финальных мест выражения P. Если $\mu'\in P_{p'}$, причем μ' не является финальным местом выражения P, то в силу леммы 3.12 каждое место μ, a-следующее за μ', принадлежит P, и, очевидным образом, $R_p=P_p$. Лемма доказана.

Лемма 3.16. Пусть π — непустой простой путь в источнике $G\in M$ и $R=\mathbf{A}(G)$. Тогда $R_{[\pi]}$ не содержит финальных мест.

Доказательство проведем индукцией по сложности n источника G.

Пусть $\|G\|=1$ (см. рис. 3.1). Тогда $\mathbf{A}(G)=\langle a_{i1}\vee\ldots\vee a_{ir}\rangle$. Источник G не содержит ни одного непустого простого пути π, и, очевидно, лемма верна.

Пусть для всех G, таких, что $\|G\|\leqslant n$, лемма уже доказана. Докажем, что она верна при $\|G\|=n+1$. Заметим сначала, что регулярное выражение $R=\mathbf{A}(G)$ имеет вид итерации, т. е.

$$R=\langle P_1\vee P_2\vee\ldots\vee P_m\rangle,\quad m\geqslant 1,$$

где P_i $(1\leqslant i\leqslant m)$ — член 2-го типа, соответствующий простому циклу π_i, проходящему через начальную вершину v_0. Если

$$\pi_i=v_0\rho_{i1}v_{i1}\ldots\rho_{is}v_{is}\rho_{i,s+1}v_0;\ [\pi_i]=a_{i1}\ldots a_{i,s+1};\ R_{ij}=A(G_{ij}),$$

$$G_{ij} = G^{v_{ij}}_{v_0 v_1 \dots v_{i,j-1}} \quad (1 \leqslant j \leqslant s),$$

то $P_i = a_{i1} R_{i1} a_{i2} R_{i2} \dots a_{is} R_{is} a_{i,\, s+1}$.

Возьмем любой непустой простой путь $\pi = v_0 \rho_1 v_1 \dots \rho_l v_l$ и слово $[\pi] = a_1 \dots a_l$. Определим $(P_i)_{[\pi]}$ для любого члена P_i дизъюнкции $P = P_1 \vee \dots \vee P_m$ и покажем, что $(P_i)_{[\pi]}$ не содержит финальных мест выражения P_i. Обозначим через $\tilde{\pi}_t = v_t \rho_{t+1} v_{t+1} \dots \rho_l v_l$ $(1 \leqslant t \leqslant l)$ конец пути π, начинающийся с вершины v_t, причем $[\tilde{\pi}_t] = a_t a_{t+1} \dots a_l$ — соответствующее слово, являющееся концом слова $[\pi]$.

Покажем, что

$$(*) \qquad (P_i)_{[\pi]} = \bigcup_{j=1}^{k} (R_{ij})_{[\tilde{\pi}_j]},$$

где $a_1 = a_{i1}, \dots, a_k = a_{ik}, \ a_{k+1} \neq a_{i\, k+1} \ (0 \leqslant k \leqslant l)$.

Если $d(\pi) = 1$, то утверждение очевидно. Предположим, что утверждение доказано для каждого простого пути π, $d(\pi) = l$, и рассмотрим путь π' длины $d(\pi') = l+1$. Представим π' в виде $\pi\rho$, где $d(\pi) = l$; ρ — ребро. Пусть $[\pi'] = a_1 \dots a_{l+1}$; $a_1 = a_{i1}, \dots, a_{k'} = a_{ik'}$, $a_{k'+1} \neq a_{i\, k'+1}$ $(1 \leqslant k' \leqslant l+1)$. Спектр $(P_i)_{[\pi']}$ состоит из всех основных мест, a_{l+1}-следующих за местами из $(P_i)_{[\pi]}$, причем по предположению индукции $(P_i)_{[\pi]} = \bigcup_{j=1}^{k} (R_{ij})_{[\tilde{\pi}_j]}$. Пусть $j < l$. Тогда путь $\bar{\pi}_j$ — непустой. Если этот путь не содержится в источнике G_{ij}, то слово $[\tilde{\pi}_j]$ не является началом никакого слова из $|R_{ij}|$, и по лемме 3.11 $(R_{ij})_{[\tilde{\pi}_j]} = \varnothing$, а тогда $(R_{ij})_{[\tilde{\pi}_j] a_{l+1}} = (R_{ij})_{[\tilde{\pi}'_j]} = \varnothing$. Если же путь $\bar{\pi}_j$ принадлежит источнику G_{ij}, то по предположению индукции (так как $\|G_{ij}\| < n$) $(R_{ij})_{[\tilde{\pi}_j]}$ не содержит финальных мест, и по лемме 3.12 множество основных мест, a_{l+1}-следующих за местами из $(R_{ij})_{[\tilde{\pi}_j]}$ в выражении P_i есть

$$(R_{ij})_{[\tilde{\pi}_j] a_{l+1}} = (R_{ij})_{[\tilde{\pi}'_j]}.$$

Пусть теперь $j = l$. Тогда $k = l$, $[\tilde{\pi}_j] = e$ и $(R_{ij})_{[\tilde{\pi}_j]}$ в выражении P_i есть основное место $\mathfrak{M}$, **следующее за буквой** a_{il}. Если $k = k'$, т. е. $a_{l+1} \neq a_{i\, l+1}$, то множество основных мест, a_{l+1}-следующих за местом $\mathfrak{M}$, есть $(R_{il})_{a_{i\,l+1}} = (R_{il})_{[\tilde{\pi}'_l]}$. Если же $k' = k+1$, т. е. $a_{l+1} = a_{i\, l+1}$, то это множество есть

$$(R_{il})_{[\tilde{\pi}'_l]} \cup (R_{i\, l+1})_{[\tilde{\pi}'_{l+1}]}.$$

Окончательно приходим к равенству

$$(P_i)_{[\pi']} = \bigcup_{j=1}^{k'} (R_{ij})_{[\tilde{\pi}'_j]},$$

что и завершает доказательство утверждения (*). Так как, очевидно, $k<s+1$, то из (*) вытекает, что спектр $(P_i)_{[\pi]}$ не содержит финальных мест выражения P_i. Используя леммы 3.13 и 3.14, получаем теперь, что $(R)_{[\pi]}=(\langle P_1\vee\ldots\vee P_m\rangle)_p$ тоже не содержит финальных мест. Лемма доказана.

Из доказательства леммы 3.16 нетрудно получить следствия.

Следствие 1. Если $\pi=v_0\rho_1v_1\ldots\rho_lv_l$ — полупростой путь в источнике G, $G\in M$; $[\pi]=a_1\ldots a_l$; $R=\mathbf{A}(G)=\langle P_1\vee\ldots\vee P_m\rangle$, где $m\geqslant 1$ и $P_i=a_{i1}R_{i1}\ldots a_{is}R_{is}a_{i\,s+1}$ соответствует простому циклу π_i $(1\leqslant i\leqslant m)$, проходящему через начальную вершину v_0, причем $[\pi_i]=a_{i1}\ldots a_{i\,s+1}$, $R_{ij}=\mathbf{A}(G_{ij})$, $G_{ij}=G^{v_{ij}}_{v_0v_{i1}\quad v_{ij-1}}$ $(1\leqslant j\leqslant s)$, то

$$(R)_{[\pi]}=\bigcup_{j=1}^{m}(R_i)_{[\pi]},$$

причем

$$(P_i)_{[\pi]}=\bigcup_{j=1}^{k_i}(R_{ij})_{[\widetilde{\pi}_j]}\,,$$

где $a_1=a_{i1},\ \ldots,\ a_{k_i}=a_{ik_i},\ a_{k_i+1}\neq a_{ik_i+1}$ $(0\leqslant k_i\leqslant l)$.

Следствие 2. Если $\pi=v_0\rho_1v_1\ldots\rho_lv_l$ — полупростой путь в источнике G с начальной вершиной v_0 и множеством F финальных вершин, $[\pi]=a_1\ \ldots\ a_l$; $R=\mathbf{A}(G)=P_1\vee\ldots\vee P_r$ $(r\geqslant 1)$, где $P_i=R_{i0}a_{i1}R_{i1}\ldots$ $\ldots a_{is}R_{is}$ соответствует простому пути π_i, ведущему из вершины v_0 в некоторую вершину $v_f\in F$, причем $[\pi_i]=a_{i1}\ldots a_{is}$, $R_{i0}=A(G^{v_0})$, $R_{ij}=\mathbf{A}(G_{ij})$ $G_{ij}=G^{v_{ij}}_{v_0v_{i1}\quad v_{ij-1}}$ то

$$R_{[\pi]}=\bigcup_{j=1}^{r}(P_i)_{[\pi]},$$

причем

$$(P_i)_{[\pi]}=\bigcup_{j=1}^{k_i}(R_{ij})_{[\widetilde{\pi}_j1]},$$

где $a_1=a_{i1},\ \ldots,\ a_{k_i}=a_{ik_i},\ a_{k_i+1}\neq a_{i\,k_i+1}$ $(0\leqslant k_i\leqslant \min\,(l,\,s))$.

Лемма 3.17. Пусть G — источник, $R=\mathbf{A}(G)$, π_1 и π_2 — различные полупростые пути в G. Тогда $(R)_{[\pi_1]}\neq(R)_{[\pi_2]}$.

Доказательство проведем индукцией по сложности источника G. Если $G\in M$ и $\|G\|=1$ (см. рис. 3.1), то $\mathbf{A}(G)=\langle a_{i1}\vee\ldots\vee a_{ik}\rangle$, $[\pi_1]=a_{ij}$, $a_{il}=[\pi_2]$ $(j\neq l;\ 1\leqslant j,\ l\leqslant k)$, $\pi_1\neq\pi_2$, и, очевидно, утверждение верно.

Предположим, что лемма доказана для любого источника $G\in M$, $\|G\|\leqslant k$; рассмотрим источник $G\in M$, $\|G\|=k+1$. Тогда $R=\mathbf{A}(G)=\langle P_1\vee\ldots\vee P_m\rangle$, $m\geqslant 1$, $P_i=a_{i1}R_{i1}\ldots a_{is}R_{is}a_{i\,s+1}$ — член 2-го типа, соответствующий простому циклу $\pi_i=v_0\rho_{i1}v_{i1}\ldots\rho_{is}v_{is}\rho_{i\,s+1}$, $[\pi_i]=a_{i1}\ldots a_{i\,s+1}$. Пусть $\pi_1=v_0\rho^{(1)}_1v^{(1)}_1\ldots\rho^{(1)}_{l_1}v^{(1)}_{l_1}$ — любой полупростой путь, принадлежащий источнику G, $[\pi_1]=a^{(1)}_1\ldots a^{(1)}_{l_1}$. В силу определения источника, существует простой путь π_1', ведущий от $v_{l_1}^{(1)}$ в начальную вершину v_0. Пусть k — максимальное, такое, что вершины $v_1^{(1)}, \dots, v_{k-1}^{(1)}$ не принадлежат π_1'. Очевидно, что путь $\tilde{\pi}_k^{(1)} = v_k^{(1)}\rho_{k+1}^{(1)} \dots \rho_{l_1}^{(1)} v_{l_1}^{(1)}$ принадлежит источнику G_k. Обозначим конец пути π_1', ведущий от $v_k^{(1)}$ к v_0, через $\overset{*}{\pi_1}$, а начало пути π_1, ведущее от v_0 к $v_k^{(1)}$ через $\overset{**}{\pi_1}$. Тогда $\overset{**}{\pi_1}\overset{*}{\pi_1} = \Pi$ — простой цикл; пусть P_i — соответствующий ему член выражения P.

Возьмем любой принадлежащий G полупростой путь $\pi_2 \neq \pi_1$, $\pi_2 = v_0\rho_1^{(2)}v_1^{(2)} \dots \rho_{l_2}^{(2)}v_{l_2}^{(2)}$, $[\pi_2] = a_1^{(2)} \dots a_{l_2}^{(2)}$. Покажем, что $(P_i)_{[\pi_1]} \neq (P_i)_{[\pi_2]}$. Член P_i выражения P можем представить в виде

$$P_i = b_1R_{i1}b_2R_{i2} \dots b_kR_{ik}b_{k+1} \dots b_sR_{is}b_{s+1}.$$

Предположим, что путь π_1 совпадает с циклом Π до некоторой вершины $v_{t'}'$, т. е. что $b_1 = a_1^{(1)}, \dots, b_{t'} = a_{t'}^{(1)}$, $b_{t'+1} \neq a_{t'+1}^{(1)}$; что путь π_2 совпадает с циклом Π до некоторой вершины v_t, т. е. что $b_1 = a_1^{(2)}, \dots, b_t = a_t^{(2)}$, $b_{t+1} \neq a_{t+1}^{(2)}$. Пусть сначала $0 \leqslant t < k$. В силу следствия 1

$$(P_i)_{[\pi_1]} = \bigcup_{j=1}^{t'} (R_{ij})_{[\tilde{\pi}_j^{(1)}]},$$

$[\tilde{\pi}_j^{(1)}] = a_j^{(1)}a_{j+1}^{(1)} \dots a_{l_1}^{(1)}$, причем из леммы 3.11 вытекает, что $(R_{ik})_{[\tilde{\pi}_k^{(1)}]} \neq \varnothing$. Но

$$(P_i)_{[\pi_2]} = \bigcup_{j=1}^{t} (R_{ij})_{[\tilde{\pi}_j^{(2)}]},$$

$[\tilde{\pi}_j^{(2)}] = a_j^{(2)}a_{j+1}^{(2)} \dots a_{l_2}^{(2)}$, и, очевидно, $(P_i)_{[\pi_1]} \neq (P_i)_{[\pi_2]}$.

Предположим теперь, что $t \geqslant k$. Если $\tilde{\pi}_k^{(2)}$ не принадлежит источнику G_{ik}, то $(R_{ik})_{[\tilde{\pi}_k^{(2)}]} = \varnothing$, и так как $(R_{ik})_{[\tilde{\pi}_k^{(1)}]} = \varnothing$, то $(P_i)_{[\pi_1]} = (P_i)_{[\pi_2]}$. Пусть теперь $\tilde{\pi}_k^{(2)}$ принадлежит источнику G_{ik}. Тогда, в силу предположения индукции, $(R_{ik})_{[\tilde{\pi}_k^{(2)}]} \neq (R_{ik})_{[\tilde{\pi}_k^{(1)}]}$ и снова получаем, что $(P_i)_{[\pi_1]} \neq (P_i)_{[\pi_2]}$.

Таким образом, мы показали, что $(P_i)_{[\pi_1]} \neq (P_i)_{[\pi_2]}$, из чего, в силу следствия 1, получаем непосредственно, что $(R)_{[\pi_1]} \neq (R)_{[\pi_2]}$, если $G \in M$.

Если теперь G — произвольный источник, $\|G\| = k+1$, то рассуждая аналогично и используя следствие 2, получаем, что $(R)_{[\pi_1]} \neq (R)_{[\pi_2]}$. Лемма доказана.

Лемма 3.18. Пусть источник $G \in M$, $R = \mathrm{A}(G)$; p — слово, такое, что для любого его начала $p' \neq p$. $R_{p'}$ не содержит ни одного финального места выражения R. Тогда, если в R_p имеется хотя бы одно финальное место выражения R, то все места в R_p финальные.

Доказательство. Согласно способу $\mathbf{A}$ анализа источников, выражение $R=\mathbf{A}(G)$ имеет вид $R=\langle P_1 \vee \dots \vee P_n \rangle$, где P_i — член 2-го типа, который соответствует простому циклу π_i $(1 \leqslant i \leqslant n)$, проходящему через начальную вершину v_0. Обозначим $P=P_1 \vee \dots \vee P_n$ На основании леммы 3.15 имеем $R_p=(P_1 \vee \dots \vee P_n)_p=P_p$. Используя способ, описанный в лемме 3.9, для выражения P построим источник G', такой, что $P=A(G')$, причем из финальных вершин G' не выходят ребра. Если в R_p имеется финальное место, то $p \in |P|$, так что в G' существует путь π', такой, что $[\pi']=p$, ведущий из начальной вершины v_0' к некоторой финальной вершине v_f'. Так как из вершины v_f' не выходят ребра, то p не является собственным началом никакого слова из $|P|$. Предположим, что в R_p имеется нефинальное место $\mathfrak{M}$. Тогда в силу леммы 3.6 найдется непустое слово p', такое, что множество мест p'-следующих за $\mathfrak{M}$, содержит финальное место. Но тогда $(P)_{pp'}$ содержит это финальное место, и $pp' \in |P|$, что противоречит отсутствию в $|P|$ слов с собственным началом p. Лемма доказана.

Лемма 3.19. Пусть G — источник, $R=\mathbf{A}(G)$; π — полупростой путь в G; ρ — ребро, выходящее из последней вершины пути π. Тогда

$$(R)_{[\pi][\rho]}=(R)_{[\overline{\pi\rho}]},$$

где $\overline{\pi\rho}$ — приведенный путь пути $\pi\rho$.

Доказательство. (А) Предположим, что путь $\pi=v_0\rho_1v_1 \dots v_{l-1}\rho_lv_l$ простой. Тогда добавлением ребра ρ, выходящего из вершины $v_l \neq v_i$ $(0 \leqslant i \leqslant l-1)$ и ведущего в некоторую вершину v, получаем путь $\pi\rho$, являющийся полупростым путем. Из определения приведенного пути имеем $\overline{\pi\rho}=\pi\rho$, и поэтому $(R)_{[\overline{\pi\rho}]}=(R)_{[\pi][\rho]}=(R)_{[\pi][\rho]}$.

(Б) Пусть полупростой путь $\pi=v_0\rho_1v_1 \dots v_{l-1}\rho_lv_l$ таков, что $v_l \neq v_t$ $(0 \leqslant t \leqslant l-1)$. Тогда доказательство утверждения поведем индукцией по сложности источника G. Пусть $G \in M$, $\|G\|=1$. Тогда $R=\mathbf{A}(G)=\langle a_{i1} \vee \dots \vee a_{ir} \rangle$, причем буква a_{ij} $(1 \leqslant j \leqslant r)$ является отметкой ребра ρ_{ij} петли $v_0\rho_{ij}v_0$. Любой непустой полупростой путь π имеет вид $v_0\rho_{ij}v_0$; $[\pi]=a_{ij}$. Очевидно, что если $\rho=\rho_{ik}$ $(1 \leqslant k \leqslant r)$ — ребро, выходящее из последней вершины v_l пути π, то $\overline{\pi\rho}=v_0\rho_{ik}v_0$; $[\overline{\pi\rho}]=a_{ik}$, причем $(R)_{[\overline{\pi\rho}]}=\mathfrak{M}_{a_{ik}}$, где $\mathfrak{M}_{a_{ik}}$ — основное место, следующее за буквой a_{ik}. Так как $(R)_{[\pi]}=\mathfrak{M}_{a_{ij}}$, где $\mathfrak{M}_{a_{ij}}$ — основное место, следующее за буквой a_{ij}, то, в силу правил 2, 3 и 5 о подчиненности мест, множество a_{ik}-следующих за местом $\mathfrak{M}_{a_{ij}}$ мест, состоит из одного места $\mathfrak{M}_{a_{ik}}$, т. е. $(R)_{[\pi][\rho]}=\mathfrak{M}_{a_{ik}}=R_{[\overline{\pi\rho}]}$, что и надо было доказать. Предположим, что утверждение доказано для любого источника G, $\|G\|=k$, $G \in M$; рассмотрим источник $G \in M$, $\|G\|=k+1$. Пусть $\mathbf{A}(G)=R$; $\pi=v_0\rho_1v_1 \dots v_{l-1}\rho_lv_l$ — полупростой путь, причем $v_l=v_t$ $(0 \leqslant t \leqslant l-1)$, $[\pi]=a_1 \dots a_l$. Выражение R имеет вид $\langle P_1 \vee \dots \vee P_m \rangle$, где $P_i=a_{i1}R_{i1} \dots a_{is_i}R_{is_i}a_{is_i+1}$ соответствует простому циклу $\pi_i=v_0\rho_{i1}v_{i1} \dots v_{is_i}\rho_{is_i+1}v_0$; $[\pi_i]=a_{i1} \dots$

$\ldots\ a_{is_i+1}$; $R_{ij}=\mathbf{A}(G_{ij})$; $G_{ij}=G^{v_{ij}}_{v_0 v_{i1}\ldots v_{ij-1}}$ $(1\leqslant j\leqslant s_i)$. На основании следствия 1 из леммы 3.16 имеем $(R)_{[\pi]}=\bigcup\limits_{i=1}^{n}(P_i)_{[\pi]}$; $(P_i)_{[\pi]}=$ $=\bigcup\limits_{j=1}^{k_i}(R_{ij})_{[\tilde{\pi}_j]}$.

Пусть ρ — ребро, выходящее из вершины v_t и ведущее к вершине v, $[\rho]=a$. Тогда $\overline{\pi\rho}=v_0\rho_1 v_1\ \ldots\ \rho_t v_t \rho v$, $\overline{[\pi\rho]}=a_1\ldots a_t a$, и снова, по следствию 1 леммы 3.16 имеем:

$$(R)_{[\overline{\pi\rho}]}=\bigcup_{i=1}^{m}(P_i)_{[\overline{\pi\rho}]},$$

(1)

$$(R_i)_{[\overline{\pi\rho}]}=\bigcup_{j=1}^{r_i}(R_{ij})_{[(\tilde{\overline{\pi\rho}})_j]}.$$

Если в $(R)_{[\pi]}$ нет финальных мест, то по леммам 3.14 и 3.15

(2) $$(R)_{[\pi]a}=\bigcup_{i=1}^{n}(P_i)_{[\pi]a}\ .$$

Если же такое место в $(R)_{[\pi]}$ есть, то все места (лемма 3.17) в $(R)_{[\pi]}$ — финальные места, причем π — простой цикл, и легко проверить, что

(3) $$(R)_{[\pi]a}\ \bigcup_{j=1}^{m}(P_i)_a=(R)_{[\rho]}=(R)_{[\overline{\pi\rho}]}.$$

Найдем множество основных мест, a-следующих за местами из $(P_i)_{[\pi]}$. Заметим прежде всего, что при $j<t$ путь $\tilde{\pi}_j$ не принадлежит источнику G_{ij}, так что $(R_{ij})_{[\tilde{\pi}_j]}=\varnothing$. Пусть при $j\leqslant t$ в $(R_{ij})_{[\tilde{\pi}_j]}$ нет финальных мест (выражения R_{ij}). Тогда по лемме 3.12 места, a-следующие (в выражении P_i) за местами из $(R_{ij})_{[\tilde{\pi}_j]}$, содержатся в R_{ij}, так что это множество мест есть $(R_{ij})_{[\tilde{\pi}_j]a}=(R_{ij})_{[(\widetilde{\pi\rho})_j]}$. Если $(\widetilde{\pi\rho})_j$ не принадлежит G_{ij}, то $(R_{ij})_{[(\widetilde{\pi\rho})_j]}=(R_{ij})_{[(\tilde{\overline{\pi\rho}})_j]}=\varnothing$. Если же $(\widetilde{\pi\rho})_j$ принадлежит G_{ij}, то равенство $(R_{ij})_{[(\widetilde{\pi\rho})_j]}=(R_{ij})_{[(\tilde{\overline{\pi\rho}})_j]}$ вытекает из предположения индукции. Пусть теперь $j\leqslant t$ и в $(R_{ij})_{[\tilde{\pi}_j]}$ имеются финальные места. Тогда по лемме 3.17 все места в $(R_{ij})_{[\tilde{\pi}_j]}$ — финальные и, в частности, получаем, что $[\tilde{\pi}_j]\in|R_{ij}|$, так что $\tilde{\pi}_j$ — простой цикл в источнике G_{ij}, и $j=t$. Если $a=a_{i\,t+1}$, то множество мест, a-следующих в выражении P_i за $(R_{ij})_{[\tilde{\pi}_j]}=(R_{it})_{[\tilde{\pi}_t]}$, есть $(R_{it})_a\cup(R_{i\,t+1})_e=$ $=(R_{it})_{[(\tilde{\overline{\pi\rho}})_t]}\cup(R_{i\,t+1})_{[(\tilde{\overline{\pi\rho}})_{t+1}]}$, $r_i=t+1$, и приходим к равенству $(P_i)_{[\overline{\pi\rho}]}=$

$= \bigcup_{j=1}^{r_i} (R_{ij})_{[\widetilde{(\pi\rho)}_j]} = \bigcup_{j=1}^{r+1} (R_{ij})_{[\widetilde{(\pi\rho)}_j]} = (P_i)_{[\pi]a}$. Если же $a \neq a_{i+1}$, то множество мест, a-следующих в выражении P_i за местами из $(R_{it})_{[\widetilde{\pi}_t]}$, есть $(R_{it})_a = (R_{it})_{[\widetilde{(\pi\rho)}_t]}$, $r_i = t$, и снова получаем $(P_i)_{[\pi]a} = (P_i)_{[\widetilde{\pi}_t]}$. Используя равенства (1), (2) и (3), окончательно получаем, что $(R)_{[\pi]a} = (R)_{[\overline{\pi\rho}]}$.

Предположим теперь, что G — произвольный источник с начальной вершиной v_0 и множеством F финальных вершин; π — полупростой путь в G, ρ — ребро, выходящее из последней вершины пути π. Тогда, рассуждая аналогично тому, как это делалось для источников специального вида, можно показать, что лемма верна.

Из последовательности доказанных выше лемм непосредственно вытекает следующая теорема.

Теорема 3.6 [15]. Пусть G — источник, $G' = S(\mathbf{A}(G))$. Тогда G' изоморфен источнику $\widetilde{G}$, определяемому по G следующим образом:

а) вершинами источника $\widetilde{G}$ служат полупростые пути источника G, причем начальной вершиной — пустой путь, а финальными вершинами — пути, ведущие к финальным вершинам источника G;

б) если π — полупростой путь в G, ведущий к вершине v, причем из вершины v выходит ребро ρ с отметкой a, то из вершины π источника $\widetilde{G}$ проводится ребро ρ к вершине $\overline{\pi\rho}$.

Способы $\mathbf{A}$ анализа источников и S синтеза источников назовем **согласованными** на некотором источнике G, если источник $S(\mathbf{A}(G))$ изоморфен источнику G.

Следующая теорема отвечает на вопрос о том, когда способы $\mathbf{A}$ анализа и S синтеза источников являются согласованными.

Теорема 3.7 [15]. Способы $\mathbf{A}$ анализа источников и S синтеза источников являются согласованными на источнике G тогда и только тогда, когда источник G — дерево с корнем в начальной вершине.

Доказательство. 1°. Пусть источник G — дерево. Тогда, в силу теоремы 3.6, по источнику G строим источник $\widetilde{G}$, изоморфный источнику $G' = S(\mathbf{A}(G))$. Но легко заметить, что источник $\widetilde{G}$ изоморфен источнику G, и отсюда следует, что G' изоморфен G.

2°. Предположим, что способ $\mathbf{A}$ анализа источников согласован со способом S синтеза источников на некотором источнике G, тогда если $r(G) = \frac{\|G'\|}{\|G\|}$, то $r(G) = 1$. Покажем, что G — дерево.

Предположим, что G — не дерево. Тогда в G существует хотя бы одна вершина v, являющаяся достижимой из начальной вершины различными полупростыми путями π_1 и π_2. Отсюда, в силу теоремы 3.6, вытекает, что $r(G) > 1$ — противоречие. Теорема доказана.

Теперь оценим усложнение $r(G) = \frac{\|G'\|}{\|G\|}$ источника $G' =$

$=S(\mathbf{A}(G))$ по сравнению с источником G. Имеет место следующая теорема.

Теорема 3.8 [15]. Пусть $r(n) = \max\limits_{\|G\|=n} r(G)$, $\tilde{r}(n) = \min\limits_{\|G\|=n} r(G)$.

Тогда

$$r(n) = \begin{cases} \dfrac{m^{n+1}-1}{n(m-1)}, & m > 1, \\ \dfrac{n+1}{n}, & m = 1, \end{cases}$$

$$\tilde{r}(n) = 1.$$

Доказательство. Равенство $\tilde{r}(n)=1$ непосредственно вытекает из доказательства теоремы 3.7.

Пусть G — источник с n вершинами, заданный в алфавите A. Если π — полупростой путь в G, то, как легко заметить, длина π не превосходит n. Поэтому число полупростых путей в G не превосходит числа слов длины, не большей чем n, в алфавите A, т. е. не превосходит величины $\dfrac{m^{n+1}-1}{m-1}$ при $m>1$ и величины $n+1$ при $m=1$ Учитывая теорему 3.6, получаем, что

$$r(n) \leqslant \begin{cases} \dfrac{m^{n+1}-1}{(m-1)n}, & m > 1, \\ \dfrac{n+1}{n}, & m = 1. \end{cases} \tag{3}$$

Рассмотрим источник G, изображенный на рис. 3.9, где v_0 — начальная и единственная финальная вершина. Заметим, что каж-

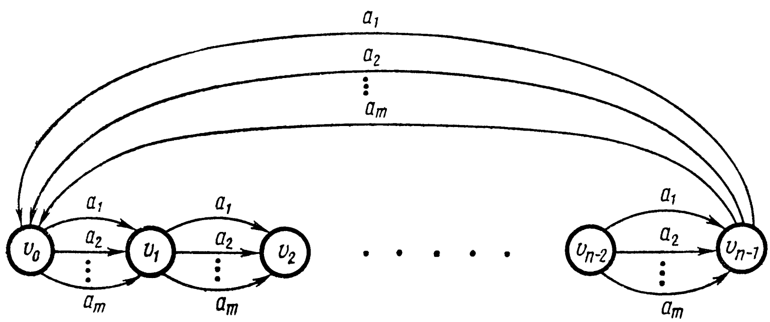

Рис. 3.9

дому слову p в алфавите A длины, не большей чем n, соответствует полупростой путь π в источнике G, такой, что $p=[\pi]$. Поэтому число полупростых путей равно $\dfrac{m^{n+1}-1}{m-1}$ при $m>1$ и $n+1$ при

$m=1$. Отсюда вытекает:

$$(3) \qquad r(n) \geqslant \begin{cases} \dfrac{m^{n+1}-1}{n(m-1)}, & m>1, \\ \dfrac{n+1}{n}, & m=1. \end{cases}$$

Из неравенств (2) и (3) вытекает равенство (1). Теорема доказана.

УПРАЖНЕНИЯ

1. Сколько различных ветвей имеет регулярное выражение
$$\langle a\langle b\rangle \vee b\rangle \vee a\langle b\rangle \vee ab?$$
2. Отделимо ли регулярное выражение $\langle a\langle b\rangle \vee c\rangle \quad a\langle b\rangle c\langle a\rangle$ от регулярного выражения $\langle a\langle b\rangle \vee c\rangle$?
3. Выяснить, какие из следующих регулярных выражений являются членами 1-го либо 2-го типа:
   1°. $a\langle a\vee c\langle ac\rangle ab\rangle c\langle ac\rangle$,
   2°. $b\langle a\vee cb\langle b\rangle c\rangle cb\langle b\rangle a$,
   3°. $ba\langle a\langle cab\rangle ac\vee ca\langle cb\rangle ca\rangle ca\langle cb\rangle ca$,
   4°. $\langle ab\vee ca\langle a\rangle b\rangle bc\langle bc\vee c\langle ab\rangle b\rangle\ ba$.
4. Выяснить, какие из следующих регулярных выражений принадлежат множеству $\tilde{R}$:
   1°. $\langle b\vee a\langle b\rangle a\langle b\rangle a\rangle \vee a\langle b\rangle$,
   2° $\langle a\vee b\langle b\rangle a\rangle b\langle b\rangle (b\vee a)$,
   3°. $\langle ab\vee \langle b\rangle ac\langle b\rangle b\rangle cb\langle ca\rangle c$,
   4°. $a\langle b\rangle\ \langle a\rangle b$.
5. Подсчитать число вершин источника $S(\mathbf{A}(G))$, где G — источник из упражнения 1 к § 2 гл. 3.
6. Представим ли в виде $S(\mathbf{A}(G))$ источник из упражнения 7 к § 1 гл. 3?

§ 4. МЕТРИЧЕСКИЕ ХАРАКТЕРИСТИКИ ОСНОВНЫХ АЛГОРИТМОВ АНАЛИЗА АВТОМАТОВ

Этот параграф посвящен метрическим характеристикам алгоритма **A** анализа автоматов, предложенного В. М. Глушковым, и алгоритма $\mathbf{A}_1$, представляющего собой некоторое видоизменение алгоритма **A**. Определим **сложность** $\|R\|$ регулярного выражения R в алфавите $A=\{a_1, ..., a_m\}$:

$$\|e\|=0;$$
$$\|a_i\|=1,\ a_i\in A;$$
$$\|\langle R\rangle\|=\|R\|+1;$$
$$\|(R_1\vee R_2)\|=\|(R_1\cdot R_2)\|=\|R_1\|+\|R_2\|+1.$$

Займемся теперь оценкой максимальной сложности регулярных выражений, принадлежащих множеству $\tilde{R}$ всех регулярных выражений, получающихся способом $\mathbf{A}$ анализа источников. Введем функцию Шеннона

$$L_{\mathbf{A}}(n) = \max_{\|G\|=n} \|\mathbf{A}(G)\|,$$

где G — источник, $\mathbf{A}(G)$ — регулярное выражение, принадлежащее $\tilde{R}$, и $\|\mathbf{A}(G)\|$ — сложность выражения $\mathbf{A}(G)$.

Нижняя и верхняя оценки величины $L_{\mathbf{A}}(n)$ даются в следующей теореме.

Теорема 3.9 [17]. Имеют место неравенства

$$2m^{\frac{n^2}{8}} \leqslant L_{\mathbf{A}}(n) \leqslant 4m^{\frac{n^2}{2}+\frac{5n}{2}} \quad (m>1).$$

Доказательство. Покажем, что верно

(1) $$L_{\mathbf{A}}(n) \leqslant 4m^{\frac{n^2}{2}+\frac{5n}{2}}.$$

Для этого сначала рассмотрим множество M источников специального вида. Если $G \in M$, $\|G\| = n$, то докажем, что

(2) $$\|\mathbf{A}(G)\| \leqslant 2m^{\frac{n^2}{2}+\frac{3n}{2}}.$$

Доказательство неравенства (2) поведем индукцией по сложности n источника G.

Пусть $\|G\| = 1$, $G \in M$. Тогда

$$\mathbf{A}(G) = \langle a_{i1} \vee \ldots \vee a_{ik} \rangle,$$

где a_{ij} $(1 \leqslant j \leqslant k)$ — буква, являющаяся отметкой ребра ρ_{ik} источника G. Источник G содержит не больше чем m петель, и, как легко заметить, $\|\mathbf{A}(G)\| \leqslant 2m$, откуда и вытекает неравенство (2) в случае $n = 1$.

Предположим, что неравенство (2) верно для любого источника $G \in M$, $\|G\| \leqslant n-1$. Покажем, что оно верно и для источников $G \in M$, $\|G\| \leqslant n$. Выражение $R = \mathbf{A}(G)$ имеет вид

(3) $$\langle P_1 \vee \ldots \vee P_r \rangle,$$

где P_i $(1 \leqslant i \leqslant r)$ — член 2-го типа, соответствующий простому циклу π_i, проходящему через начальную вершину v_0. Если π — простой цикл, проходящий через начальную вершину v_0 источника G, то, как легко заметить, длина π не превосходит n. Поэтому, так как каждое слово, определяющее простой цикл в G, можно дополнить до слова длины n, число простых циклов в G, проходящих через v_0, не превосходит числа слов длины n в алфавите A, т. е. не превосходит величины m^n. Отсюда вытекает, что число членов дизъюнкции $P = P_1 \vee \ldots \vee P_n$ не превосходит m^n. Член P_i можно представить в виде:

(4) $$a_{i1} R_{i1} a_{i2} R_{i2} \ldots a_{in_i-1} R_{in_i-1} a_{in_i},$$

где $n_i \leqslant n$, $a_{is} \in A$ $(1 \leqslant s \leqslant n_i - 1)$, $R_{is} = \mathbf{A}(G_{is})$, $G_{is} = G^{v_{is}}_{v_0 v_{i1} \cdot v_{i\,s-1}}$ — источник, уже определявшийся. Теперь оценим сверху сложность выражения P_i. Источник G_{is} содержит не больше чем $n-s$ вершин, и поэтому сложность выражения $R_{is} = \mathbf{A}(G_{is})$ не превосходит $L_{\mathbf{A}}(n-s)$. В выражении (4) имеется, как легко заметить, $2n_i - 2$ конъюнкций, между n_i буквами алфавита A и $n_i - 1$ выражениями R_{is}. Отсюда вытекает, что сложность выражения (4) не превосходит величины $3n - 2 + \sum\limits_{s=1}^{n-1} 2m^{\frac{(n-s)^2}{2} + \frac{3(n-s)}{2}}$. Так как выражение P содержит не больше чем m^n членов, то число операций дизъюнкции между этими членами не превосходит $m^n - 1$. Поэтому

$$\|\mathbf{A}(G)\| \leqslant m^n \left(3n - 2 + \sum_{s=1}^{n-1} 2m^{\frac{(n-s)^2}{2} + \frac{3(n-s)}{2}}\right) + m^n - 1 + 1,$$

т. е.

$$\|\mathbf{A}(G)\| \leqslant m^n (3n - 1 + 2m^{\frac{(n-1)^2}{2} + \frac{3(n-1)}{2}} + 2m^{\frac{(n-2)^2}{2} + \frac{3(n-2)}{2}} + \ldots$$

$$\ldots + 2m^{\frac{(n-i)^2}{2} + \frac{3(n-i)^2}{2}} + 2m^{\frac{(n-i+1)^2}{2} + \frac{3(n-i+1)}{2}} + \ldots + 2m^{\frac{1^2}{2} + \frac{3}{2}}) =$$

$$(5) \qquad = m^n \Bigg(3n - 1 + 2m^{\frac{(n-1)^2}{2} + \frac{3(n-1)}{2}} \Bigg(1 + \frac{1}{m^{\frac{2n-3}{2} + \frac{3}{2}}} +$$

$$+ \frac{1}{m^{\frac{4n-8}{2} + 2\frac{3}{2}}} + \ldots + \frac{1}{m^{\frac{2n(i-1)+1-i^2}{2} + \frac{3}{2}(i-1)}} +$$

$$+ \frac{1}{m^{\frac{2ni+1-(i+1)^2}{2} + \frac{3}{2}i}} + \ldots \Bigg)\Bigg).$$

Так как отношение i-го члена выражения

$$S(m, n) = 1 + \frac{1}{m^{\frac{2n-3}{2} + \frac{3}{2}}} + \frac{1}{m^{\frac{4n-8}{2} + 2\frac{3}{2}}} + \ldots + \frac{1}{m^{\frac{2n(i-1)+1-i^2}{2} + \frac{3}{2}(i-1)}} +$$

$$+ \frac{1}{m^{\frac{2ni+1-(i+1)^2}{2} + \frac{3}{2}i}} + \ldots + \frac{1}{m^{\frac{(n-1)^2}{2} + \frac{3(n-1)}{2} - 2}}$$

к $(i-1)$-му члену равно m^{i-n-1}, причем имеет наибольшее значение m^{-2} для $i = n-1$, то из свойств геометрической прогрессии вытекает, что $S(m, n) \leqslant \frac{m^2}{m^2 - 1}$. Отсюда получаем, что

$$\|\mathbf{A}(G)\| \leqslant m^n \left(3n - 1 + 2m^{\frac{(n-1)^2}{2} + \frac{3(n-1)}{2}} \cdot \frac{m^2}{m^2 - 1}\right) =$$

$$=m^n(3n-1)+\frac{2m}{m^2-1}\cdot m^{\frac{n^2}{2}+\frac{3n}{2}}=$$

$$=m^{\frac{n^2}{2}+\frac{3n}{2}}\left(\frac{3n-1}{m^{\frac{n^2}{2}+\frac{n}{2}}}+\frac{2m}{m^2-1}\right).$$

Но, как легко показать, для любых $m\geqslant 2$ и $n\geqslant 2$ будет $\frac{3n-1}{m^{\frac{n^2}{2}+\frac{n}{2}}}\leqslant$ $\leqslant\frac{2}{3}$ и $\frac{2m}{m^2-1}\leqslant\frac{4}{3}$, так что окончательно получаем

$$\|\mathbf{A}(G)\|\leqslant 2m^{\frac{n^2}{2}+\frac{3n}{2}},$$

что и надо было доказать.

Пусть теперь G — произвольный источник, $\|G\|=n$, с начальной вершиной v_0 и множеством F финальных вершин. Согласно способу **А** анализа источников выражение $R=\mathbf{A}(G)$ имеет вид

$$P_1\vee\ldots\vee P_k, \tag{6}$$

где P_i $(1\leqslant i\leqslant k)$ — член 1-го типа, соответствующий простому пути π_i, ведущему из начальной вершины v_0 в некоторую финальную вершину v_f, $[\pi_i]=a_{i1}a_{i2}\ldots a_{il}$, $l\leqslant n-1$. Как легко заметить, длина произвольного π_i не превосходит $n-1$. Поэтому число простых путей в G не превосходит числа слов длины, не большей чем $n-1$, в алфавите A, т. е. не превосходит величины $\frac{m^n-1}{m-1}$. Отсюда вытекает, что число членов дизъюнкции не превосходит $\frac{m^n-1}{m-1}$, а число операций дизъюнкции между этими членами также не превосходит $\frac{m^n-1}{m-1}$. Член P_i можно представить в виде

$$R_0a_{i1}R_{i1}a_{i2}R_{i2}\ldots a_{i\,n_i-1}R_{i\,n_i-1}, \tag{7}$$

где $n_i\leqslant n$, $a_{is}\in A$ $(1\leqslant s\leqslant n_i-1)$, $R_{is}=\mathbf{A}(G_{is})$, $G_{is}=G^{v_{is}}_{v_0v_{i1}\ldots v_{i\,s-1}}$, $R_0=\mathbf{A}(G_0)$, $G_0=G^{v_0}$. Теперь оценим сверху сложность выражения P_i. Каждый из источников G_{is}, а также источник G^{v_0} принадлежит множеству M источников специального вида, для которых уже показано, что $\|\mathbf{A}(G_{is})\|\leqslant 2m^{\frac{(n-s)^2}{2}+\frac{3(n-s)}{2}}$ $(0\leqslant s\leqslant n-1)$. В выражении (7) имеется, как легко заметить, $2n_i-2$ конъюнкций, причем в него входит n_i-1 букв алфавита A. Из сказанного выше вытекает, что сложность выражения (7) не превосходит величины

$$3n-3+\sum_{s=0}^{n-1}2m^{\frac{(n-s)^2}{2}+\frac{3(n-s)}{2}}.$$

В результате получаем

$$L_{\mathrm{A}}(n) \leqslant \frac{m^n-1}{m-1}\,(3n-2+2m^{\frac{n^2}{2}+\frac{3n}{2}}+2m^{\frac{(n-1)^2}{2}+\frac{3(n-1)}{2}}+\ldots$$

$$\ldots+2m^{\frac{1^2}{2}+\frac{3\,1}{2}}) \leqslant \frac{m^n-1}{m-1}\,(3(n+1)-1+2m^{\frac{n^2}{2}+\frac{3n}{2}}+$$

$$+2m^{\frac{(n-1)^2}{2}+\frac{3(n-1)}{2}}+\ldots+2m^{\frac{1^2}{2}+\frac{3\,1}{2}}) = \frac{m^n-1}{m-1}\cdot\frac{1}{m^{n+1}}\,m^{n+1}\,(3(n+1)-1+$$

$$+2m^{\frac{n^2}{2}+\frac{3n}{2}}+2m^{\frac{(n-1)^2}{2}+\frac{3(n-1)}{2}}+\ldots+2m^2) \leqslant$$

$$\text{(8)} \qquad \leqslant \frac{m^n-1}{m-1}\,2m^{\frac{(n+1)^2}{2}+\frac{3(n+1)}{2}-n-1} = \frac{m^n-1}{m-1}\,2m^{\frac{n^2}{2}+\frac{3n}{2}+1} \leqslant 4m^{\frac{n^2}{2}+\frac{5n}{2}},$$

что и надо было показать.

Теперь покажем, что

$$\text{(9)} \qquad L_{\mathrm{A}}(n) \geqslant 2m^{\frac{n^2}{8}}.$$

Рассмотрим источник G_l, заданный в основном алфавите A, с $n=2l$ ($l=1, 2, \ldots$) вершинами, изображенный на рис. 3.10, где v_0 — начальная и единственная финальная вершина. Число простых

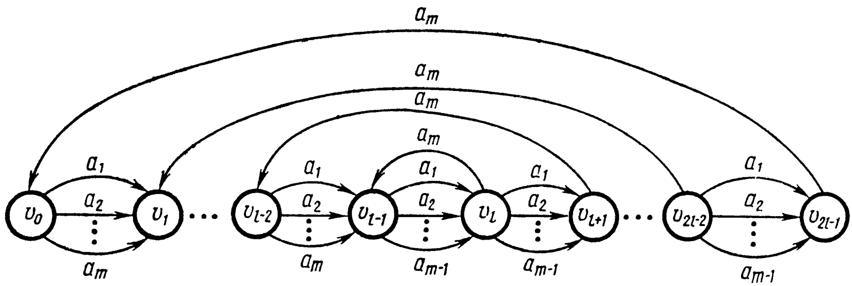

Рис 3.10.

циклов, проходящих через v_0, как легко заметить, равняется $m^l(m-1)^{l-1}$. Согласно способу **A** анализа источников, выражение $R_l=\mathrm{A}(G_l)$ имеет вид (3), где P_i представимо в виде

$$\text{(10)} \qquad a_{i1}\tilde{R}_{l-1}a_{i2}\tilde{R}_{l-2}\ldots a_{i\,l-1}\tilde{R}_1 a_{il}a_{i\,l+1}\,.\;\; a_{i\,2l-1}a_{2l},$$

причем $\tilde{R}_{l-j}=\mathrm{A}(G^{v_j}_{v_0v_1\ldots v_{j-1}})=R_{l-j}$. Если обозначить $\|R_l\|=A_l$, то будем иметь

$$\text{(11)} \qquad A_l=m^l(m-1)^{l-1}(5l-1+A_{l-1}+A_{l-2}+\ldots+A_1).$$

Доказательство неравенства (9) поведем индукцией отдельно для четных и нечетных n. При четном $n=2l$ оцениваем снизу сложность выражения $\mathbf{A}(G_l)$.

Если $n=2$, то $l=1$; $A_1=4m$ и $4m \geqslant 2m^{1/2}$, что и требовалось.

Предположим, что $\|\mathbf{A}_1(G_{l'})\| \geqslant 2m^{\frac{(2l')^2}{8}}$ для любого источника $G_{l'}$, $l'<l$. Покажем, что это неравенство верно и для источника G_l. В силу равенства (11) и предположения индукции надо показать, что

$$m^l (m-1)^{l-1} (5l-1+A_{l-1}+A_{l-2}+\ldots+A_1) \geqslant 2m^{\frac{l^2}{2}},$$

т. е.

$$m^l (m-1)^{l-1} (5l-1+2m^{\frac{1}{2}(l-1)^2}+2m^{\frac{1}{2}(l-2)^2}+\ldots+2m^{\frac{1}{2}}) \geqslant 2m^{\frac{l^2}{2}}.$$

Последнее неравенство верно, если

(12) $$m^l (m-1)^{l-1} 2m^{\frac{(l-1)^2}{2}} \geqslant 2m^{\frac{l^2}{2}}.$$

Неравенство (12), как нетрудно показать, можно привести к виду

$$m^{\frac{1}{2}+(l-1)\log_m(m-1)} \geqslant 1,$$

что эквивалентно неравенству $1/2+(l-1)\log_m(m-1) \geqslant 0$ и верно для любого $m \geqslant 2$. Таким образом, мы показали, что неравенство (9) верно для любого четного n.

Если n — нечетное, рассматриваем источник $\tilde{G}_l$, изображенный на рис. 3.11 и имеющий $2l+1$ вершину.

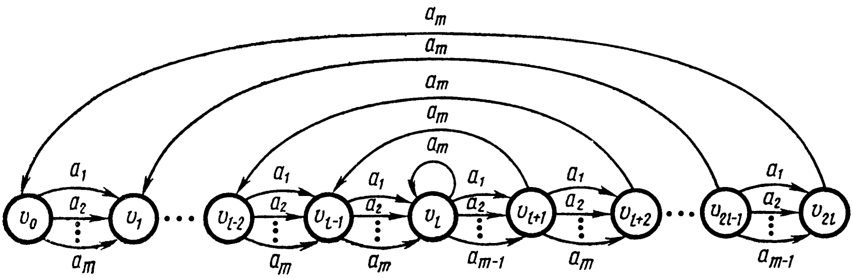

Рис 3.11.

Рассуждая аналогично тому, как это делали для $n=2l$, можно показать, что неравенство (9) верно. Теорема доказана.

Описанный в § 2 способ $\mathbf{A}_1$ анализа источников, как уже отмечено, представляет собой некоторую модификацию способа $\mathbf{A}$. Для алгоритма $\mathbf{A}_1$ анализа источников рассмотрим задачу, аналогичную задаче, рассматриваемой в предыдущей теореме. Пусть

G — источник, $R=\mathbf{A}_1(G)$ — регулярное выражение, построенное способом анализа источников и

$$L_{\mathbf{A}_1}(n)=\max_{\|G\|=n}\|\mathbf{A}_1(G)\|,$$

где max берется по всем источникам G сложности n. В следующей теореме даются верхняя и нижняя оценки функции $L_{\mathbf{A}_1}(n)$.

Теорема 3.10 [17]. Имеют место следующие неравенства

$$2m^n \leqslant L_{\mathbf{A}_1}(n) \leqslant 5m^{3n} \quad (m>1).$$

Доказательство. Сначала покажем, что

(1) $$L_{\mathbf{A}_1}(n) \leqslant 5m^{3n}.$$

Рассмотрим сначала множество M источников специального вида. Покажем, что если $\widetilde{L}_{\mathbf{A}_1}(n)=\max_{\substack{\|G\|=n,\\ G\in M}}\|\mathbf{A}_1(G)\|$, то

(2) $$\widetilde{L}_{\mathbf{A}_1}(n) \leqslant 3m^{3n}.$$

Доказательство неравенства (14) поведем индукцией по n.

Если $G\in M$, $\|G\|=1$, то легко показать, рассуждая аналогично тому, как это делалось в теореме 3.9, что неравенство (2) выполняется.

Предположим, что неравенство (2) верно для любого $k\leqslant n$. Рассмотрим источник $G\in M$, $\|G\|=n$. При помощи способа $\mathbf{A}_1$ анализа источников для множества $\mathfrak{M}$ слов, соответствующих простым циклам, проходящим через начальную вершину v_0 источника G, строим дерево $T(\mathfrak{M})$. Выражение $R=\mathbf{A}_1(G)$ имеет вид

(3) $$\langle R_{v_1}\vee\ldots\vee R_{v_{s_1}}\rangle,$$

где R_{v_i} $(1\leqslant i\leqslant s_1)$ — регулярное выражение, сопоставленное i-й вершине первого яруса дерева $T(\mathfrak{M})$ $(1\leqslant s_1\leqslant m)$;

$$R_{v_i}=a_i\mathbf{A}_1(G(\pi_{v_i}))(R_{w_1}\vee\ldots\vee R_{w_{s_2}}),$$

причем a_i — буква, являющаяся отметкой ребра дерева $T(\mathfrak{M})$, ведущего к вершине v_i; $\mathbf{A}_1(G(\pi_{v_i}))$— выражение, определенное для источника $G(\pi_{v_i})=G_{v_0}^{v_i}$; R_{w_j} $(1\leqslant j\leqslant s_2;\ 1\leqslant s_2\leqslant m)$ — регулярные выражения, сопоставленные вершинам 2-го яруса дерева $T(\mathfrak{M})$. Но выражение R_{w_j} представимо в том же самом виде, что и выражение R, причем теперь роль выражений R_{w_j} играют выражения, которые сопоставляем вершинам 3-го яруса дерева $T(\mathfrak{M})$ и т. д. Вообще, любое выражение, сопоставленное некоторой вершине J-го яруса $(1\leqslant J\leqslant n-1)$ имеет сложность не более чем $m+2+\widetilde{L}_{\mathbf{A}_1}(n-J)+mB$, где B — максимальная сложность выражений, сопоставленных $(J+1)$-му ярусу дерева $T(\mathfrak{M})$. Так как J-й ярус содержит не более m^J вершин, $1\leqslant J\leqslant n$, то, учитывая вид выражения (3), непосредственно получаем, что

$$\widetilde{L}_{\mathbf{A}_1}(n) \leqslant m + m(m+2+\widetilde{L}_{\mathbf{A}_1}(n-1)) + m^2(m+2+\widetilde{L}_{\mathbf{A}_1}(n-2)) + \ldots$$
$$\ldots + m^{n-1}(m+2+\widetilde{L}_{\mathbf{A}_1}(1)) + m^n,$$

т. е.

$$\widetilde{L}_{\mathbf{A}_1}(n) \leqslant m + m^n + m(m+2) + m^2(m+2) + \ldots + m^{n-1}(m+2) +$$
$$+ m\widetilde{L}_{\mathbf{A}_1}(n-1) + m^2\widetilde{L}_{\mathbf{A}_1}(n-2) + \ldots + m^{n-1}\widetilde{L}_{\mathbf{A}_1}(1). \qquad (4)$$

В силу предположения индукции, из рекуррентного неравенства (4) вытекает, что

$$\widetilde{L}_{\mathbf{A}_1}(n) \leqslant m + m^n + (m+2)m(1+m+\ldots+m^{n-2}) +$$
$$+ 3mm^{3(n-1)} + 3m^2m^{3(n-2)} + \ldots + 3m^{n-1}m^{3\cdot 1} \leqslant$$
$$\leqslant m(m+2)(1+m+m^2+\ldots+m^{n-1}) +$$
$$+ 3m^{3n-2}\left(1+\frac{1}{m^2}+\ldots+\frac{1}{m^{2i}}+\ldots+\frac{1}{m^{2(n-2)}}\right) \leqslant$$
$$\leqslant m(m+2)\frac{m^n-1}{m-1} + 3m^{3n-2}\cdot\frac{m^2}{m^2-1} \leqslant$$
$$\leqslant 3m^{3n}\left(\frac{1}{3}(m+2)\frac{m^n-1}{m^{3n-1}(m-1)} + \frac{1}{m^2-1}\right).$$

Но, как легко показать, для любых $m \geqslant 2$, $n \geqslant 2$ имеем: $\frac{1}{3}\cdot\frac{m+2}{m-1}\cdot\frac{m^n-1}{m^{3n-1}} \leqslant \frac{2}{3}$ и $\frac{1}{m^2-1} \leqslant \frac{1}{3}$, так что окончательно получаем неравенство (2).

Пусть теперь G — произвольный источник с начальной вершиной v_0 и множеством F финальных вершин, $\|G\| = n$. Как указано в описании способа $\mathbf{A}_1$ анализа источников, для множества $\mathfrak{M}$ слов, соответствующих простым путям в источнике G, ведущим из вершины v_0 в некоторую вершину из F, строим дерево $T(\mathfrak{M})$. Очевидно, при оценке $L_{\mathbf{A}_1}(n)$ сверху можно считать, что любая вершина источника G является финальной. Выражение $R = \mathbf{A}_1(G)$ тогда имеет вид

$$\mathbf{A}_1(G(\pi_{v_0}))(e \vee R_{v_1} \vee \ldots \vee R_{v_t}),$$

где $\mathbf{A}_1(G(\pi_{v_0}))$ — регулярное выражение, соответствующее источнику $G(\pi_{v_0})$, имеющее сложность не более чем $\widetilde{L}_{\mathbf{A}_1}(n)$; R_{v_i} $(1 \leqslant i \leqslant t;\ 1 \leqslant t \leqslant m)$ — регулярное выражение, сопоставленное i-й вершине первого яруса дерева $T(\mathfrak{M})$. Рассуждая совершенно аналогично тому, как это делали в случае источников из M, получаем неравенство:

$$L_{\mathbf{A}_1}(n) \leqslant m + 2 + \widetilde{L}_{\mathbf{A}_1}(n) + m(m+4+\widetilde{L}_{\mathbf{A}_1}(n-1)) + m^2(m+4+$$
$$+\widetilde{L}_{\mathbf{A}_1}(n-2)) + \ldots + m^{n-2}(m+4+\widetilde{L}_{\mathbf{A}_1}(2)) + m^{n-1}(2+\widetilde{L}_{\mathbf{A}_1}(1)),$$

т. е.

$$L_{A_1}(n) \leqslant m+2+2m^{n-1}+m(m+4)+m^2(m+4)+\ldots+m^{n-2}(m+4)+$$
$$+\widetilde{L}_{A_1}(n)+m\widetilde{L}_{A_1}(n-1)+m^2\widetilde{L}_{A_1}(n-2)+\ldots+m^{n-2}\widetilde{L}_{A_1}(2)+m^{n-1}\widetilde{L}_{A_1}(1).$$
(5)

Используя неравенство (2) для источников, принадлежащих M, из (5) получаем

$$L_{A_1}(n) \leqslant m(m+4)(1+m+m^2+\ldots+m^{n-2})+$$
$$+3m^{3n}\left(1+\frac{1}{m^2}+\frac{1}{m^4}+\ldots+\frac{1}{m^{2(n-1)}}\right) \leqslant$$
$$\leqslant m(m+4)\frac{m^{n-1}-1}{m-1}+3m^{3n}\frac{m^2}{m^2-1} \leqslant 6m^n+4m^{3n} \leqslant 5m^{3n}$$

при $m \geqslant 2$, $n \geqslant 2$, что и надо было показать.

Теперь покажем, что

(6) $$L_{A_1}(n) \geqslant 2m^n.$$

Рассмотрим источник G с n вершинами, изображенный на рис. 3.12, где v_0 — начальная и единственная финальная вершина.

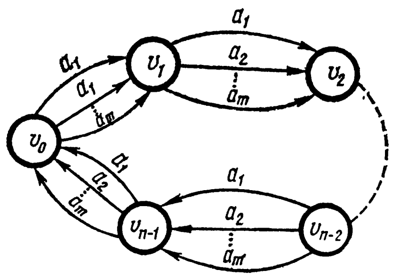

Рис. 3.12.

Согласно способу $\mathbf{A}_1$ анализа источников, для множества $\mathfrak{R}$ слов, соответствующих простым циклам в источнике G, проходящим через v_0, строим дерево $T(\mathfrak{R})$ высоты n. Из каждой вершины дерева $T(\mathfrak{R})$, не являющейся концевой, выходит ровно n ребер. i-й ярус дерева $T(\mathfrak{R})$ содержит m^i вершин, причем каждая из них при $i<n$ отмечена выражением вида

(7) $$a_i(R_1^{(i)} \vee R_2^{(i)} \vee \ldots \vee R_m^{(i)}),$$

где $R_j^{(i)}$ — регулярное выражение, сопоставленное некоторой вершине $(i+1)$-го яруса дерева $T(\mathfrak{R})$, в которую ведет ребро, выходящее из рассматриваемой вершины i-го яруса. Легко видеть, что сложность (7) равна $m+1+ml$, где $l=\|R_j^{(i)}\|$ $(1 \leqslant j \leqslant m)$. Учитывая, что выражение $R=\mathbf{A}_1(G)$ имеет вид итерации, получаем, обозначив $\|R\|=B_n$:

$$B_n = m(m+2)+m^2(m+1)+\ldots+m^{n-1}(m+1)+m^n=$$
$$=2m(1+m+m^2+\ldots+m^{n-1})=2m\frac{m^n-1}{m-1}.$$

Так как для любых $m \geqslant 2$, $n \geqslant 2$ имеет место $2m\frac{m^n-1}{m-1} \geqslant 2m^n$, то неравенство (6) верно. Теорема доказана.

Доказанное утверждение показывает, что величина $L_{A1}(n)$ существенно меньше, чем $L_A(n)$, т. е., что небольшое изменение алгоритма **A** приводит к алгоритму, дающему выражения гораздо меньшей сложности. В этом смысле можно сказать, что алгоритм **A**, предложенный В. М. Глушковым, неоптимальный.

Как известно [14], произвольное регулярное событие может быть представлено различными регулярными выражениями. Отсюда возникает задача представления его выражением минимальной сложности. Пусть $R(G)$ — регулярное выражение минимальной сложности, такое, что $|R(G)| = |G|$; обозначим

$$L(n) = \max_{\|G\|=n} \| R(G) \|.$$

Если $\mathfrak{A}$ — произвольный алгоритм анализа, то функция $L_{\mathfrak{A}}(n) = \max_{\|G\|=n} \|\mathfrak{A}(G)\|$, рассматриваемая в качестве меры эффективности алгоритма $\mathfrak{A}$, должна мажорировать функцию $L(n)$. Поведение функции $L(n)$ может быть охарактеризовано при помощи следующего утверждения.

Теорема 3.11 [17]. При $m \geqslant 2$ имеет место оценка

$$2[m/2]([n/2])^2 - 1 \leqslant L(n) \leqslant 5m^{3n}.$$

Доказательство. Верхняя оценка вытекает из предыдущей теоремы. Для получения нижней оценки разберем сначала случай $m=2$. Если n — четно $(n=2l)$, то рассматриваем источник G, указанный на рис. 3.13. У этого источника v_0 — начальная вершина, $\{v_f\}$ — множество финальных вершин.

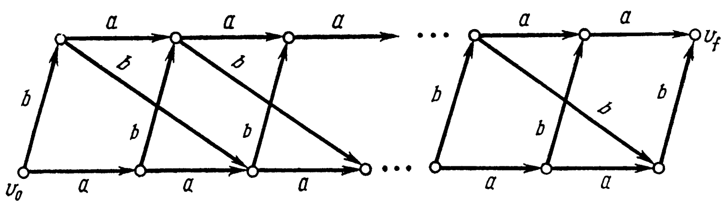

Рис. 3.13.

Пусть R — регулярное выражение, такое, что $|R| = |G|$, причем $\|R\|$ — минимально. Как нетрудно видеть, R обладает следующими свойствами:

1) В R нет символа итерации (если в R встречается выражение вида $\langle S \rangle$, где $|S| = \{e\}$, то это выражение можно было бы заменить на e, и сложность R при этом уменьшилась бы, что невозможно).

2) В $|R|$ входят все слова длины l в алфавите $\{a, b\}$, содержащие нечетное число букв b.

3) Для любого основного места m выражения R длина всех слов p, таких, что $m \in R_p$, одинакова.

В силу свойства 3), каждому основному месту m выражения можно сопоставить число N_m, равное длине слов p, таких, что $m \in R_p$.

Для оценки величины $\|R\|$ воспользуемся некоторыми результатами из алгебры логики. Пусть F — формула алгебры логики, получающаяся из R заменой каждого вхождения буквы b на символ переменной x_i, где $i \in N_m$ и m — основное место, расположенное после данного вхождения буквы b, и аналогичной заменой вхождений букв a на символы $\bar{x}_i$. Используя дистрибутивность конъюнкции относительно дизъюнкции, можно привести R к виду дизъюнкции слов; обозначим эту дизъюнкцию R'. При этом, как легко заметить, каждому члену $\alpha_1 \ldots \alpha_l$ выражения R' взаимно-однозначно соответствует член вида $x_1^{\sigma_1} \ldots x_l^{\sigma_l}$ формулы F', где $\sigma_i = 1$ при $\alpha_i = b$ и $\sigma_i = 0$ при $\alpha_i = a$. Таким образом, F' состоит из всевозможных членов вида $x_1^{\sigma_1} \ldots x_l^{\sigma_l}$, у которых в наборе $(\sigma_1, \ldots, \sigma_l)$ имеется нечетное число единиц, так что F' вместе с F определяет функцию алгебры логики $f(x_1, \ldots, x_l) = x_1 + \ldots$ $\ldots + x_l \pmod 2$. Согласно оценке, полученной В. М. Храпченко [18], формула F имеет не менее чем l^2 символов переменных. Таким образом, выражение R имеет не менее чем $l^2 - 1$ символов операций $\vee$, $\cdot$ и $\|R\| \geqslant 2l^2 - 1 = \frac{n^2}{2} - 1 = 2\left[\frac{n}{2}\right]^2 - 1$.

В случае нечетного n, $n = 2l+1$ достаточно рассмотреть источник G', указанный на рис. 3.14, у которого v_0 — начальная вершина, $\{v_f\}$ — множество финальных вершин.

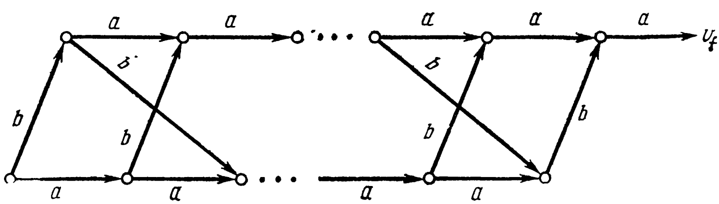

Рис. 3.14.

Если R' — регулярное выражение, такое, что $|R'| = |G'|$, причем $\|R'\|$ — минимально, то рассуждениями, аналогичными приведенным выше, устанавливается оценка $\|R'\| \geqslant 2l^2 - 1 =$ $= 2[n/2]^2 - 1$.

Пусть теперь $m > 2$, выделим в алфавите A символы $a_1, \ldots$ $\ldots, a_{[m/2]}$; $b_1, \ldots, b_{[m/2]}$. При четном n рассмотрим источник G^m, получающийся из источника G заменой каждого ребра с отметкой a на пучок параллельных ребер с отметками $a_1, \ldots, a_{[m/2]}$, а ребра с отметкой b — на пучок параллельных ребер с отметками $b_1, \ldots, b_{[m/2]}$. Если R^m — регулярное выражение, такое, что $|R^m| =$ $= |G^m|$, то для произвольного i, $i = 1, \ldots, [m/2]$ рассмотрим выражение $R^{m,i}$, полученное из R^m всевозможными заменами видов

$\alpha x \to \alpha$; $x \cdot \alpha \to \alpha$; $\alpha \vee x \to x$; $x \vee \alpha \to x$, где $\alpha \in \{a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{[m/2]}, b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_{[m/2]}\}$. Как легко заметить, $|R^{m,i}| = |G^i|$, где G^i — источник, полученный из G заменой символов a и b на a_i и b_i. Поэтому выражение $R^{m,i}$ имеет не менее l^2 вхождений символов a_i и b_i: выражение R^m — соответственно не менее $[m/2]\,l^2$ вхождений символов $a_1, \ldots, a_{[m/2]}, b_1, \ldots, b_{[m/2]}$ и $\|R^m\| \geqslant 2[m/2]\,l^2 - 1 = 2[m/2]\,[n/2]^2 - 1$. Случай нечетного n рассматривается аналогично. Теорема доказана.

УПРАЖНЕНИЯ

1. Источник G_n над алфавитом $\{0, 1\}$ имеет вершины $v_0, v_1, \ldots, v_{n-1}$. Из каждой вершины v_i $(i=0, 1, \ldots, n-1)$ выходит ребро с отметкой 0, ведущее к вершине v_{i+1} (при $i=n-1$ — к вершине v_{n-1}), а также ребро с отметкой 1, ведущее к вершине v_{i-1} (при $i=0$ — к вершине v_0). Начальная вершина источника G_n есть v_0; множество финальных вершин — $\{v_{n-1}\}$. Найти величины $L(\mathbf{A}(G_n))$, $L(\mathbf{A}_1(G_n))$.
2. Источник G_n над алфавитом $\{0, 1, 2, 3\}$ имеет множество вершин $\{v_{ij} : i=0, 1, \ldots, n-1;\ j=0, 1, \ldots, n-1\}$. Из каждой вершины v_{ij} выходят: ребро с отметкой 0, ведущее к вершине $v_{(i+1)(\mathrm{mod}\,n),j}$; ребро с отметкой 1, ведущее к вершине $v_{(i-1)(\mathrm{mod}\,n),j}$; ребро с отметкой 2, ведущее к вершине $v_{i,(j+1)(\mathrm{mod}\,n)}$, и ребро с отметкой 3, ведущее к вершине $v_{i,(j-1)(\mathrm{mod}\,n)}$. Начальная вершина источника G_n есть v_{00}; множество финальных вершин — $\{v_{n-1,n-1}\}$. Найти величины $L(\mathbf{A}(G_n))$ и $L(\mathbf{A}_1(G_n))$.
3. Пусть G_3 — источник из упражнения 1. Найти регулярное выражение R сложности не более чем 13, такое, что $|R| = |G_3|$.
4. Найти регулярное выражение наименьшей возможной сложности, определяющее то же событие, что и выражение: $(0^* \vee 10^*)^* \cdot (1 \vee 01)^* \cdot 1^*$.
5. В случае двухбуквенного алфавита найти величину $L(2)$.

§ 5. ЭФФЕКТИВНОСТЬ ОСНОВНЫХ АЛГОРИТМОВ АНАЛИЗА И СИНТЕЗА АВТОМАТОВ

При исследовании эффективности алгоритмов анализа автоматов естественно выделять такие классы источников, применение к которым исследуемого алгоритма дает только минимальные либо, наоборот, только не минимальные регулярные выражения. Аналогичный подход естественно применять при исследовании эффективности алгоритмов синтеза. В этом параграфе данный подход применяется к рассматривавшимся ранее алгоритму анализа **A** и улучшенному алгоритму синтеза

Обозначим K_n множество источников над алфавитом A, имеющих не более чем n вершин; K_n' — множество всех таких источников G из K_n', что регулярное выражение $A(G)$ минимально.

Посредством $|K|$ будем обозначать число источников в классе K.

Следующее утверждение показывает, что «почти всегда» регулярное выражение, построенное при помощи алгоритма **A**, не минимально.

Теорема 3.12 [16]. При $n\to\infty$

$$\frac{|K_n'|}{|K_n|}\to 0.$$

Доказательство. Конечный ориентированный граф H с выделенной вершиной v_0, каждому ребру которого сопоставлен символ алфавита A, назовем **предысточником**, если путем выделения в H некоторого множества $F\neq\varnothing$ можно получить источник с начальной вершиной v и множеством F финальных вершин.

Если H — предысточник, то множество всех источников, получающихся из H, обозначим $M(H)$.

Пусть H — предысточник, имеющий $k\geqslant 2m$ вершин. Оценим долю $p(H)$ источников $G\in M(H)$, таких, что $\mathbf{A}(G)$ — минимально. Если ни один из источников $G\in M(H)$ не дает минимального выражения $\mathbf{A}(G)$, то $p(H)=0$. Пусть $G\in M(H)$, причем $\mathbf{A}(G)$ — минимально. Рассмотрим множество F финальных вершин источника G; предположим, что $|F|>m$. Тогда, очевидно, найдутся два различных простых пути π_1 и π_2, ведущих от начальной вершины v_0 к различным финальным вершинам, начинающихся с одного и того же ребра. В этом случае, как нетрудно видеть, в выражении $\mathbf{A}(G)$ путям π_1 и π_2 соответствуют члены вида RR_1 и RR_2, где $R\neq e$, т. е. $\mathbf{A}(G)$ имеет вид $RR_1\vee RR_2\vee R_3$ и $\mathbf{A}(G)$ не минимально, так как выражение $R(R_1\vee R_2)\vee R_3$ имеет меньшую сложность. Поэтому $|F|\leqslant m$ и число различных источников G в $M(H)$, таких, что $\mathbf{A}(G)$ минимально, не превосходит величины

$$C_k^1+C_k^2+\ldots+C_k^m\leqslant mC_k^m\leqslant m\frac{k^m}{m!}\leqslant k^m.$$

Пусть, далее, $G\in M(H)$ и $\mathbf{A}(G)$ минимально, т. е. множество F финальных вершин источника G содержит не более чем m вершин. Рассматривая различные множества $F'\supseteq F$ финальных вершин, будем получать различные источники из $M(H)$; очевидно, число таких подмножеств F' не менее чем 2^{k-m}, т. е. $M(H)\geqslant 2^{k-m}$ и $p(H)\leqslant k^m/2^{k-m}$.

Рассмотрим теперь произвольное $\varepsilon>0$ и покажем, что существует такое $N(\varepsilon, m)$, что $\dfrac{|K_n'|}{|K_n|}<\varepsilon$ при $n>N(\varepsilon, m)$.

Выберем $N_1(\varepsilon, m)\geqslant 2m$ так, чтобы при $k\geqslant N_1(\varepsilon, m)$ выполнялось неравенство $k^m/2^{k-m}<\varepsilon/2$. Тогда для любого предысточника H, имеющего $k\geqslant N_1(\varepsilon, m)$ вершин, $p(H)<\varepsilon/2$. Следовательно, так как множество всех источников с k вершинами разбивается на попарно непересекающиеся подмножества вида $M(H)$, доля источников G с k вершинами, таких, что $\mathbf{A}(G)$ — минимально, при $k \geqslant N_1(\varepsilon, m)$ не превосходит $\varepsilon/2$. Ясно также, что доля источников G с минимальным $\mathbf{A}(G)$ среди всех источников, число вершин k которых удовлетворяет неравенствам $N_1(\varepsilon, m) \leqslant k \leqslant n$, меньше $\varepsilon/2$. Пусть $\mathbf{A}(x)$ — число источников, имеющих менее x вершин; $B(x, y)$ — число источников, имеющих не менее x и не более чем y вершин. Тогда, очевидно,

$$|K_n'| \leqslant \mathbf{A}(N_1(\varepsilon, m)) + \frac{\varepsilon}{2} B(N_1(\varepsilon, m), n),$$

$$|K_n| = \mathbf{A}(N_1(\varepsilon, m)) + B(N_1(\varepsilon, m), n),$$

т. е.

$$\frac{|K_n'|}{|K_n|} \leqslant \frac{\mathbf{A}(N_1(\varepsilon, m)) + \frac{\varepsilon}{2} B(N_1(\varepsilon, m), n)}{\mathbf{A}(N_1(\varepsilon, m)) + B(N_1(\varepsilon, m), n)}. \tag{27}$$

Нетрудно проверить, что $B(N_1(\varepsilon, m), n) \to \infty$ при $n \to \infty$, так что найдется такое $N(\varepsilon, m) \geqslant N_1(\varepsilon, m)$, что при $n > N(\varepsilon, m)$ правая часть неравенства (27) меньше ε. Теорема доказана.

Вместе с доказанным утверждением можно эффективно указать два бесконечных подкласса K_1 и K_2 источников, применение к которым алгоритма $\mathbf{A}$ дает, соответственно, только минимальные и только не минимальные выражения.

Пусть K_1 — класс источников вида, указанного на рис. 3.15, где $a_{ir_i} \neq a_{jr_j}$ при $i \neq j$, v_0 — начальная и v_f — финальная вершина. Пусть также K_2 — класс источников, имеющих более чем m финальных вершин (m — число букв алфавита A).

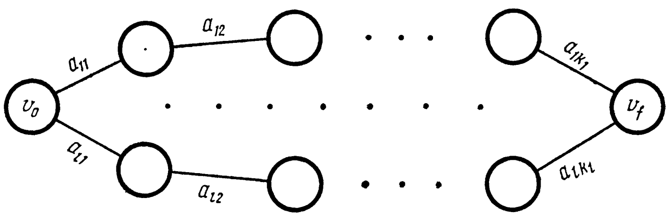

Рис. 3.15

Теорема 3.13 [16].

а) Для любого источника $G \in K_1$ выражение $\mathbf{A}(G)$ — минимально.

б) Для любого источника $G \in K_2$ выражение $\mathbf{A}(G)$ — не минимально.

Доказательство. Рассмотрим источник G вида, указанного на рис. 3.15, где $a_{ir_i} \neq a_{jr_j}$ при $i \neq j$. Каждый источник такого вида определяет выражения $\mathbf{A}(G)$, имеющее вид $R = \mathscr{P}_1 \vee \ldots \vee \mathscr{P}_l$, где $\mathscr{P}_i = a_{i1}a_{i2} \ldots a_{ir_i}$, причем первые и последние буквы разных слов $\mathscr{P}_i$ $(1 \leqslant i \leqslant l)$ различны. Покажем, что каждое регулярное выражение Q такого вида минимально. Пусть сначала $l = 1$, т. е. $R = \{\mathscr{P}\}$, где $\mathscr{P}$ — слово. Если R' — минимальное выражение, такое, что $\{\mathscr{P}\}=|R|$, то, в силу конечности $|R'|$, R' не имеет вида $\langle Q\rangle$. Если $R'=Q_1\vee\ldots\vee Q_q$ $(q\geqslant 1)$, то некоторое событие $|Q_j|$ $(1\leqslant j\leqslant q)$ содержит слово $\mathscr{P}$, и тогда $|R'|=|Q_j|=\{\mathscr{P}\}$, в противоречие с минимальностью R'. Поэтому R' можно представить в виде $Q_1,\ldots Q_s$, где Q_i $(1\leqslant i\leqslant s)$ есть либо буква, либо выражение вида $Q'\vee Q''$. Последний случай невозможен, так как тогда в $|R'|$ содержится не менее двух слов. Поэтому каждое Q_i — буква, т е. R' имеет вид $a_{11}\ldots a_{1r_1}$. Пусть для всех $l\leqslant n-1$ уже доказано, что единственное минимальное выражение, задающее событие $\{\mathscr{P}_1,\ldots,\mathscr{P}_l\}$, имеет вид $\bigvee\limits_{i=1}^{l} a_{i_1}\ldots a_{ir_i}$, и пусть R' — минимальное выражение, задающее событие $\{\mathscr{P}_1,\ldots,\mathscr{P}_l\}$ при $l=n$. Очевидно, что R' не содержит операции итерации. Пусть $R'=Q_1\ldots Q_q$. Так как $|R'|$ содержит не менее двух слов, то для некоторого i $|Q_i|$ содержит не менее двух слов, и тогда, как легко заметить, в $|R'|$ входят либо два слова, начинающиеся с одной и той же буквы, либо два слова, кончающиеся на одну и ту же букву. Поэтому случай $R'=Q_1\ldots Q_q$ невозможен, и R' имеет вид $Q_1\vee\ldots\vee Q_q$. Очевидно, что для любого i $1\leqslant|Q_i|\leqslant l-1$, причем каждое Q_i $(1\leqslant i\leqslant q)$ — минимальное выражение, задающее событие $|Q_i|$. По предположению индукции Q_i должно иметь вид дизъюнкции слов, входящих в $|Q_i|$, причем в силу минимальности R' имеем $|Q_i|\cap|Q_j|=\varnothing$ при $i\neq j$. Отсюда и вытекает, что R' имеет вид дизъюнкции слов $\mathscr{P}_1,\ldots,\mathscr{P}_l$, так что регулярное выражение $\mathbf{A}_1(G)$, где G — источник вида, указанного на рис. 3.15, действительно минимально. Вторая часть утверждения теоремы извлекается из доказательства теоремы 3.12. Теорема доказана.

Ситуация, аналогичная теореме 3.12, возникает и для улучшенного способа синтеза $S(\pi, \mathscr{D})$ В. М. Глушкова, описанного в § 2 этой главы. Перед тем как перейти к исследованию эффективности алгоритма синтеза $S(\pi, \mathscr{D})$, введем ряд новых понятий.

Пусть v — произвольная вершина источника G; G_v — источник, получающийся из источника G выбором вершины v в качестве начальной и удалением всех вершин источника G, которые недостижимы из вершины v, вместе с инцидентными им ребрами. Различные вершины v_1 и v_2 источника G будем называть **эквивалентными** (обозначать $v_1\sim v_2$), если $|G_{v_1}|=|G_{v_2}|$.

Источник G над алфавитом A назовем **минимальным**, если не существует источника G' над A с меньшим, чем у G, числом вершин, и такого, что $|G|=|G'|$.

Нетрудно установить справедливость следующего утверждения.

Утверждение. Источник G минимален тогда и только тогда, когда любые две его различные вершины v_1 и v_2 не эквивалентны.

Слова p и q будем называть **циклически подобными**, если найдутся такие слова r_1 и r_2, что $p=r_1^k$, $q=r_2^l$, причем слова r_1 и r_2 получаются друг из друга циклическим сдвигом (k, l — натуральные).

Пусть $\mathscr{M}$ — класс всех принадлежащих $\tilde{R}$ регулярных выражений вида

$$\mathscr{D}=\mathscr{D}_1\vee \dots \vee\mathscr{D}_m,$$

где $\mathscr{D}_i = \mathscr{P}_{i0} \langle Q_{i1}\rangle \mathscr{P}_{i1} \dots \mathscr{P}_{i,s_i-1} \langle Q_{is_i}\rangle \mathscr{P}_{is_i}$ $(1 \leqslant i \leqslant m)$, $s_i \geqslant 0$, $\mathscr{P}_{ij}$, Q_{ij} $(0\leqslant j\leqslant s_i)$ — слова, $Q_{ij}\neq e$; при $j\neq 0, s_i$ $\mathscr{P}_{ij}\neq e$, последняя буква слова $\mathscr{P}_{ij}$ отличается от последней буквы слова $Q_{i\,j+1}$ $(0\leqslant j\leqslant \leqslant s_i - 1)$ и начальная буква слова $\mathscr{P}_{ij}$ отличается от начальной буквы слова Q_{ij} $(0\leqslant j\leqslant s_i)$.

Обозначим $\mathscr{M}_1$ — подкласс класса $\mathscr{M}$ регулярных выражений, у которых слова Q_{is_i} не являются циклически подобными.

Пусть $\mathscr{M}_2$ — подкласс класса $\mathscr{M}$, такой, что существуют $k, l \in \{1, 2, \dots, m\}$, такие, что $\mathscr{D}_l = R_l \langle Q_{ls_l}^{\cdot}\rangle \mathscr{P}_{ls_l}^{\cdot}$, $\mathscr{D}_k = R_k \langle Q_{ls_l}\rangle \mathscr{P}_{ls_l}$, причем кратчайшее слово события $|R_t|$ $(t\in\{k, l\})$ не является началом ни одного слова события $\mathscr{D}_r$ при $r\neq t$ и $|Q_{ls_l}|\geqslant 2$ ($|Q_{ls_l}|$ — длина слова Q_{ls_l}).

Теорема 3.14 [16]. а) Для каждого регулярного выражения $\mathscr{D}\in\mathscr{M}_1$ существует такая последовательность отождествлений π, что источник $S(\pi, \mathscr{D})$ — минимален.

б) Для любого выражения $\mathscr{D}\in\mathscr{M}_2$ и последовательности отождествлений π источник $S(\pi, \mathscr{D})$ — не минимален

Доказательство. Докажем сначала пункт а) теоремы.

Рассмотрим произвольное регулярное выражение $\mathscr{D}\in\mathscr{M}_1$. Как нетрудно заметить, основные места, расположенные после последних букв слов $\mathscr{P}_{ij}$ и $Q_{i\,j+1}$ подобны. Применим к этим местам операции отождествления мест и, следуя улучшенному способу синтеза В. М. Глушкова, построим источник $G=S(\pi, \mathscr{D})$.

Если m — обобщенное место выражения R, то назовем **m-пучком** в R множество всех таких слов p, что хотя бы одно из мест p-спектра в R принадлежит обобщенному месту m.

Пусть m — обобщенное место выражения $\mathscr{D}$, соответствующее указанной выше последовательности π отождествлений мест. Сопоставим этому месту m выражения $N_m(\mathscr{D})$ и $K_m(\mathscr{D})$, которые назовем m-началом и m-концом выражения $\mathscr{D}$. Возможны следующие случаи:

а) m состоит из одного места, расположенного в члене $\mathscr{D}_i$ после буквы p_s слова $\mathscr{P}_{ij}=p_1 \dots p_s \dots p_r$, где $r>s$ при $j\neq s_i$. Тогда

$$N_m(\mathscr{D}) =\mathscr{P}_{i0}\langle Q_{i1}\rangle \dots \langle Q_{ij}\rangle p_1 \dots p_s,$$

$$K_m(\mathscr{D}) = p_{s+1} \dots p_r \langle Q_{i\,j+1}\rangle \mathscr{P}_{i\,j+1} \dots \langle Q_{is_i}\rangle \mathscr{P}_{is_i}.$$

б) m состоит из одного места, расположенного в члене $\mathscr{D}_i$ после буквы q_s слова $Q_{ij}=q_1 \dots q_s \dots q_r$; $r>s$. Тогда

$$N_m(\mathscr{D}) =\mathscr{P}_{i0}\langle Q_{i1}\rangle \dots \langle Q_{i\,j-1}\rangle\mathscr{P}_{i\,j-1}\langle Q_{ij}\rangle q_1 \dots q_s,$$

$$K_m(\mathscr{D}) = q_{s+1} \dots q_r \langle Q_{ij}\rangle \mathscr{P}_{ij} \dots \langle Q_{is_i}\rangle \mathscr{P}_{is_i}.$$

в) m состоит из двух мест, расположенных в члене $\mathscr{D}_i$ после последних букв слов $\mathscr{P}_{ij}$ и $Q_{i\,j+1}$. Тогда

$$N_m(\mathscr{D})=\mathscr{P}_{i0}\langle Q_{i1}\rangle\ldots\mathscr{P}_{i\,j-1}\langle Q_{ij}\rangle\mathscr{P}_{ij}\langle Q_{i\,j+1}\rangle,$$
$$K_m(\mathscr{D})=\langle Q_{i\,j+1}\rangle\mathscr{P}_{i\,j+1}\ldots\langle Q_{is_i}\rangle\mathscr{P}_{is_i}.$$

г) m — начальное место. Тогда

$$N_m(\mathscr{D})=e \text{ (пустое слово)},$$
$$K_m(\mathscr{D})=\mathscr{D}.$$

Ясно, что событие $|N_m(\mathscr{D})|$ состоит из всех таких слов p, что m входит в обобщенный p-спектр $\mathscr{D}$. (**Обобщенный p-спектр выражения** $\mathscr{D}$ — множество всех обобщенных мест m таких, что хотя бы одно из основных мест, входящих в m, принадлежит р-спектру выражения $\mathscr{D}$.)

Лемма 3.20. Если $N_{m_1}(\mathscr{D})\neq N_{m_2}(\mathscr{D})$, то события $|N_{m_1}(\mathscr{D})|$ и $|N_{m_2}(\mathscr{D})|$ не пересекаются.

Доказательство. Пусть $N_{m_i}(\mathscr{D})=R_{i0}\langle S_{i1}\rangle R_{i1}\langle S_{i2}\rangle\ldots R_{it_i-1}\langle S_{it_i}\rangle R_{it_i}$; $i\in\{1, 2\}$. Пусть слово $p\in|N_{m_1}(\mathscr{D})|\cap|N_{m_2}(\mathscr{D})|$; тогда p можно представить в виде

$$R_{i0}S_{i1}^{l_{i1}}R_{i1}S_{i2}^{l_{i2}}\ldots R_{it_i-1}S_{it_i}^{l_{it_i}}R_{it_i}.$$

Отсюда видно, что одно из слов R_{10} и R_{20} является началом другого; пусть, например, R_{10} есть начало слова R_{20}. Если $t_1>0$, то, в силу слабой отделимости членов выражения $\mathscr{D}$, R_{10} должно совпадать с R_{20} и S_{11} — с S_{21}. Если же $t_1=0$, то $p=R_{10}$, и тогда необходимо, чтобы R_{20} совпало с R_{10} (иначе длина слова p, началом которого служит слово R_{20}, была бы больше, чем длина слова R_{10}). При этом, в силу слабой отделимости членов $\mathscr{D}$, необходимо $t_2=0$ и $N_{m_1}(\mathscr{D})\equiv N_{m_2}(\mathscr{D})$, что противоречит условию леммы. Поэтому $t_1>0$; $R_{10}=R_{20}$; $S_{11}=S_{21}$. Таким образом, p можно представить в виде

$$p=R_{10}S_{11}^{l_{11}}R_{11}r_1=R_{10}S_{11}^{l_{21}}R_{21}r_2,$$

где r_1 и r_2 — некоторые слова. Если $l_{11}<l_{21}$, то, сокращая слева на $R_{10}S_{11}^{l_{11}}$ предыдущее равенство, получим:

$$R_{11}r_1=S_{11}^{l_{21}-l_{11}}R_{21}r_2.$$

Заметим, что по определению $N_{m_i}(\mathscr{D})$ $(i=1, 2)$ либо первая буква слова R_{11} отличается от первой буквы слова S_{11}, либо R_{11} есть собственное начало S_{11}, причем в последнем случае $r_1=e$, и длина слова R_{11} меньше длины слова, расположенного в правой части равенства. В обоих случаях приходим к противоречию, из которого заключаем, что $l_{11}\geqslant l_{21}$. Аналогично доказывается невозможность случая $l_{11}>l_{21}$, т. е., окончательно, $l_{11}=l_{21}$. Точно так же устанавливаем, что $R_{11}=R_{21}$, $S_{12}=S_{22}$, $l_{12}=l_{22}$ и т. д. В конце концов получаем, что $N_{m_1}(\mathscr{D})=N_{m_2}(\mathscr{D})$, что противоречит условию леммы, так что не существует слово $p\in|N_{m_1}(\mathscr{D})|\cap|N_{m_2}(\mathscr{D})|$. Лемма доказана.

Лемма 3.21. Множество обобщенных мест выражения $\mathscr{D}$ является вершиной источника $G = S(\pi, \mathscr{D})$ тогда и только тогда, когда оно есть множество обобщенных мест m, имеющих одно и то же m-начало.

Доказательство. Пусть v — вершина источника G, достижимая из начальной вершины v_0 по слову p, т. е. v — множество всех обобщенных мест выражения $\mathscr{D}$, принадлежащих обобщенному p-спектру $\mathscr{D}$. Пусть обобщенное место $m \in v$. Тогда $p \in |N_m(\mathscr{D})|$, т. е. все m-начала мест m, входящих в v, содержат (как события) слово p; в силу леммы 3.20 эти m-начала совпадают. Если m' — произвольное обобщенное место выражения $\mathscr{D}$, такое, что $N_{m'}(\mathscr{D}) \equiv N_m(\mathscr{D})$, где $m \in v$, то $p \in |N_{m'}(\mathscr{D})|$, т. е. m' входит в обобщенный p-спектр $\mathscr{D}$, так что v действительно есть множество всех обобщенных мест m, имеющих одно и то же m-начало.

Обратно, пусть $\tilde{m}$ — множество всех обобщенных мест m, имеющих одно и то же m-начало N. Рассмотрим слово $p \in |N|$. Покажем, что $\tilde{m}$ есть обобщенный p-спектр $\mathscr{D}$. При $m \in \tilde{m}$ имеем: $N_m(\mathscr{D}) = N$, т. е. $p \in |N_m(\mathscr{D})|$ и m входит в обобщенный p-спектр $\mathscr{D}$. Если же $m \notin \tilde{m}$, то $|N_m(\mathscr{D})| \cap |N| = \varnothing$, т. е. $p \notin |N_m(\mathscr{D})|$ и m не входит в обобщенный p-спектр $\mathscr{D}$. Лемма доказана.

Пусть v — вершина источника $G = S(\pi, \mathscr{D})$. Будем обозначать M_v множество всех слов, переводящих вершину v в одну из финальных вершин источника G и говорить, что M_v есть событие, соответствующее вершине v.

Очевидна следующая лемма.

Лемма 3.22. Если v — вершина источника $G = S(\pi, \mathscr{D})$, то

$$M_v = |\bigvee_{m \in v} K_m(\mathscr{D})|.$$

Выражение $\bigvee\limits_{m \in v} K_m(\mathscr{D})$ называем регулярным выражением, соответствующим вершине v.

Лемма 3.23. В источнике $G = S(\pi, \mathscr{D})$ не существует вершин, достижимых по одной и той же букве из двух различных вершин.

Доказательство. Пусть N есть m-начало выражения $\mathscr{D}$. Будуем обозначать вершину v источника G, образованную всеми обобщенными местами m, такими, что $N_m(\mathscr{D}) = N$, посредством $\mathfrak{M}_N$. Возможны следующие случаи:

а) $N = \mathscr{P}_{i0}\langle Q_{i1}\rangle\mathscr{P}_{i1} \ldots \langle Q_{ij}\rangle r_1 \ldots r_s$, где $s \geqslant 1$ (r_i — буквы). Тогда единственная вершина, из которой можно перейти в $\mathfrak{M}_N$ есть вершина $\mathfrak{M}_{N'}$, где $N' = \mathscr{P}_{i0}\langle Q_{i1}\rangle\mathscr{P}_{i1} \ldots \langle Q_{ij}\rangle r_1 \ldots r_{s-1}$.

б) $N = \mathscr{P}_{i0}\langle Q_{i1}\rangle\mathscr{P}_{i1} \ldots \langle Q_{ij}\rangle$. Тогда в $\mathfrak{M}_N$, можно перейти либо из вершины $\mathfrak{M}_{N'}$, где $N' = \mathscr{P}_{i0}\langle Q_{i1}\rangle\mathscr{P}_{i1} \ldots \langle Q_{i\,j-1}\rangle p_1 \ldots p_{t-1}$, $\mathscr{P}_{ij} = p_1 \ldots \ldots p_{t-1} p_t$, либо из вершины $\mathfrak{M}_{N''}$, где $N'' = \mathscr{P}_{i0}\langle Q_{i1}\rangle\mathscr{P}_{i1} \ldots \langle Q_{i\,j-1}\rangle \mathscr{P}_{i\,j-1}\langle Q_{ij}\rangle q_1 \ldots q_{s-1}$, $Q_{ij} = q_1 \ldots q_s$. В первом случае переход осуществляется по букве p_t, а во втором — по букве q_s, и по условию на $\mathscr{D}$ $p_r \neq q_s$.

в) $N = e$. Тогда в $\mathfrak{M}_N$ нельзя перейти ни из какой вершины.

Как нетрудно заметить, во всех перечисленных случаях утверждение леммы верно. Лемма доказана.

Лемма 3.24. Если $\mathfrak{M}_1$ и $\mathfrak{M}_2$ ($\mathfrak{M}_1 \neq \mathfrak{M}_2$) — вершины источника $G=S(\pi, \mathscr{D})$ и $\mathfrak{M}_2$ достижима из $\mathfrak{M}_1$, то $\mathfrak{M}_1$ и $\mathfrak{M}_2$ не эквивалентны.

Доказательство. Предположим, что вершины $\mathfrak{M}_1$ и $\mathfrak{M}_2$ эквивалентны. Так как $\mathfrak{M}_2$ достижимо из $\mathfrak{M}_1$ по некоторому слову p, то слово p является началом некоторого слова q, по которому некоторая финальная вершина достижима из вершины $\mathfrak{M}_1$. В силу того, что $\mathfrak{M}_2$ эквивалентно $\mathfrak{M}_1$, по слову q из состояния $\mathfrak{M}_2$ достижима некоторая финальная вершина, причем слово p переводит $\mathfrak{M}_2$ в некоторую вершину $\mathfrak{M}_3$. Очевидно, что $\mathfrak{M}_2$ и $\mathfrak{M}_3$ эквивалентны. Берем теперь вершины $\mathfrak{M}_2$ и $\mathfrak{M}_3$ и по ним, как и по вершинам $\mathfrak{M}_1$ и $\mathfrak{M}_2$, находим некоторую вершину $\mathfrak{M}_4$ и т. д. В конце концов получаем цепочку вершин $\mathfrak{M}_1, \mathfrak{M}_2, \mathfrak{M}_3, \ldots, \mathfrak{M}_s$, причем $\mathfrak{M}_s = \mathfrak{M}_i$ для некоторого $i \in \{1, 2, \ldots, s-1\}$. Если $i>1$, то, как легко заметить, в источнике найдется вершина, которая по одной и той же букве достижима из двух различных вершин, что противоречит лемме 3.23 Если $i=1$, т е. $\mathfrak{M}_1 = \mathfrak{M}_s$, то в источнике G вершины $\mathfrak{M}_1$ и $\mathfrak{M}_2$ принадлежат одному и тому же циклу. Но тогда кратчайшие слова событий, соответствующих вершинам $\mathfrak{M}_1$ и $\mathfrak{M}_2$, имеют разную длину, что противоречит предположению об эквивалентности вершин $\mathfrak{M}_1$ и $\mathfrak{M}_2$. Таким образом, мы показали, что в любом случае $\mathfrak{M}_1$ не эквивалентно $\mathfrak{M}_2$. Лемма доказана.

Обозначим C_v множество всех членов выражения $\mathscr{D}$, которые содержат места m, принадлежащие вершине v источника G.

Лемма 3.25. Пусть $\mathfrak{M}_1$ и $\mathfrak{M}_2$ — различные вершины источника $G=S(\pi, \mathscr{D})$, $\mathscr{D} \in \mathscr{M}_1$, причем $C_{\mathfrak{M}_1} \cap C_{\mathfrak{M}_2} \neq \varnothing$. Тогда вершины $\mathfrak{M}_1$ и $\mathfrak{M}_2$ не эквивалентны.

Доказательство. Пусть $\mathscr{D}_i \in C_{\mathfrak{M}_1} \cap C_{\mathfrak{M}_2}$, где $\mathscr{D}_i$ — член выражения $\mathscr{D}$. Так как $\mathfrak{M}_1 \neq \mathfrak{M}_2$, то обобщенные места $m_1 \in \mathfrak{M}_1$ и $m_2 \in \mathfrak{M}_2$, расположенные в члене $\mathscr{D}_i$, различны. Пусть, например, m_1 находится левее обобщенного места m_2. Тогда нетрудно указать слово p, такое, что одно из мест, входящих в m_2, p-следует за одним из мест, входящих в $\mathfrak{M}_1$, так что это слово переводит вершину $\mathfrak{M}_1$ в вершину $\mathfrak{M}_2$. По лемме 3.23 находим, что $\mathfrak{M}_1 \not\sim \mathfrak{M}_2$. Лемма доказана.

Очевидна следующая лемма.

Лемма 3.26. Если $p=q^k$ (q — слово; k — натуральное число) и $\tilde{p}$ получено циклическим сдвигом слова p, то $\tilde{p}=\tilde{q}^k$, где $\tilde{q}$ получено циклическим сдвигом слова q.

Лемма 3.27. Пусть $p^m=q^n$ (p, q — слова). Тогда найдется такое слово r, что $p=r$, $q=r^l$.

Доказательство. Рассмотрим сверхслово $pp\ldots$. Так как $p^m = q^n$, то оно совпадает со сверхсловом $qq\ldots$. Обозначим i-ю букву этого сверхслова через a_i; $i=1, 2, \ldots$. Пусть $d_p=[p]$, $d_q = [q]$ — длины слов p и q. Тогда, очевидно, для любого i имеем $a_{i+d_p} = a_i$, $a_{i+d_q} = a_i$. Пусть $d=(d_p, d_q)$; тогда $d=t\cdot d_p+s\cdot d_q$

для подходящих целых t и s, так что при i, больших некоторого i_0, выполняется $a_{i+d}=a_i$. Пусть $md_p>i_0$, $md_q>i_0$. Имеем:

$$p = a_{md_p+1} \ldots a_{(m+1)d_p}; \quad q = a_{md_q+1} \ldots a_{(m+1)d_q},$$

причем $p = r^{d_p/d}$; $q = r^{d_q/d}$, где $r = a_{md_p+1} \ldots a_{md_p+d} = a_{md_q+1} \ldots a_{md_q+d}$, что и доказывает лемму.

Лемма 3.28. Пусть $R = \mathscr{P}_1 \langle Q_1 \rangle \mathscr{P}_2 \langle Q_2 \rangle \ldots \mathscr{P}_s \langle Q_s \rangle \mathscr{P}_{s+1}$, где $\mathscr{P}_i$, Q_i — слова ($Q_i \neq e$) и $p=q\cdot r^n h \in |R|$ — слово, причем $r \neq e$, первые буквы слов r и h различны и $n>m(s+1)([q]+[r]+1)$ ($[q]$, $[r]$ — длины слов q и r; m — наибольшая из длин $[\mathscr{P}_i]$, $[Q_j]$ слов $\mathscr{P}_i$, Q_j). Тогда найдется такое $l \geqslant 1$, что r циклически подобно одному из слов $Q_1, \ldots, Q_l$, причем $h \in |\mathscr{P}'_{l+1} \langle Q_{l+1} \rangle \ldots$ $\ldots \langle Q_s \rangle \mathscr{P}_{s+1}|$, где $[\mathscr{P}'_{l+1}] \leqslant \max([\mathscr{P}_{l+1}], [Q_{l+1}])$.

Доказательство. Так как $p \in |R|$, то $p = \mathscr{P}_1 Q_1^{i_1} \mathscr{P}_2 Q_2^{i_2} \ldots \mathscr{P}_s Q_s^{i_s} \mathscr{P}_{s+1}$ ($i_j \geqslant 0$; $1 \leqslant j \leqslant s$). Тогда $qr^n = \mathscr{P}_1 Q_1 \ldots \mathscr{P}_{\tilde{l}+1} Q_{\tilde{l}+1}^{i'_{\tilde{l}+1}} Q'$, где $i'_{\tilde{l}+1} \leqslant i_{\tilde{l}+1}$, причем при $i'_{\tilde{l}+1} < i_{\tilde{l}+1}$ Q' есть начало слова $Q_{\tilde{l}+1}^{i_{\tilde{l}+1}}$, а при $i'_{\tilde{l}+1} = i_{\tilde{l}+1}$ Q' есть начало слова $\mathscr{P}_{\tilde{l}+2}$ (в силу выбора n, $[qr^n] > [\mathscr{P}_1]$). Предположим, что $i_1 \leqslant [q]+[r], \ldots, i'_{\tilde{l}+1} \leqslant [q]+[r]$. Тогда длина $\mathscr{P}_1 Q_1^{i_1} \ldots \mathscr{P}_{\tilde{l}+1} Q_{\tilde{l}+1}^{i'_{\tilde{l}+1}} Q'$ не превосходит

$$\sum_{i=1}^{s+1} ([\mathscr{P}_i] + ([q]+[r]) \cdot [Q_i]) \leqslant m(s+1)([q]+[r]+1),$$

в то время как длина qr^n не менее $n>m(s+1)([q]+[r]+1)$ по условию. Поэтому найдется такое j, что $i_j > [q]+[r]$ (либо при $j=\tilde{l}+1$, $i'_j > [q]+[r]$).

Пусть $j = \tilde{l}+1$; $i'_{\tilde{l}+1} < i_{\tilde{l}+1}$. Тогда Q' — начало $Q_{\tilde{l}+1}$, т. е. $Q_{\tilde{l}+1} = Q'Q''$, и слово h можно представить в виде $Q''h'$, где h' — некоторое слово. С другой стороны, $qr^n = \mathscr{P}' Q_{\tilde{l}+1}^{i'_{\tilde{l}+1}} Q'$ ($\mathscr{P}' = \mathscr{P}_1 Q_1^{i_1} \ldots$ $\ldots Q_{\tilde{l}}^{i_{\tilde{l}}} \mathscr{P}_{\tilde{l}+1}$), причем $i'_{\tilde{l}+1} > [q]+[r]$. Обозначим $\tilde{Q}_{\tilde{l}+1} = Q''Q'$, тогда последнее равенство перепишется в виде

$$qr^n = \mathscr{P}' Q_{\tilde{l}+1}^{i'_{\tilde{l}+1}-[r]} Q' \tilde{Q}_{\tilde{l}+1}^{[r]} = \mathscr{P}'' \tilde{Q}_{\tilde{l}+1}^{[r]},$$

где $[\mathscr{P}''] \geqslant i'_{\tilde{l}+1} - [r] > [q]$. Далее, $[qr^n] = +n[r] = [\mathscr{P}''] + r[\tilde{Q}_{\tilde{l}+1}]$, и из $[q] < [\mathscr{P}'']$ вытекает, что $n > [\tilde{Q}_{\tilde{l}+1}]$. Отсюда $qr^{n-[\tilde{Q}_{\tilde{l}+1}]} = \mathscr{P}''$, и так как длины слов $r^{[\tilde{Q}_{\tilde{l}+1}]}$ и $\tilde{Q}_{\tilde{l}+1}^{[r]}$ равны, то $r^{[\tilde{Q}_{\tilde{l}+1}]} = \tilde{Q}_{\tilde{l}+1}^{[r]}$, т. е. первые буквы слов r и Q'' совпадают. Так как $h = Q''h'$, то получаем, что совпадают и первые буквы слов r и h, что противоречит предположению леммы. Поэтому при $i'_{\tilde{l}+1} < i_{\tilde{l}+1}$ имеет место $j \neq \tilde{l}+1$.

Обозначим $\tilde{\mathscr{P}} = \mathscr{P}_1 Q_1^{i_1} \dots Q_{j-1}^{i_{j-1}} \mathscr{P}_j$; $\tilde{\tilde{\mathscr{P}}} = \mathscr{P}_{j+1} Q_{j+1}^{i_{j+1}} \dots Q_{\tilde{l}+1}^{i'_{\tilde{l}+1}} Q'$. Тогда $qr^n = \tilde{\mathscr{P}} Q_j^{i_j} \tilde{\tilde{\mathscr{P}}}$, причем $i_j > [q] + [r]$, т. е. $qr^n = \tilde{\mathscr{P}} Q_j^{i_j - [r]} Q_j^{[r]} \tilde{\tilde{\mathscr{P}}} = \mathscr{P}^* Q_j^{[r]} \tilde{\tilde{\mathscr{P}}}$. При этом $[\mathscr{P}^*] > (i_j - [r]) > [q]$, так что $Q_j^{[r]} \tilde{\tilde{\mathscr{P}}}$ можно представить в виде $r'' r^{n'}$, где r'' — конец слова r; $r = r' r''$, $[r''] < [r]$; $n' \leqslant n$. Обозначим $\tilde{r} = r'' r'$, тогда $\tilde{r}^{n'} r'' = Q_j^{[r]} \tilde{\tilde{\mathscr{P}}}$. Если $n' < [Q_j]$, то $[\tilde{r}^{n'} r''] = n' [r] + [r''] \leqslant ([Q_j] - 1) \cdot [r] + [r''] = [Q_j] \cdot [r] + [r''] - [r] < [Q_j] \cdot [r]$, что невозможно. Поэтому $n' \geqslant [Q_j]$; $\tilde{r}^{[Q_j]} \tilde{r}^{n' - [Q_j]} r'' = Q_j^{[r]} \tilde{\tilde{\mathscr{P}}}$, и так как длины слов $\tilde{r}^{[Q_j]}$, $Q_j^{[r]}$ равны, то $r^{[Q_j]} = Q_j^{[r]}$. По лемме 3.27 слова $\tilde{r}$ и Q_j суть степени одного и того же слова t, и по лемме 3.26 слова r и Q_j циклически подобны. При $i'_{\tilde{l}+1} < i_{\tilde{l}+1}$ в качестве l берем $\tilde{l}$, тогда r циклически подобно слову Q_j, где $1 \leqslant j \leqslant l$ в силу сделанного выше замечания, причем $h = Q'' Q_{l+1}^{i_{l+1} - i'_{l+1} - 1} \mathscr{P}_{l+2} \dots$ $\dots Q_s^{i_s} \mathscr{P}_{s+1}$, т. е. $h \in | Q'' \langle Q_{l+1} \rangle \dots \langle Q_s \rangle \mathscr{P}_{s+1} |$ и $[Q''] \leqslant \max([\mathscr{P}_{l+1}], [Q_{l+1}])$. В случае $i'_{\tilde{l}+1} = i_{\tilde{l}+1}$ достаточно положить $l = \tilde{l} + 1$. Лемма доказана.

Лемма 3.29. Пусть $\mathfrak{M}_1$ и $\mathfrak{M}_2$ — вершины источника $G = S(\pi, \mathscr{D})$, причем $C_{\mathfrak{M}_1} \cap C_{\mathfrak{M}_2} = \varnothing$ и хотя бы одно из регулярных выражений, соответствующих этим вершинам, содержит символ итерации. Тогда $\mathfrak{M}_1 \not\sim \mathfrak{M}_2$.

Доказательство. Предположим, что $\mathfrak{M}_1 \sim \mathfrak{M}_2$. Пусть $\bigvee_{m \in \mathfrak{M}_1} K_m(\mathscr{D}) = \bigvee_{i=1}^{t} \mathscr{L}_i$; $\bigvee_{m \in \mathfrak{M}_2} K_m(\mathscr{D}) = \bigvee_{i=1}^{t'} \mathscr{L}'_i$. Так как $\mathfrak{M}_1 \sim \mathfrak{M}_2$, то $|\bigvee_{i=1}^{t} \mathscr{L}_i| = |\bigvee_{i=1}^{t'} \mathscr{L}'_i|$. Пусть $\mathscr{L}_j$ — член, имеющий наибольшее среди членов $\mathscr{L}_i$ и $\mathscr{L}'_i$ число символов итерации; $\mathscr{L}_j = p_1 \langle q_1 \rangle p_2 \dots p_r \langle q_r \rangle p_{r+1}$. Рассмотрим слова $\alpha_n = p_1 q_1^n p_2 q_2^n p_3 \dots p_r q_r^n p_{r+1}$; $\alpha_n \in |\mathscr{L}_j|$. Тогда найдется такой член $\mathscr{L}'_{j'}$, что $|\mathscr{L}'_{j'}|$ содержит бесконечно много слов α_n; пусть $\mathscr{L}'_{j'} = \mathscr{P}_1 \langle Q_1 \rangle \mathscr{P}_2 \dots \mathscr{P}_s \langle Q_s \rangle \mathscr{P}_{s+1}$. Рассмотрим n_0, такое, что $\alpha_{n_0} \in |\mathscr{L}'_{j'}|$, причем $n_0 > K(s+1)(\max\limits_{i=1,\dots,r}([p_i] + [q_i]) + 1)$, где $K = \max\limits_{\mathscr{P}_u, Q_v}([\mathscr{P}_u], [Q_v])$. Тогда по лемме 3.28 существует такое $l_1 \geqslant 1$, что q_1 циклически подобно одному из слов $Q_1, \dots, Q_{l_1}$, причем $\alpha'_{n_0} = p_2 q_2^n p_3 \dots p_r q_r^0 p_{r+1} \in |\mathscr{P}'_{l_1+1} \langle Q_{l_1+1} \rangle \dots \langle Q_s \rangle \mathscr{P}_{s+1}|$, где $\max\limits_{\substack{u \geqslant l_1+2, \\ v \geqslant l_1+1}} \{[\mathscr{P}_u], [Q_v], [\mathscr{P}'_{l_1+1}]\} = K' \leqslant K$, и снова можно применить лемму 3.28 к слову α'_{n_0} и выражению $\mathscr{P}'_{l_1+1} \langle Q_{l_1+1} \rangle \dots \langle Q_s \rangle \mathscr{P}_{s+1}$. Повторяя это рассуждение r раз, получим, что слова $q_1, q_2, \dots, q_r$ циклически подобны словам $Q_{i_1}, Q_{i_2}, \dots, Q_{i_r}$ (i_j — различны), и так как $s \leqslant r$, то $i_1 = 1$, $i_2 = 2, \dots, i_r = r = s$, т. е. слова Q_s и q_r циклически подобны, что противоречит предположению о выражении $\mathscr{D}$. Лемма доказана.

Лемма 3.30. Существует такая последовательность $\tilde{\pi}$ отождествлений соответствующих и подобных мест выражения $\mathscr{D}$, продолжающая отождествления мест в $\mathscr{D}$, соответствующие способу $S(\pi, \mathscr{D})$, что если $\mathfrak{M}_1 \sim \mathfrak{M}_2$ — различные вершины источника $G=S(\pi, \mathscr{D})$, то каждое место $m_1 \in \mathfrak{M}_1$ отождествлено с каждым местом $m_2 \in \mathfrak{M}_2$.

Доказательство. Пусть M_1 — множество обобщенных мест выражения $\mathscr{D}$, возникших при описании способа $S(\pi, \mathscr{D})$. Отождествим всевозможные соответственные места из M_1; получим некоторое множество обобщенных мест, которое обозначим M_2. Затем в произвольной последовательности отождествляем подобные места из M_2, пока это возможно, и полученное множество обобщенных мест обозначим M_3.

Легко заметить, что для любой вершины $\mathfrak{M}$ источника G любые обобщенные места $m, m' \in \mathfrak{M}$; $m, m' \in M_1$, являются соответственными. Поэтому все места $m \in \mathfrak{M}$ входят в одно и то же обобщенное место из M_3; обозначаем его $\widehat{\mathfrak{M}}$.

Пусть $\mathfrak{M}_1$, $\mathfrak{M}_2$ — вершины источника $G=S(\pi, \mathscr{D})$, причем $\mathfrak{M}_1 \neq \mathfrak{M}_2$ и $\mathfrak{M}_1 \sim \mathfrak{M}_2$. По лемме 3 25 $C_{\mathfrak{M}_1} \cap C_{\mathfrak{M}_2} = \varnothing$, причем по лемме 3.29 выражения $R_1 = \bigvee\limits_{m \in \mathfrak{M}_1} K_m(\mathscr{D})$ и $R_2 = \bigvee\limits_{m \in \mathfrak{M}_2} K_m(\mathscr{D})$ не содержат символов итераций, т. е. каждое $K_m(\mathscr{D})$, $m \in \mathfrak{M}_1 \cup \mathfrak{M}_2$ есть слово в алфавите A. Очевидно, что в этом случае вершины источника G, достижимые из $\mathfrak{M}_1$ и $\mathfrak{M}_2$, не принадлежат циклам. Предположим, что $\widehat{\mathfrak{M}}_1 \neq \widehat{\mathfrak{M}}_2$. Пусть $L(\mathfrak{M}_1, \mathfrak{M}_2)$ — число вершин источника $G=S(\pi, \mathscr{D})$, достижимых из $\mathfrak{M}_1$ и $\mathfrak{M}_2$. Без ограничения общности можно считать, что

$$L(\mathfrak{M}_1, \mathfrak{M}_2) = \min_{\substack{v_1 \sim v_2 \\ \widehat{v}_1 \neq \widehat{v}_2}} (L(v_1, v_2)).$$

Если из вершин $\mathfrak{M}_1$ и $\mathfrak{M}_2$ не выходят ребра, то обобщенные места $\widehat{\mathfrak{M}}_1$ и $\widehat{\mathfrak{M}}_2$, очевидно, подобны, что противоречит построению множества M_3. Пусть из вершин $\mathfrak{M}_1$ и $\mathfrak{M}_2$ выходят ребра, тогда в силу $\mathfrak{M}_1 \sim \mathfrak{M}_2$ множества их отметок одинаковы. Если из вершины $\mathfrak{M}_1$ выходит ребро с отметкой a, ведущее к вершине $\mathfrak{M}_1'$, а из $\mathfrak{M}_2$ — ребро с той же отметкой, ведущее к вершине $\mathfrak{M}_2'$, то $\mathfrak{M}_1' \sim \mathfrak{M}_2'$ и либо $\mathfrak{M}_1' \equiv \mathfrak{M}_2'$, либо, так как $L(\mathfrak{M}_1', \mathfrak{M}_2') < L(\mathfrak{M}_1, \mathfrak{M}_2)$, $\widehat{\mathfrak{M}}_1' = \widehat{\mathfrak{M}}_2'$. В результате $\widetilde{\mathfrak{M}}_1$ и $\widehat{\mathfrak{M}}_2$ снова оказываются подобными. Полученное противоречие и доказывает, что $\widehat{\mathfrak{M}}_1 = \widehat{\mathfrak{M}}_2$. Лемма доказана

Из леммы 3.30 непосредственно вытекает доказательство пункта а) теоремы 3.14.

Доказательство пункта б) теоремы 3.14 непосредственно следует из следующей леммы.

Лемма 3.31. Не существует такой последовательности π отождествлений соответственных и подобных мест выражения $\mathscr{D} \in M_2$, что источник $G=S(\pi, \mathscr{D})$ минимален.

Доказательство. Пусть $d(\pi)$ — длина последовательности π;

$Q_{ts_l} = q_1 \dots q_h, h \geqslant 2$, где $q_i \in A$. Обозначим $m_j^{(t)}$ $(t \in \{k, l\};\ j \in \{1, \dots, h\})$ место, расположенное в члене $\mathscr{D}_t$ после буквы q_j слова Q_{ts_l}; $m_0^{(t)}$ — конечное место выражения $R_t (t \in \{k, l\})$. Покажем, что в результате отождествлений, определяемых последовательностью π, ни одно из мест $m_j^{(t)}$ при $j \neq 0, h$ не отождествляется ни с одним другим местом выражения $\mathscr{D}$, а места $m_h^{(t)}$ и $m_0^{(t)}$ $(t \in \{k, l\})$ могут быть отождествлены лишь друг с другом. Доказательство поведем индукцией по длине $d(\pi)$ последовательности π.

Если $d(\pi) = 0$, то утверждение очевидно. Предположим, что оно доказано для любой последовательности отождествлений длины, меньшей чем n, и пусть $d(\pi) = n$. Тогда π можно представить в виде $\pi'\xi$, где $d(\pi') = n - 1$; ξ — последнее отождествление. По предположению индукции, в результате последовательности отождествлений π' ни одно из мест $m_j^{(t)}$ $(t \in \{k, l\}$; $j \in \{1, \dots, h - 1)\}$ не отождествлялось ни с каким другим местом в $\mathscr{D}$, а места $m_0^{(t)}$ и $m_h^{(t)}$ $(t \in \{k, l\})$ отождествлены, быть может, лишь друг с другом.

Пусть $m_j'^{(t)}$ — обобщенное место выражения $\mathscr{D}$, возникшее после отождествлений последовательности π', содержащее место $m_j^{(t)}$; $(t \in \{k, l\}$; $j \in \{0, 1, \dots, h\})$. Возможны два случая:

1) ξ есть отождествление соответственных мест выражения $\mathscr{D}$. При $j \notin \{0, h\}$ кратчайшее слово в $m_i'^{(t)}$- пучке есть слово $p_{tj} = p_t q_1 \dots q_j$, где p_t — кратчайшее слово события $|R_t|$. При $j \in \{0, h\}$ кратчайшее слово $m_j'^{(t)}$- пучка есть либо $p_{tj} = p_t$ (если $m_j'^{(t)} = \{m_0^{(t)}\}$ либо $m_j'^{(t)} = \{m_0^{(t)}, m_h^{(t)}\}$), либо $p_{tj} = p_t q_1 \dots q_h$ (если $m_j'^{(t)} = \{m_h^{(t)}\}$). Пусть $m \neq m_j'^{(t)}$ — обобщенное место выражения $\mathscr{D}$ возникшее в результате отождествлений π', причем m и $m_j'^{(t)}$ — соответственные места. Так как p_t не является началом никакого слова, входящего в $\mathscr{D}_r$ при $r \neq t$, то в m найдется место m' из члена $\mathscr{D}_t$, m'-пучку которого принадлежит слово p_{tj}. Легко проверить, что если m' отлично от мест, входящих в $m_j'^{(t)}$, то слово p_{tj} не принадлежит m'-пучку. Поэтому в m должно входить хотя бы одно место из $m_j'^{(t)}$, что противоречит условию $m \neq m_j'^{(t)}$. Таким образом $m_j'^{(t)}$ не является соответственным никакому другому обобщенному месту, возникающему после отождествлений π', и не может быть отождествлено на данном шаге с другим обобщенным местом.

2) ξ есть отождествление подобных мест выражения $\mathscr{D}$. При $j \notin \{0, h\}$ обобщенное место $m_{j+1}'^{(t)}$ q_{j+1}-следует за $m_j'^{(t)}$ $(t \in \{k, l\}$; $j \in \{1, \dots l - 1\})$, причем из предположения индукции, а также из того, что последние буквы выражений R_t и Q_{ts_l} различны, вытекает, что $m_{j+1}'^{(t)}$ не является q_{j+1}-следующим ни за каким другим обобщенным местом. Поэтому $m_j^{(t)}$ не подобно ни какому другому обобщенному месту. Аналогично, при $j \in \{0, h\}$ нетрудно

проверить, что подобными могут оказаться лишь места $m_0'^{(t)} = \{m_0^{(t)}\}$ и $m_h^{(t)} = \{m_h^{(t)}\}$.

Нетрудно заметить, что p_{t0}-спектр ($t \in \{k, l\}$) выражения состоит из единственного места $m_0^{(t)}$, и по доказанному места $m_0^{(k)}$ и $m_0^{(l)}$ не отождествляются при любой последовательности π. Следовательно, вершины, достижимые из начальной вершины источника $G = S(\pi, \mathscr{D})$ по словам p_{k0} и p_{t0}, различны. Очевидно, эти вершины эквивалентны, т. е. источник G не минимален. Лемма доказана.

УПРАЖНЕНИЯ

1. Принадлежит ли источник G из упражнения 1 к § 2 гл. III классу K_3'?
2. При каких n источник G_n из упражнения 1 к § 4 гл. III не принадлежит классу K'_n?
3. Найти минимальное регулярное выражение R, такое, что $|R| = |G|$, где G источник из упражнения 1 к § 2 гл. III
4. Выяснить, какие из следующих регулярных выражений принадлежат классу M_1 введенному при формулировке теоремы 3.14:
   1°. $ab\langle bcba\rangle cb\langle bac\rangle ab \vee abc\langle cba\rangle bc$;
   2°. $cb\langle abc\rangle acba\langle cba\rangle a\langle bcabca\rangle a$;
   3°. $cb\langle abc\rangle acba \vee b\langle cba\rangle bc\langle ac\rangle bb$.
   Применяя улучшенный способ синтеза источников к найденным выражениям, построить минимальные источники.
5. Выяснить, какие из следующих регулярных выражений принадлежат классу M_2 (M_2 — из теоремы 3.14).
   1°. $ab\langle bca\rangle cb \vee b\langle ab\rangle c\langle bca\rangle cb \vee bc\langle b\rangle a$;
   2° $a\langle cab\rangle ba\langle ac\rangle b \vee a\langle ac\rangle b \vee b\langle a\rangle c$;
   3°. $ab\langle abc\rangle a \vee a\langle bc\rangle b\langle abc\rangle a$.
   Построить для этих регулярных выражений минимальные источники.

Глава IV
НЕКОТОРЫЕ ДРУГИЕ ВИДЫ ПОВЕДЕНИЙ

§ 1. КОНЕЧНЫЕ АВТОМАТЫ КАК СВЕРХАКЦЕПТОРЫ

В предыдущей главе рассматривалась задача распознавания автоматами множеств входных слов — так называемых событий. В этом параграфе будет рассмотрено естественное обобщение этой задачи — задача распознавания автоматами множеств входных сверхслов. Такие множества будут называться сверхсобытиями.

Пусть заданы ограниченно-детерминированная функция $g(x)$, реализуемая инициальным автоматом $\mathfrak{A}_q=(A, Q, B, \varphi, \psi, q)$ и набор подмножеств $B^{(1)}, B^{(2)}, \ldots, B^{(k)}$ множества B. Буква $a \in A$ называется **предельной** для сверхслова $\alpha^\infty = a(1)a(2)\ldots$, если для некоторой бесконечной последовательности $\{t_1, t_2, \ldots\}$ имеем: $a(t_i)=a$; $i=1, 2, \ldots$. Множество всех предельных букв образует **предел** сверхслова α^∞ и обозначается как $\lim(\alpha^\infty)$.

Будем говорить, что автомат $\mathfrak{A}_q$ **представляет подмножество** E, $E \subseteq A^\infty$, с помощью выделенного набора подмножеств $N=\{B^{(1)}, B^{(2)}, \ldots, B^{(k)}\}$, если для любого сверхслова α^∞ из A^∞ вхождение α^∞ в E эквивалентно соотношению $\exists i(\lim(\beta^\infty)=B^{(i)})$, где $\beta^\infty = g(\alpha^\infty)$.

Подмножества множества A^∞ будем называть **сверхсобытиями** над алфавитом A. Сверхсобытие E, $E \subseteq A^\infty$ назовем **представимым**, если существуют автомат $\mathfrak{A}_q$ и $N=\{B^{(1)}, \ldots, B^{(k)}\}$; $B^{(i)} \subseteq B$, $i=1, \ldots k$, такие, что E представимо автоматом $\mathfrak{A}_q$ с помощью набора $N=\{B^{(1)}, B^{(2)}, \ldots, B^{(k)}\}$, т. е. объектом $(A, Q, B, \varphi, \psi, q, B^{(1)}, B^{(2)}, \ldots, B^{(k)})$. Займемся описанием представимых сверхсобытий. Введем некоторые операции над сверхсобытиями.

а) **Объединением сверхсобытий** E_1 и E_2 называется множество $E_1 \cup E_2$, состоящее в точности из всех тех сверхслов α^∞, которые входят хотя бы в одно из множеств E_1 или E_2.

Нетрудно видеть, что эта бинарная операция ассоциативна и коммутативна, что позволяет использовать сокращенное обозначение $\bigcup\limits_{i=1}^{n} E_i$ для выражения $E_1 \cup E_2 \cup \ldots \cup E_n$ и не следить за порядком применения операции.

б) Пусть R — подмножество A^*. Свяжем с R **унарную операцию** O_R над сверхсобытиями. Сверхсобытие $O_R(E)$, $E \subseteq A^\infty$, состоит в точности из всех сверхслов α^∞ из A^∞, таких, что

$$\alpha^\infty = \beta^r \gamma^\infty,\ \beta^r \in R,\ \gamma^\infty \in E.$$

Если $R=\varnothing$, то $O_R(E)=\varnothing$ для любого E. Множество $O_R(E)$ будем иногда также обозначать как $R\cdot E$.

Укажем также некоторый способ «порождения» сверхсобытий. Для произвольного события $R, R\subseteq A^*$, рассмотрим сверхсобытие R^∞, состоящее в точности из всех сверхслов α^∞ из A^∞, таких, что $\alpha^\infty=\alpha_1^{r_1}\alpha_2^{r_2}\ldots$, где $\{\alpha_i^{r_i};\ i=1,2,\ldots\}$ — бесконечная последовательность слов из R. В обозначениях предыдущей главы, распространяя операцию произведения событий на бесконечные множества индексов, имеем

$$R^\infty=\prod_{i=1}^{\infty}R_i,\ \text{где } R_i=R;\quad i=1,2,\ldots .$$

Введем индуктивно понятие **общерегулярного множества** (сверхслов) над алфавитом $A=\{a_1, \ldots, a_m\}$ (для краткости — общерегулярные множества).

а) Для любого регулярного события R, $R\subseteq A^*$, множество R^∞ является общерегулярным.

б) Если множества E_1, E_2 общерегулярны, то множество $E_1\cup E_2$ также является общерегулярным.

в) Если E — общерегулярное множество, а R — регулярное событие, $R\subseteq A^*$, то $O_R(E)$ — общерегулярное множество (в других обозначениях $R\cdot E$ — общерегулярное множество).

Следующая теорема Мак-Нотона [19] дает исчерпывающее описание представимых сверхсобытий.

Теорема 4.1. Сверхсобытие является представимым тогда и только тогда, когда оно является общерегулярным.

Доказательство. Докажем сначала, что каждое общерегулярное множество является представимым. Для этого приведем ряд вспомогательных утверждений.

Лемма 4.1. Если сверхсобытия E_1 и E_2; E_1, $E_2\subseteq A^\infty$ представимые, то сверхсобытие $E_1\cup E_2$ также представимое.

Доказательство. Пусть сверхсобытия E_1 и E_2 представимы автоматами $\mathfrak{A}_q=(A, Q, B, \varphi, \psi, q)$ и $\mathfrak{A}'_{q'}=(A, Q', B', \varphi', \psi', q')$ с помощью наборов подмножеств $N_1=\{B_1, \ldots, B_{k_1}^*\}$ и $N_2=\{B'_1, \ldots, B'_{k_2}\}$ соответственно. Рассмотрим автомат $\mathfrak{A}_q\times\mathfrak{A}'_{q'}=(A, Q\times Q', B\times B', (\varphi,\varphi'), (\varphi,\psi'), (q,q'))$, и пусть $N=\{\bar{B}_1, \bar{B}_2, \ldots, \bar{B}_k\}$ — набор подмножеств множества $B\times B'$, который состоит в точности из всех таких подмножеств $\bar{B}$, что хотя бы для одного $i\in\{1, 2\}$ имеем $\mathrm{pr}^i(\bar{B})\in N_i$.

Нетрудно видеть, что сверхсобытие, представимое объектом $(\mathfrak{A}_q\times\mathfrak{A}'_{q'}, N)$, совпадает с сверхсобытием $E_1\cup E_2$. Лемма доказана.

Лемма 4.2. Если R — регулярное событие, $R\subseteq A^*$ и E — представимое сверхсобытие, то $O_R(E)$ — представимое сверхсобытие.

Доказательство. Пусть событие R и сверхсобытие E представимы объектами $(\mathfrak{A}_q, B_1)$ и $(\mathfrak{A}'_{q'}, N')$; $B_1\subseteq B$, $N'=\{B'_i;\ i=1,\ldots k\}$ соответственно, $\mathfrak{A}_q=(A, Q, B, \varphi, \psi, q)$; $\mathfrak{A}'_{q'}=(A, Q', B', \varphi', \psi', q')$

причем $|Q'|=n$. Рассмотрим отображение $v: \underbrace{Q''\times Q''\times\ldots\times Q''}_{n+1}\to$ $\to\underbrace{Q''\times Q''\times\ldots\times Q''}_{n+1}$; $Q''=Q'\cup\{\Lambda\}$, $\Lambda\notin Q'$, определенное следующим образом: пусть $(q_1, q_2, \ldots, q_{n+1})\in[Q'']^{n+1}$ и пусть i_1 — наименьший номер, такой, что $q_1\neq q_{i_1}$; i_2 — наименьший номер, такой, что $q_1\neq q_{i_2}$, $q_{i_1}\neq q_{i_2}$; i_l — наименьший номер, такой, что $q_1\neq q_i$, ..., $q_{i_{l-1}}\neq q_{i_l}$ и для каждого $j>i_l$ найдется $j'\leqslant i_l$, такое, что $q_j=q_{j'}$. Тогда

$$v(q_1, \ldots, q_{n+1})=(q_1, \Lambda, \ldots, \Lambda, q_{i_1}, \Lambda, \ldots, \Lambda, q_{i_2}, \ldots, \Lambda, q_{i_l}, \Lambda, \ldots).$$

Рассмотрим теперь объект

$$\mathscr{D}_{T_0}=(A, \mathscr{T}, \underbrace{B\times B''\times\ldots\times B''}_{n+1}, \Phi, \Psi, T_0, N),$$

где

$$B''=B'\cup\{\Lambda\},\ \mathscr{T}=Q\times[Q'']^{n+1},\ T_0=(q, \underbrace{\Lambda, \ldots, \Lambda}_{n+1}),$$

а функции Φ, Ψ и набор N определены следующим образом. Пусть $T=(t_1, t_2, t_{n+2},)$, $t_1\in Q$, $t_i\in Q''$, $i>1$, и i_0 — наименьший номер, такой, что $t_{i_0}=\Lambda$. Тогда полагаем

$$\Phi(T, a)=(\varphi(t_1, \alpha), v(\varphi'(t_2, a), \ldots, \varphi'(t_{i_0-1}, a), \xi, \varphi'(t_{i_0+1}, a), \ldots$$
$$\ldots, \varphi'(t_{n+2}, a))),$$

считая, что $\varphi'(\Lambda, a)=\Lambda$, а $\xi=q'$, если $\psi(t_1, a)\in B_1$, и $\xi=\Lambda$ в противном случае; полагаем

$$\Psi(T, a)=(\psi(t_1, a), \psi'(t_2, a), \ldots, \psi'(t_{n+2}, a)),$$

считая что $\psi'(\Lambda, a)=\Lambda$. Набор N состоит в точности из всех таких множеств $\bar{B}\subseteq B\times[B'']^{n+1}$, что хотя бы для одного $i\in\{2, 3, \ldots$ $\ldots, n+2\}\mathrm{pr}_i(\bar{B})\in N'$. Покажем, что объект $(\mathscr{D}_{T_0}, N)$ представляет сверхсобытие $O_R(E)$

а) Пусть $\alpha^\infty=\alpha^r\cdot\beta^\infty$, $\alpha^r\in R$, $\beta^\infty\in E$. Тогда $\psi(q\ \alpha^r)\in B_1$. Из определения функции Φ следует, что при подаче на автомат $\mathscr{D}$ последней буквы слова α^r компонента ξ примет значение q'. Если для любого начала β^s сверхслова β^∞ i_0-я компонента вектора $\Phi(T_0, \alpha^r\beta^s)$ не равна Λ, то нетрудно видеть, что $\lim \mathrm{pr}^{i_0}(H(\alpha^\infty))\in$ $\in N'$, где H — о.-д. функция, реализуемая автоматом $\mathscr{D}$. Если для некоторого β^s i_0-я компонента вектора $\Phi(T_0, \alpha^r\beta^s)$ приняла (под действием отображения v) значение Λ, то, в силу определения v, найдется номер $n_1<i_0$, такой, что либо состояния компоненты с номером n_1 бесконечно долго будут принимать значения, отличные от Λ, либо найдется номер $n_2<n_1$ и т. д. Этот процесс необходимо стабилизируется на некотором номере $\tilde{n}$. Компонента с этим номером вектора $\Phi(T_0, \alpha^r\beta)$, где β — начало β^∞ достаточной длины, будет принимать значения $\varphi'(q', \beta)$. Отсюда следует, что $\lim \mathrm{pr}^{\tilde{n}}(H(\alpha^\infty))\in N'$, так как $\beta^\infty\in E$

и для любого сверхслова β_1^∞, такого, что $\beta^\infty=\gamma\beta_1^\infty$ для некоторого слова γ имеем: $\lim h(\beta^\infty)=\lim h(\beta_1^\infty)$, где h — о.-д. функция, реализуемая автоматом $\mathfrak{A}'_{q'}$.

б) Пусть, обратно, $\lim(H(\alpha^\infty))\in N$. Это значит, что для некоторого $i\geqslant 2$ $\lim \mathrm{pr}^i(H(\alpha^\infty))\in N'$. Так как буква Λ не принадлежит ни одному из подмножеств набора N', то начиная с некоторого момента i-я компонента не «стирается» под действием отображения v. Пусть d — длина наменьшего начала α^d сверхслова α^∞, такая, что для любого начала $\alpha^{d'}$, $d'>d$, $\mathrm{pr}^i(\Phi(T_0,\ \alpha^{d'}))\neq\Lambda$. Тогда в силу определения Φ имеем $\Psi(q,\ \alpha^d)\in B_1$ и $\lim h(\beta^\infty)\in N'$, где $\alpha^\infty=\alpha^d\beta^\infty$. Следовательно, $\alpha^d\in R$ и $\beta^\infty\in E$. Лемма доказана.

Покажем, что, порождая, как это было определено выше, из регулярных событий сверхсобытия, мы получаем также представимые сверхсобытия.

Введем вспомогательное понятие. Пусть R — некоторое событие, $R\subseteq A^*$, $\mathfrak{A}_q=(A,\ Q,\ B,\ \varphi,\ \psi,\ q)$ — конечный автомат и α^∞ — сверхслово из A^∞. Будем говорить, что $\mathfrak{A}_q$ **R-устойчив по отношению** к α^∞, если существует бесконечно много слов $\alpha_1^{k_1}, \alpha_2^{k_2}, \ldots$, $k_1<k_2<\ldots$ из события R, таких, что $\alpha^\infty=\alpha_i^{k_i}\gamma_i\beta_i^\infty$; $i=1,\ 2,\ \ldots$, и для слов γ_i; $i=1,\ 2,\ \ldots$ имеем $\varphi(q,\alpha_i^{k_i}\gamma_i)=\varphi(q,\gamma_i)$. Обозначим через $U(R,\ \mathfrak{A}_q)$ множество всех сверхслов, по отношению к которым $\mathfrak{A}_q$ R-устойчив.

Лемма 4.3. Пусть R — регулярное событие, $R\subseteq A^*$, $R^*=R$ и $\mathfrak{A}_q$ — автомат, представляющий R с помощью B_1. Тогда

$$R^\infty=O_R[U(R,\ \mathfrak{A}_q)]\cup U(R,\ \mathfrak{A}_q).$$

Доказательство. 1. Пусть $\alpha^\infty\in U(R,\ \mathfrak{A}_q)$. Можно считать, что последовательность $k_1, k_2, \ldots$ выбрана так, что $\alpha_{i+1}^{k_{i+1}}=\alpha_i^{k_i}\gamma_i\delta_i$, $\delta_i\in A^*$. Для всех i имеем $\varphi(q,\alpha_i^{k_i}\gamma_i)=\varphi(q,\gamma_i)$, отсюда $\psi(q,\alpha_{i+1}^{k_{i+1}})=$ $=\psi(q,\alpha_i^{k_i}\gamma_i\delta_i)=\psi\varphi(q,\alpha_i^{k_i}\gamma_i)\,\delta_i)=\psi(\varphi(q,\gamma_i),\delta_i)=\psi(q,\gamma_i\,\delta_i)$. Так как $\psi(q,\alpha_{i+1}^{k_{i+1}})\in B_1$, то $\psi(q,\ \gamma_i\delta_i)\in B_1$, следовательно, $\gamma_i\delta_i\in R$. Поэтому сверхслово α^∞ можно представить в виде $\alpha^\infty=\alpha_1^{k_1}\gamma_1\delta_1\gamma_2\delta_2\gamma_3\delta_3\ldots$, где $\gamma_i\delta_i\in R$, т. е. $\alpha^\infty\in R^\infty$. Но тогда для любого слова r, $r\in R$, $r\alpha^\infty$ также принадлежит R^∞. Таким образом, $O_R[U(R,\ \mathfrak{A}_q)]\subseteq R^\infty$.

2. Пусть теперь $\alpha^\infty\in R^\infty$. Тогда $\alpha^\infty=r_1r_2r_3\ldots$, $r_i\in R$, $i=1,\ 2,\ \ldots$. Пусть δ_i^∞ — сверхслово, такое, что $\alpha^\infty=r_1r_2\ldots r_i\delta_i^\infty$, т. е. $\delta_i^\infty=$ $=r_{i+1}r_{i+2}\ldots$. Если можно указать бесконечную последовательность индексов $i_1,\ i_2,\ \ldots$, такую, что $\varphi(q,r_1\ldots r_{i_s}\beta_{i_s})=\varphi(q,\ \beta_{i_s})$, где β_{i_s} — начало сверхслова $\delta_{i_s}^\infty$, то, в силу равенства $R^*=R$, $\alpha^\infty\in$ $\in U(R,\ \mathfrak{A}_q)$.

Предположим, что начиная с некоторого i_1 для любого $i\geqslant i_1$ и любого начала β_i сверхслова δ_i^∞ имеет место $\varphi(q,\ r_1\ldots r_i\beta_i)\neq$ $\neq\varphi(q,\ \beta_i)$. Рассмотрим сверхслово $\delta_{i_1}^\infty$. Повторяя для него рассуждения проведенные для α^∞, получим, что либо $\delta_{i_1}^\infty\in U(R,\mathfrak{A}_q)$

и тогда $\alpha^\infty \in O_R[U(R, \mathfrak{A}_q)]$, либо начиная с некоторого $i_2 > i_1$ для любого $i > i_2$ и любого начала β_i сверхслова δ_i^∞ будем иметь $\varphi(q, r_{i_1+1} \ldots r_i\beta_i) \neq \varphi(q, \beta_i)$. В силу предположения об i_1 имеем одновременно:

$$q^1 = \varphi(q, r_1 \ldots r_{i_1} \ldots r_{i_2}\beta_{i_2}) \neq \varphi(q, r_{i_1} r_{i_1+1} \ldots r_{i_2}\beta_{i_2}) = q^2,$$

$$q^1 = \varphi(q, r_1 \ldots r_{i_1} \ldots r_{i_2}\beta_{i_2}) \neq \varphi(q, \beta_{i_2}) = q^3,$$

$$q^2 = \varphi(q, r_{i_1} r_{i_1+1} \ldots r_{i_2}\beta_{i_2}) \neq \varphi(q, \beta_{i_2}) = q^3.$$

Таким образом, автомат $\mathfrak{A}_q$ имеет по крайней мере 3 различных состояния q^1, q^2, q^3, которые мы можем ассоциировать с i_1 и i_2.

Пусть уже показано, что $\mathfrak{A}_q$ имеет по крайней мере l различных состояний, ассоциированных с номерами $i_1, i_2, \ldots, i_{l-1}$ Рассмотрим $\delta_{i_{l-1}}^\infty$. Либо оно принадлежит $U(R, \mathfrak{A}_q)$, и лемма доказана, либо начиная с i_l для любого начала β_{i_l} сверхслова $\delta_{i_l}^\infty$ имеем:

$$q^1 = \varphi(q, r_1 \ldots r_{i_l}\beta_{i_l}) \neq \varphi(q, \beta_{i_l}) = q^{l+1} \text{ (свойство } \alpha^\infty),$$

$$q^2 = \varphi(q, r_{i_1} \ldots r_{i_l}\beta_{i_l}) \neq \varphi(q, \beta_{i_l}) = q^{l+1} \text{ (свойство } i_1),$$

. . . .

$$q^l = \varphi(q, r_{i_{l-1}} \ldots r_{i_l}\beta_{i_l}) \neq \varphi(q, \beta_{i_l}) = q^{l+1} \text{ (свойство } i_{l-1}).$$

Принимая в качестве индуктивного предположения, что $q^i \neq q^j$; $i, j \leqslant l$; $i \neq j$, получим, что $\mathfrak{A}_q$ должен иметь по крайней мере $l+1$ состояние. В силу конечности автомата, на некотором шаге получим $\delta_i^\infty \in U(R, \mathfrak{A}_q)$. Лемма доказана.

Лемма 4.4. В условиях леммы 3 сверхсобытие $U(R, \mathfrak{A}_q)$ представимо.

Доказательство. Пусть объект $(A, Q, B, \varphi, \psi, q, B_1)$ представляет событие R, $|Q| = n$; $Q' = Q \cup \{\Lambda\}$, $\Lambda \notin Q$, буква $*$ не принадлежит множеству Q'. Пусть $v : [Q']^n \to [Q']^n$ — отображение, определенное в доказательстве леммы 2. Рассмотрим отображение $w : [Q']^{n+1} \times \{\Lambda, *\} \to [Q']^{n+1} \times \{\Lambda, *\}$. Если $T = (t_1, t_2, \ldots, t_{n+2})$; $t_i \in Q'$, $i \leqslant n+1$, $t_{n+2} \in \{\Lambda, *\}$, и для некоторого $i > 1$, $t_1 = t_i$, то

$$w(t_1, t_2, \ldots, t_{n+1}, t_{n+2}) = (t_1, \Lambda, \ldots \Lambda, *).$$

В противном случае

$$w(t_1, t_2, \ldots, t_{n+1}, t_{n+2}) = (t_1, v(t_2, \ldots, t_{n+1}), \Lambda).$$

Рассмотрим автомат $\mathcal{D}_{T_0} = (A, \mathcal{T}, \{0, 1\}, \varphi', \psi', T_0)$, где $\mathcal{T} = [Q']^{n+1} \times \{\Lambda, *\}$, $T_0 = (q, \Lambda, \ldots, \Lambda)$, а функции φ', ψ' определены следующим образом. Пусть $T = (t_1, t_2, \ldots, t_{n+1}, t_{n+2})$ и i — наименьший номер, такой, что $t_i = \Lambda$. Тогда

$$\varphi^i(T, a) = w[\varphi(t_1, a), \ldots, \varphi(t_{i-1}, a), \xi, \varphi(t_{i+1}, a), \varphi(t_{n+1}, a), t_{n+2}],$$

считая, что

$$\varphi(\Lambda, a) = \Lambda \text{ и } \xi = \begin{cases} q, & \text{если } \psi(t_1, a) \in B_1 \\ \Lambda & \text{в противном случае;} \end{cases}$$

$$\psi'(T, a) = 0 \Leftrightarrow t_{n+2} = *.$$

Покажем, что объект $(\mathcal{D}_{T_0}\{0\}, \{0, 1\})$ представляет сверхсобытие $U(R, \mathfrak{A}_q)$. Заметим, что сверхслово α^∞ представимо в этом объекте тогда и только тогда, когда выходное сверхслово содержит бесконечно много нулей.

а) Пусть $\alpha^\infty \in U(R, \mathfrak{A}_q)$. Тогда нетрудно видеть, что каждая пара $\alpha_i^{k_i}, \beta_i$ (см. определение множества $U(R, \mathfrak{A}_q)$) порождает в некоторый момент равенство $t_1 = t_j$, $j > 1$, так как $\psi(q, \alpha_i^{k_i}) \in B_1$ и, следовательно, $\xi \neq \Lambda$, а $t_1 = \varphi(q, \alpha_i^{k_i}\beta_i) = \varphi(q, \beta_i) = t_{j'}$, $j' > 1$. Поэтому на выходе $\mathcal{D}_{T_0}$ бесконечно много раз возникает буква 0.

б) Пусть выходная последовательность содержит бесконечно много нулей. Рассмотрим два момента d_1, d_2, в которые появляются нули. При появлении первого нуля $\mathcal{D}_{T_0}$ перейдет из состояния $(t_1, \Lambda, \ldots, \Lambda, *)$ в некоторое другое состояние T. Теперь новая непустая компонента у вектора T появится лишь в случае, если α^∞ имеет начало $\alpha^{d'}$, $d' > d_1$, такое, что $\psi(q, \alpha^{d'}) \in B_1$. Кроме того, чтобы значения t_1 и t_i совпали, α^∞ должно иметь начало $\alpha^{d'}\beta$, такое, что $\varphi(q, \alpha^{d'}\beta) = \varphi(q, \beta)$. В противном случае в момент d_2 не появится 0 на выходе. Таким образом, $\mathfrak{A}_q$ R-устойчив по отношению к α^∞. Лемма доказана.

Лемма 4.5. Если R — регулярное событие, то сверхсобытие R^∞ представимо.

Доказательство следует из лемм 4.2, 4.3, 4.4. Из лемм 4.1, 4.2, 4.5 непосредственно вытекает представимость произвольного общерегулярного события. Покажем, что имеет место и обратное утверждение. Для этого воспользуемся некоторыми фактами, доказанными в § 1 гл. III, и докажем ряд вспомогательных утверждений.

Пусть на $A = \{a_1, \ldots, a_m\}$ задано бинарное отношение R. Как было ранее показано, множество всех R-слов из A^*, начинающихся с некоторой буквы $a \in A$ и оканчивающихся буквой $b \in A$, регулярно.

Лемма 4.6. Множество всех R-слов, начинающихся с a и кончающихся b, каждое из которых содержит все буквы подалфавита A_1 алфавита A, регулярно.

Доказательство. Пусть $A^1, A^2, \ldots, A^l$ — все собственные подалфавиты алфавита A, не содержащие целиком алфавита A_1, но содержащие как a, так и b. Обозначим через $S, S^1, \ldots, S^l$ множества всех R-слов, начинающихся с a, кончающихся буквой b в алфавитах $A, A^1, \ldots, A^l$ соответственно. Рассмотрим последовательность множеств: $C_1 = S \setminus S^1$, $C_2 = C_1 \setminus S^2$, $\ldots$, $C_l = C_{l-1} \setminus S^l$. Каждое из множеств $S, S^1, \ldots, S^l$ регулярно и по теореме Клини является представимым. Если множество C_{i-1} представимо объектом $(\mathfrak{A}_q, B_1)$, а множество S^i — объектом $(\mathfrak{A}'_{q'}, B'_1)$, то множество $C_i = C_{i-1} \setminus S^i$ представимо, очевидно, объектом $(\mathfrak{A}_q \times \mathfrak{A}'_{q'}, B_1 \times (B' \setminus B'_1))$, где B' — выходной алфавит автомата $\mathfrak{A}'_{q'}$. Поэтому все множества C_1, ..., C_l представимы и в силу теоремы Клини регулярны. Нетрудно видеть, что C_l есть множество, удовлетворяющее условию леммы. Лемма доказана.

Рассмотрим объект $(A, Q, B, \varphi, \psi, q, B_1, B_2, \ldots, B_k)$; $B_i \subseteq B$; $i = 1, 2, \ldots, k$; $Q = \{q_1, q_2, \ldots, q_n\}$. Для произвольных $i, j \in \{1, \ldots n\}$, $s \in \{1, 2, \ldots, k\}$ рассмотрим множество слов R^s_{ij} из $A^* : R^s_{ij} = \{\alpha \in A^* \mid \varphi(q_i, \alpha) = q_j, \overline{\varphi}(q_i, \alpha) \in B^*_s$ и слово $\psi(q_i, \alpha)$ содержит все буквы $B_s\}$.

Лемма 4.7. Множества R^s_{ij}; $i, j = 1, \ldots, n$; $s = 1, \ldots, k$ регулярны.

Доказательство. Рассмотрим множество $\mathcal{T}$ троек (a, q, b), таких, что $\psi(q, a) = b$, $a \in A$, $q \in Q$, $b \in B_s$. На множестве $\mathcal{T}$ зададим бинарное отношение R, такое, что $(a, q, b) R (a', q', b')$ тогда и только тогда, когда $\varphi(q, a) = q'$. Пусть $\mathcal{T}_1, \ldots \mathcal{T}_d$ — все подалфавиты алфавита $\mathcal{T}$, такие, что $pr^3(\mathcal{T}_1) = \ldots = pr^3(\mathcal{T}_d) = B_s$. Тогда для любых троек $t = (a, q_i, b)$, $t' = (a', q_j, b')$ из $\mathcal{T}$ множество $V_l(aa')$ всех R-слов, начинающихся с t, кончающихся t' и содержащих все буквы множества $\mathcal{T}_l$ $(l = 1, \ldots, d)$, является регулярным. Поэтому регулярно и множество $V = \bigcup\limits_{a, a'} \bigcup\limits_{l=1}^{d} V_l(a, a')$. Нетрудно видеть, что $P^s_{ij} = pr^1(V)$. Лемма доказана.

Пусть E, $E \subseteq A^\infty$, — представимое множество сверхслов и объект $(A, Q, B, \varphi, \psi, q, B_1, \ldots, B_k)$ представляет E, $Q = \{q_1, q_2, \ldots, q_n\}$. Докажем общерегулярность множества E. Очевидно, что $E = \bigcup\limits_{i=1}^{k} E_i$, где множество E_i представимо объектом $(A, Q, B, \varphi, \psi, q, B_i)$. Пусть $\alpha^\infty \in E_i$. Сверхслово α^∞ порождает в автомате $\mathfrak{A}_q$ сверхслово состояний $q^\infty = q(1) q(2) \ldots$, и пусть $\lim q^\infty = Q_j \subseteq Q$. Подавая разные сверхслова из E_i на автомат, мы будем получать сверхслова состояний с теми или иными пределами. Пусть $Q^i_1, \ldots, Q^i_{s_i}$ — всевозможные пределы, полученные таким образом. Обозначим через $E_i{}^j$, $E_i{}^j \subseteq E_i$, множество всех сверхслов, породивших сверхслова состояний с пределом Q^i_j, $Q^i_j = \{q^1_{ij}, \ldots, q^{n_{ij}}_{ij}\}$. Для каждого сверхслова α^∞ из $E_i{}^j$ можно указать бесконечную последовательность множеств слов $M_i = \{\alpha^i_{12}, \alpha^i_{23}, \ldots, \alpha^i_{n_{ij}1}\}$ и слово α_0, такие, что $\varphi(q, \alpha_0) = q^1{}_{ij}$ и для всех $l = 1, 2, \ldots$

$$\varphi(q^d_{ij}, \alpha^l_{d\,d+1}) = q^{d+1}_{ij}, \; d = 1, 2, \ldots, n_{ij} - 1, \; \varphi(q^{n_{ij}}_{ij}, \alpha^l_{n_{ij}\,1}) = q^1_{ij},$$

причем α^∞ представляется в виде:

$$\alpha^\infty = \alpha_0 \alpha^1_{12} \alpha^1_{23} \ldots \alpha^1_{n_{ij}1} \alpha^2_{12} \ldots \alpha^2_{n_{ij}1} \alpha^3_{12} \ldots .$$

Заметим, что при этом слова $\alpha^l{}_{ss'}$, где $s' = s+1$ при $s \neq n_{ij}$ и $s' = 1$ при $s = n_{ij}$ можно выбрать так, что (в силу $\alpha^\infty \in E_i$) $\overline{\psi}(q^s_{ij}, \alpha^l_{ss'}) \in B^*$

и содержит все буквы из B_i. Таким образом, теперь каждое слово $\alpha^l_{ss'}$ переводит автомат из состояния q^s_{ij} в состояние q^{s+1}_{ij} и порождает на выходе слово, содержащее все буквы B_i. Поэтому $\alpha^l_{ss'} \in R^i_{i'j'}$, где $q^s_{ij} = q_{i'}$; $q^{s'}_{ij} = q_{j'}$; $i', j' \in \{1, \ldots, n\}$. Множество $R_{i'j'}^{i}$ далее обозначаем $R^i_{i,j,s,s'}$. Имеем $\alpha^\infty \in \alpha_0 \cdot (R^i_{i,j,1,2} \cdot R^i_{i,j,2,3} \times \times \ldots \cdot R^i_{i,j,n_{ij},1})^\infty$. Если обозначить через H^1_{ij} множество слов $\{\alpha_0 | \varphi(q, \alpha_0) = q^1_{ij}\}$, которое, очевидно, является регулярным, то

$$E^j_i \subseteq H^1_{ij} \cdot (R^i_{i,j,1,2} \cdot R^i_{i,j,2,3} \cdot \ldots \cdot R^i_{i,j,n_{ij},1})^\infty \subseteq E_i.$$

Последнее включение имеет место, так как каждое сверхслово из $H^1_{ij} \cdot (R^i_{i,j,1,2} \cdot \ldots \cdot R^i_{i,j,n_{ij},1})^\infty$ порождает на выходе такое сверхслово β^∞, что $\lim \beta^\infty = B_i$. Заметим, что, вообще говоря, сверхслово из $H^1_{ij} \cdot (R^i_{i,j,1,2} \cdot \ldots \cdot R^i_{i,j,n_{ij},1})^\infty$ порождает сверхслово состояний, предел которого содержит, а не в точности совпадает с множеством Q^i_j). В заключение имеем

$$E_i \subseteq \bigcup_{j=i}^{s_i} E^j_i \subseteq \bigcup_{j=1}^{s_i} H^1_{ij} \cdot (R^i_{i,j,1,2} \cdot \ldots \cdot R^i_{i,j\, n_{ij},1})^\infty \subseteq E_i.$$

Отсюда E_i, $i = 1, \ldots k$, — общерегулярные множества, а вместе с ними $E = \bigcup_{i=1}^{k} E_i$ — общерегулярно. Теорема доказана

УПРАЖНЕНИЯ

1. Представимо ли сверхсобытие, состоящее из всех периодических сверхслов в алфавите $A = \{0, 1\}$?
2. Построить автомат, представляющий с помощью некоторого набора множеств общерегулярное сверхсобытие: $(\{10, 01\})^* \cdot (\{01\} \cup \cup \{0\}^*)^\infty$. Каково наименьшее возможное число состояний такого автомата?
3. Выразить посредством операций $\cup$, $\cdot$, $*$, ∞, O_R сверхсобытие, представимое при помощи набора $\{\{1\}\}$ автоматом $\mathfrak{A}$, диаграмма которого указана на рис. 1 30.

§ 2. КОНЕЧНЫЕ АВТОМАТЫ КАК ПЕРЕЧИСЛИТЕЛИ

В этом параграфе в качестве характеристики функционирования конечных автоматов изучаются множества слов, возникающих на выходе автомата при подаче на него произвольных входных последовательностей.

Пусть B — конечный алфавит; B^* — множество слов в этом алфавите. Множество $\mathscr{D} \subseteq B^*$ называется **автоматно-перечислимым** (или перечислимым конечным автоматом), если существует инициальный конечный автомат $\mathfrak{A} = (A, Q, B, \varphi, \psi, q_0)$, такой, что для любого $\beta \in \mathscr{D}$ существует слово α в алфавите A, такое, что

$\psi(q_0, \alpha)=\beta$ и для любого $\alpha\in A^*$ $\bar{\psi}(q_0, \alpha)\in\mathscr{D}$. Справедливо следующее утверждение.

Теорема 4.2. Пусть B — конечный алфавит. Множество $\mathscr{D}\subseteq B^*$ автоматно перечислимо тогда и только тогда, когда это множество регулярно и обладает следующими свойствами:

а) если слово принадлежит $\mathscr{D}$, то любое его собственное начало также принадлежит $\mathscr{D}$;

б) если слово β длины p принадлежит $\mathscr{D}$, то существует слово β' из $\mathscr{D}$, длина которого равна $p+1$ и такое, что его собственное начало длины p совпадает со словом β.

Доказательство. Пусть множество $\mathscr{D}$ перечислимо в конечном автомате $\mathfrak{A}=(A, Q, B, \varphi, \psi, q_0)$. Рассмотрим диаграмму переходов $\mathscr{D}_{\mathfrak{A}}$ автомата $\mathfrak{A}$. Вычеркнем первую координату в каждой паре, приписанной ребрам этой диаграммы. В результате такого вычеркивания получим некоторый квазиисточник $U_{\mathfrak{A}}$ с начальной вершиной, соответствующей состоянию q_0, и множеством финальных вершин, совпадающим со множеством всех его вершин, который задает событие $\mathscr{D}$. Следовательно, событие $\mathscr{D}$ регулярно. Выполнение условий а) и б) очевидно.

Пусть теперь множество $\mathscr{D}$ регулярно, причем выполнены условия а) и б). Тогда для некоторого источника G с начальной вершиной v_0 и множеством F финальных вершин имеем $\mathscr{D}=|G|$. В силу условия а) F должно совпадать со множеством всех вершин источника G. В силу условия б) из любой вершины источника G выходит не менее одного ребра. Эти свойства источника G позволяют рассматривать его как результат применения к диаграмме некоторого конечного автомата $\mathfrak{A}$ процедуры вычеркивания первых координат пар, сопоставленных ребрам этой диаграммы, с последующей склейкой одинаково отмеченных параллельных ребер Автомат $\mathfrak{A}$ и будет искомым автоматом, перечисляющим множество $\mathscr{D}$.

Рассмотрим еще одну задачу, связанную с распознаванием перечислительных возможностей конечных автоматов. Пусть $\mathfrak{A}=(A, Q, B, \varphi, \psi)$ — некоторый не инициальный конечный автомат. Обозначим $\mathscr{F}(\mathfrak{A})$ множество всех слов $\beta\in B^*$, для которых существуют $q\in Q$ и $\alpha\in A^*$, такие, что $\beta=\psi(q, \alpha)$. Если $\mathscr{F}(\mathfrak{A})=B^*$, то автомат $\mathfrak{A}$ назовем **генератором выходных последовательностей** (или, коротко, просто генератором). Если $\mathfrak{A}$ не является генератором, то обозначим $l(\mathfrak{A})$ длину кратчайшего слова, входящего в $B^*\setminus\mathscr{F}(\mathfrak{A})$. Обозначим также

$$L(m, n, p)=\max_{|A|=m,\ |Q|=n,\ |A|=p} l(\mathfrak{A}),$$

где максимум берется по всем конечным автоматам $\mathfrak{A}$, у которых алфавиты A, Q, B состоят из m, n, p символов соответственно. Очевидно, что автомат с параметрами m, n, p является генератором тогда и только тогда, когда на его выходе можно получить произвольное слово из B^* длины $L(m, n, p)$, и этим обстоятельством можно пользоваться для распознавания автоматов-генераторов. Займемся получением оценок для функции $L(m, n, p)$. Заметим прежде всего, что число слов длины l в $\mathcal{F}(\mathfrak{A})$ не превосходит числа различных выборов $q \in Q$ и $\alpha^l \in A^*$, т. е. не превосходит nm^l. Поэтому если $\mathfrak{A}$ — генератор, то для любого l имеем:

$$(1) \qquad nm^l \geqslant p^l,$$

так что $m \geqslant p$. При $m < p$ $\mathfrak{A}$ не является генератором; в этом случае из (1) находим $L(m, n, p) \leqslant 1 + \left[\frac{\ln n}{\ln p - \ln m}\right]$. С произвольным автоматом $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ свяжем помеченные ориентированные графы $G(\mathfrak{A})$ и $\bar{G}(\mathfrak{A})$. Граф $G(\mathfrak{A})$ имеет своими вершинами элементы Q. Из вершины q_1 ведет ребро к вершине q_2, помеченное символом $b \in B$, если существует такое $a \in A$, что $q_2 = \varphi(q_1, a)$, $b = \psi(q_1, a)$. Допускаются параллельные ребра, помеченные различными символами из B. Вершинами графа $\bar{G}(\mathfrak{A})$ являются всевозможные непустые подмножества множества Q. Пусть $S \subseteq Q$ — вершина графа $\bar{G}(\mathfrak{A})$ и $b \in B$. Рассмотрим множество $b(S)$ вершин графа $G(\mathfrak{A})$, к которым от вершин из S ведут ребра, помеченные символом b. Если $b(S) \neq \varnothing$, то в $\bar{G}(\mathfrak{A})$ от вершины S к вершине $b(S)$ проводится ребро, помеченное символом b. Вершину графа $\bar{G}(\mathfrak{A})$, соответствующую множеству Q, далее обозначаем V_0.

Лемма 4.8. Слово β принадлежит множеству $\mathcal{F}(\mathfrak{A})$ тогда и только тогда, когда в графе $\bar{G}(\mathfrak{A})$ существует начинающийся с вершины V_0 маршрут, отметки ребер которого образуют слово β.

Доказательство. Пусть $\beta = b(1)b(2)\ldots b(l)$. Заметим, что $b(1)(V_0)$ есть множество всех состояний, в которых может оказаться $\mathfrak{A}$ после того, как на его выходе появилась буква $b(1)$; $b(2)(b(1)(V_0))$ — множество состояний, в которых может оказаться $\mathfrak{A}$ после появления на выходе слова $b(1)b(2)$, и т. д. Таким образом, непустота множества $b(l)(b(l-1)(\ldots(b(1)(V_0)\ldots)$, с одной стороны, означает, что слово β может быть получено на выходе автомата $\mathfrak{A}$, т. е. $\beta \in \mathcal{F}(\mathfrak{A})$, а с другой стороны, эквивалентна существованию в графе $\bar{G}(\mathfrak{A})$ маршрута указанного вида.

Теорема 4.2 [20]. Имеет место неравенство $L(m, n, p) \leqslant 2^n - 1$.

Доказательство. Пусть автомат $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, $|A| = m$, $|Q| = n$, $|B| = p$, не является генератором. Рассмотрим кратчайшее слово β, входящее в $B^* \setminus \mathcal{F}(\mathfrak{A})$. Очевидно, слово $\beta' = b(1)\ldots$ $\ldots b(l(\mathfrak{A})-1)$ принадлежит $\mathcal{F}(\mathfrak{A})$. В силу леммы в графе $\bar{G}(\mathfrak{A})$ существует маршрут $V_0, x_1, V_1, x_2, \ldots, x_{l(\mathfrak{A})-1}, V_{l(\mathfrak{A})-1}$, отметки ребер которого образуют слово β', причем из вершин $V_{l(\mathfrak{A})-1}$ не выходит ребра, отмеченного символом $b(l(\mathfrak{A}))$. Легко видеть, что этот маршрут является кратчайшим маршрутом от V_0 к вершинам графа $\bar{G}(\mathfrak{A})$, из которых ведут ребра, отмеченные не всеми символами алфавита B. В таком маршруте должны отсутствовать циклы, так что все вершины $V_0, V_1, \ldots, V_{l(\mathfrak{A})-1}$ различны и имеем неравенство $l(\mathfrak{A}) \leqslant 2^n - 1$, где $2^n - 1$ — число вершин в графе $\bar{G}(\mathfrak{A})$, что и доказывает теорему.

Теорема 4.3 [20]. Пусть $p \geqslant n$, $m \geqslant p+n-2$. Тогда

$$L(m, n, p)=2^n-1.$$

Доказательство. Построим граф $G(\mathfrak{A})$ некоторого автомата $\mathfrak{A}=(A, Q, B, \varphi, \psi)$ с $|A|=m$, $|Q|=n$ и $|B|=p$. Пусть $Q=\{q_1, ..., q_n\}$, $B=\{b_1, ..., b_p\}$. Ребра графа $G(\mathfrak{A})$ таковы.

а) Ребра, помеченные b_j, где $1 \leqslant j \leqslant n$:

$$(q_i, q_i) \text{ при } j<n,\ j+1 \leqslant i \leqslant n,$$

$$\left.\begin{matrix}(q_i, q_j)\\(q_j, q_i)\end{matrix}\right\} \text{ при } j>1,\ 1 \leqslant i \leqslant j-1;$$

б) ребра, помеченные b_j, где $n+1 \leqslant j \leqslant p$:

$$(q_i, q_i) \text{ при } 1 \leqslant i \leqslant n.$$

На рис. 4.1 указан $\bar{G}(\mathfrak{A})$ для $p=n=3$, $m=4$.

Сопоставим произвольной вершине $V=\{q_{i_1},...,p_{i_s}\}$ графа $\bar{G}(\mathfrak{A})$ $|i_1<...<i_s|$ номер $N(V)$: $N(V)=\sum\limits_{i=1}^{n} 2^{i-1}\sigma_i$,

где $\sigma_i=1$, если $q_i \in V$ и $\sigma_i=0$ в противном случае. Заметим, что наибольший номер 2^n-1 имеет вершина $V_0=\{q_1, ..., q_n\}$, а наименьший, равный 1, — вершина $V^*=\{q_1\}$. Пусть V — некоторая вершина графа $\bar{G}(\mathfrak{A})$, имеющая номер $N(V)>1$. Тогда $V=\{q_{i_1}, \ldots, q_{i_s}\}$, где $i_1<...<i_s$, $s \geqslant 1$, $i_s>1$. Так как в графе $G(\mathfrak{A})$ для любого b_i из вершины q_{is} при $i_s>1$ ведет ребро с отметкой b_i, то для любого b_i и в графе $\bar{G}(\mathfrak{A})$ из V выходит ребро с отметкой b_i. Покажем, что при $i \neq i_1$ выполняется $N(b_i(V)) \geqslant N(V)$, а при $i=i_1$ $N(b_i(V))=N(V)-1$. Если $i>n$,

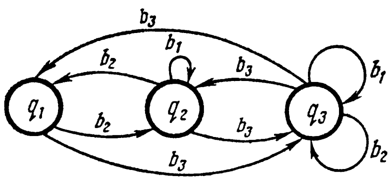

Рис. 4.1

то, как легко проверить, $b_i(V)=V$, и это утверждение верно. Точно так же $b_i(V)=V$ при $i<i_1$. Если $i_1<i \leqslant n$, то рассмотрим два случая: $q_i \notin V$ *и* $q_i=q_{i_p}$. В первом случае $в_i(V)=\{q_i, q_{i_r}, \ldots, q_{s^{s^i}}\}$ где r — наименьшее, для которого $i_r>i$. Ясно, что в этом случае выполняется $N(b_i(V))>N(V)$. Во втором случае

$$b_i(V)=\{q_1, q_2, \ldots, q_{i_p}, q^t{}_{p+1}, \ldots, q_{i_s}\},$$

и снова $N(b_i(V)) \geqslant N(V)$. Если, наконец, $i=i_1$, то $b_i(V)=\{q_1, \ldots, \ldots, q_{i_1-1}, q_{i_2}, \ldots, b_{si}\}$ и $N(b_i(V))=N(V)-1$. Из доказанного утверждения вытекает, что для получения кратчайшего маршрута $v_0, x_1, V_1, ..., x_l, V_l=V^*$, соединяющего вершину V_0 графа $\bar{G}(\mathfrak{A})$ с вершиной V^*, на каждом шаге ребро x_i следует выбирать так, чтобы выполнялось $N(V_i)=N(V_{i-1})-1$, при этом длина маршрута l равна 2^n-2. Пусть $b_{i1}, ..., b_{il}$ — отметки ребер этого маршрута, тогда, так как в $\bar{G}(\mathfrak{A})$ из вершины V^* не выходит ребра с отметкой b_1, слово $b_{i_1}b_{i_2}\ldots b_{i_l}b_1$ не принадлежит $\mathcal{F}(\mathfrak{A})$, и $\mathfrak{A}$ — не генератор. Очевидно, что построенное слово является кратчайшим в $B^* \setminus \mathcal{F}(\mathfrak{N})$, т. е. $l(\mathfrak{A}) = 2^n - 1$. Но $L(m, n, p) \geqslant l(\mathfrak{A})$, так что, учитывая теорему 2.15, получаем $L(m, n, p) = 2^n - 1$, что и требовалось доказать.

В случае $p < n$ нижняя оценка для $L(m, n, p)$ устанавливается значительно сложнее, чем в теореме 2.16, причем снова оказывается, что $L(m, n, p)$ — величина, близкая к 2^n:

Теорема 4.4 [20]. Пусть $p \geqslant 12$, $p < n$ и $m \geqslant p + 16\left[\frac{p-3}{9}\right]^2$. Тогда $L(m, n, p) > 2^n\left(1 - 2^{1-\left[\frac{p-3}{9}\right]}\right)$.

Доказательство. Пусть параметры m, n, p удовлетворяют условиям теоремы. Построим, как и при доказательстве теоремы 2.16, граф $G(\mathfrak{A})$ некоторого автомата $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, такого, что $|A| = m$, $|Q| = n$, $|B| = p$. Положим: $B = \{b_1, \ldots, b_p\}$, $Q = \{q\} \cup \bigcup_{i=1}^{r} Q_i$, где $Q_0 = \{q_{01}, \ldots, q_{0t}\}$; $Q_i = \{q_{i1}, \ldots, q_{ih}\}$ при $1 \leqslant i \leqslant r$. Здесь $h = 2\left[\frac{p-3}{9}\right] \geqslant 2$; $r = \left[\frac{n-1}{h}\right] - 1 \leqslant 3$, $t = h + s$, где s — остаток от деления $n-1$ на h. Очевидно, $t < 2h = 4\left[\frac{p-3}{9}\right]$. Ребра графа $G_{\mathfrak{A}}$ таковы:

а) Ребра, помеченные символом b_1:
(q, q_{rk}) при $2 \leqslant k \leqslant h$; (q_{ij}, q_{rk}) при любых допустимых i и j и $2 \leqslant k \leqslant h$;

б) ребра, помеченные b_2:
(q, q_{rk}) при $2 \leqslant k \leqslant h$; $(q_{ij}, q_{i-1\,j})$ при $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant h$; (q_{0i}, q_{rj}) при $1 \leqslant i \leqslant t$, $2 \leqslant j \leqslant h$; (q_{ik}, q_{rj}) при $1 \leqslant i \leqslant r$, $1 \leqslant k \leqslant h$, $1 \leqslant j \leqslant l$;

в) ребра, помеченные b_j $(3 \leqslant j \leqslant t+2)$:
(q, q_{rk}) при $2 \leqslant k \leqslant h$; (q_{0k}, q_{0k}) при $j < t+2$, $j-1 \leqslant k \leqslant t$; $(q_{0k}, q_{0\,j-2})$ при $j > 3$, $1 \leqslant k \leqslant j-3$; (q_{ik}, q_{ik}) при $1 \leqslant i \leqslant r$, $1 \leqslant k \leqslant h$; $(q_{0\,j-2}, q_{0k})$ при $j > 3$, $1 \leqslant k \leqslant j-3$; (q_{ik}, q) при $1 \leqslant i \leqslant r$, $1 \leqslant k \leqslant h$;

г) ребра, помеченные $b_j (t+3 \leqslant j \leqslant 2t+2)$:
(q, q_{rk}) при $2 \leqslant k \leqslant h$; (q_{0k}, q_{0k}) при $j \leqslant 2t+2$, $j-t-1 \leqslant k \leqslant t$; $(q_{0k}, q_{0\,j-t-2})$ при $j > t+3$, $1 \leqslant k \leqslant j-t-3$; $(q_{0\,j-t-2}, q_{0k})$ при $t+3 \leqslant j < l+t+3$, $1 \leqslant k \leqslant j-t-3$, а также при $1 \leqslant i \leqslant r$, $1 \leqslant k \leqslant h$; (q_{ik}, q_{ik}) при $1 \leqslant i \leqslant r$, $1 \leqslant k \leqslant l$; (q_{ik}, q_{ru}) при $1 \leqslant i \leqslant r$, $l+1 \leqslant k \leqslant h$, $2 \leqslant u \leqslant l$;

д) ребра, помеченные b_{2t+3}:
(q, q); $(q_{ik}, q_{i+1\,k})$ при $1 \leqslant i \leqslant r-1$, $1 \leqslant k \leqslant h$; (q_{ri}, q_{rk}) при $l+1 \leqslant i \leqslant h$, $2 \leqslant k \leqslant h$; (q_{ik}, q_{0j}) при $0 \leqslant i \leqslant r$, $1 \leqslant j \leqslant t$, $1 \leqslant k \leqslant h$.

е) ребра, помеченные b_j $(2t+4 \leqslant j \leqslant 2t+l+3)$:
(q_{ik}, q_{ik}) при любых i и k; $(q_{r,\,j-2t-3}, q_{ri})$ при $2 \leqslant i \leqslant h$;

ж) ребра, помеченные b_j $(2t+l+4 \leqslant j \leqslant p)$:
(q, q); (q_{ik}, q_{ik}) при любых i и k.

Здесь $l = \left[\frac{p-3}{9}\right]$, т. е. $1 \leqslant l < h$. Имеем:

$$2t + l + 3 < 9\left[\frac{p-3}{9}\right] + 3 \leqslant p.$$

Можно проверить, что из каждой вершины графа $G_{\mathfrak{A}}$ выходит не менее одного и не более $p+2th$ ребер. Но $p+2th \leqslant p+16\left[\frac{p-3}{9}\right]^2 \leqslant m$, так что автомат $\mathfrak{A}$ с параметрами m, n, p, определяющий данный граф $G_{\mathfrak{A}}$, действительно существует.

Занумеруем все подмножества множества Q_i $(0 \leqslant i \leqslant r)$. А именно, если $P \subseteq Q_i$, то положим $M(P) = \sum_{j=1}^{|Q_i|} 2^{j-1}\gamma_j$, где $|Q_i|$ — число элементов в Q_i, γ_j есть 1 при $q_{ij} \in P$ и $\gamma_j = 0$ в противном случае. Далее, занумеруем все подмножества множества $Q \setminus \{q\}$. Если $P = \bigcup_{i=0}^{r} R_i$, $R_i \subseteq Q_i$, то $N(P) = \sum_{i=0}^{r} 2^{\mu_i} M(R_i)$, где $\mu_0 = 0$, а при $i \geqslant 1$ $\mu_j = \sum_{k=0}^{r-1} |Q_k|$. Нетрудно проверить следующие свойства операторов $b_j(P)$.

а) Для любого $P \subseteq Q$, $P \neq \varnothing$ имеем: $b_1(P) = \{q_{r2}, \ldots, q_{rh}\}$.

б) Если $q \in P$ или $q_{0i} \in P$, то $b_2(P) \supseteq \{q_{r2}, \ldots, q_{rh}\}$. Если эти включения не выполнены, то $b_2(P) = P' \cup \{q_{r1}, \ldots, q_{rl}\}$, где P' состоит из всех таких q_{ij}, что $q_{i+1\, j} \in P$.

в) пусть $3 \leqslant j \leqslant t+2$. Если $q \in P$, то $b_j(P) \supseteq \{q_{r2}, \ldots, q_{rh}\}$. Пусть $q \notin P$ и $P = P_1 \cup P_2$, где $P_1 \subseteq Q_0$, $P_2 \subseteq \bigcup_{i=1}^{r} Q_i$. Пусть $b_j(P) = P_1' \cup P_2' \neq \neq \varnothing$, где $P_1' \subseteq Q_0$, $P_2' \subseteq Q \setminus Q_0$. Если $P_i = \varnothing$, то и $P_i' = \varnothing$. Пусть $P_2 \neq \varnothing$. Тогда $P_2' = P_2 \cup \{q\}$. Пусть $P_1 \neq \varnothing$. Представим P_1 в виде $\{q_{0i_1}, \ldots, q_{0i_s}\}$, где $i_1 < i_2 < \ldots < i_s$. Как и при доказательстве предыдущей теоремы, можно убедиться, что $M(P_1') < M(P_1)$ лишь при $j = i_1 + 2$, причем в этом случае $M(P_1') = M(P_1) - 1$.

г) Пусть $t+3 \leqslant j \leqslant 2t+2$. Если $q \in P$ либо $q_{ik} \in P$ при $i \geqslant 1, k \geqslant l+1$, то $b_j(P) \supseteq \{q_{r2}, \ldots, q_{rh}\}$. Если эти включения не выполнены, то представим P в виде $P_1 \cup P_2$, где $P_1 \subseteq Q_0, P_2 \subseteq \bigcup_{i=1}^{r} Q_i$. Пусть $b_j(P) = = P_1' \bigcup P_2' \neq \varnothing$, где $P_1' \subseteq Q_0$, $P_2' \subseteq Q \setminus Q_0$. Если $P_i = \varnothing$, то и $P_i' = = \varnothing$. Пусть $P_2 \neq \varnothing$. Тогда $P_2' = P_2 \cup \{q\}$. Пусть $P_1 \neq \varnothing$; $P_1 = \{q_{0i_1}, \ldots \ldots, q_{0i_s}\}$, где $i_1 < i_2 < \ldots < i_s$. Тогда $M(P_1') < M(P_1)$ лишь при $j = t + + i_1 + 2$, причем в этом случае $M(P_1') = M(P_1) - 1$ при $i_1 \leqslant l$, а при $i_1 > l$. $M(P_1') = M(P_1) - 2$.

д) Если $q_{ri} \in P$ при $i \geqslant l+1$, то $b_{2t+3}(P) \supseteq \{q_{r2}, \ldots, q_{rh}\}$. Если же для каждого $i \geqslant l+1$ $q_{ri} \notin P$ и $P \cap \bigcup_{i=1}^{r} Q_i \neq \varnothing$, то $b_{2t+3}(P) = P' \cup \{q_{01}, \ldots \ldots, q_{0t}\} \cup (\{q\} \cap P)$, где P' состоит из таких q_{ij}, что $q_{i-1\, j} \in P$.

е) Пусть $2t+4 \leqslant j \leqslant 2t+l+3$. Тогда $b_j(P) \supset \{q_{r2}, \ldots, q_{rh}\}$, если $q_{r,\, j-2t-3} \in P$, и $b_j(P) = P \setminus \{q\}$ в противном случае.

ж) Если $l+2t+4 \leqslant j \leqslant p$, то $b_j(P) = P$.

Предположим, что $\beta = b(1) \ldots b(k)$ — кратчайшее слово, принадлежащее множеству $B^* \setminus \mathcal{F}(\mathfrak{A})$, и установим, какой вид должно иметь такое слово. Слово $\beta' = b(1) \ldots b(k-1)$ принадлежит множеству $\mathcal{F}(\mathfrak{A})$, так что для него существует начинающийся с вершины $V_0 = Q$ маршрут в графе $\bar{G}(\mathfrak{A})$, отметки ребер которого образуют слово β'; пусть этот маршрут μ есть $V_0, x_1, V_1, \ldots$ $\ldots, x_{k-1}, V_{k-1}$. В силу того, что μ — кратчайший маршрут в $\bar{G}(\mathfrak{A})$, ведущий от вершины V_0 к вершинам, из которых выходят ребра, отмеченные не всеми символами из B, при $i<j$ не может иметь место включение $V_i \subseteq V_j$. Имеем $b_1(V_0) = \{q_{r2}, \ldots, q_{rh}\}$, а при $j \neq 1$ $b_j(V_0) \supset b_1(V_0)$. Поэтому без ограничения общности можно считать, что $b(1) = b_1$; $V_1 = b_1(V_0) = \{q_{r2}, \ldots, q_{rh}\}$. Так как $V_j \neq \varnothing$, то $b_1(V_j) = V_1$, т. е. $b(i) = b_1$ при $i>1$. Кроме того, $b_i(V_j) = V_j$ при $i \geqslant 2t+l+4$, так что $b(j) \neq b_i$ при $i \geqslant 2t+l+4$.

Пусть K — множество всех $P \subseteq Q \setminus \{q\}$, таких, что $\{q_{r1}, \ldots, q_{rl}\} \setminus P_r \neq \varnothing$ и $P_r \setminus \{q_{r1}, \ldots, q_{rl}\} \neq \varnothing$, где $P_r = P \cap Q_r$, причем $N(P) \leqslant N(V_1) = 2^{n-1} - 2^{n-h}$.

Ясно, что число элементов в K равно $2^{n-h-1} \cdot (2^h - 2^{h-l} - 2^l) + 1 = 2^{n-1}(1 - 2^{1-l}) + 1$, причем элемент K с наименьшим номером есть $\{q_{r,l+1}\}$, $N(\{q_{r,l+1}\}) = 2^{n-l-1}$. Пусть $V_i \in K$; $N(V_i) > 2^{n-l-1}$, причем доказано, что каждое $V \in K$ с номером $N(V) \geqslant N(V_i)$ есть V_j при некотором $j \leqslant i$. Для $i=1$ это, очевидно, верно. Положим:

$$V_i = \bigcup_{q=1}^{s} P_{i_q};\quad P_{i_q} \neq \varnothing;\quad P_{i_q} = V_i \cap Q_{i_q};\quad i_1 < \ldots < i_s. \tag{2}$$

Очевидно, $i_s = r$, причем $q_{r\tau} \in V_i$ при некотором $\tau \geqslant l+1$. Пусть $i_1 > 0$. Тогда $V_i \cap Q_0 = \varnothing$, и в силу свойства в) при $3 \leqslant j \leqslant t+2$ имеем $b_j(V_i) = V_i \cup \{q\}$, а так как $q_{r\tau} \in V_i$ при $\tau \geqslant l+1$, то в силу свойства г) при $t+3 \leqslant j \leqslant 2t+2$ имеем $b_j(V_i) \supseteq V_1$. В силу свойства д) $b_{2t+3}(V_i) \supseteq V_1$, а в силу свойства е) при $2t+4 \leqslant j \leqslant 2t+l+3$ либо $b_j(V_i) \supseteq V_1$, либо $b_j(V_i) = V_i$. Итак, при $j \neq 2$ либо $b_j(V_i) \supset V_1$, либо $b_j(V_i) \supseteq V_i$. Поэтому $b(i+1) = b_2$ и V_{i+1} в силу свойства б) есть

$$\bigcup_{q'=1}^{s} P_{i_{q'}}^{(1)} \cup \{q_{r1}, \ldots, q_{rl}\},$$

где $P_{i_{q'}}^{(1)}$ состоит из всех $q_{i_{q'}-1, j}$, таких, что $q_{i_{q'}, j} \in P_{i_{q'}}$. Пусть уже доказано для $a>0$:

$$V_{i+a} = \bigcup_{q=1}^{s} P_{i_q}^{(a)} \cup \bigcup_{\tau=r-a+1}^{r} R_\tau,$$

где $R_\tau = \{q_{\tau_1}, \ldots, q_{\tau_l}\}$, а $P_{i_q}^{(a)}$ состоит из всех $q_{i_q - a, j}$, таких, что $q_{i_q, j} \in P_{i_r}$.

Пусть, кроме того, $i_1 - a > 0$. Тогда при $3 \leqslant j \leqslant t+2$ имеем $b_j(V_{i+a}) \supseteq V_{i+a}$; при $t+3 \leqslant j \leqslant 2t+2$ имеем $b_j(V_{i+a}) \supseteq V_1$; при $j = 2t+3$ имеем $b_j(V_{i+a}) \supseteq V_{i+a-1}$, при $2t+4 \leqslant j \leqslant 2t+l+3$ имеем $b_j(V_{i+a}) \supseteq V_1$. Поэтому $b(i+a-1) = b_2$;

$$V_{i+a+1} = \bigcup_{q=1}^{s} P_{i_q}^{(a+1)} \cup \bigcup_{\tau=r-a}^{r} R_\tau.$$

Таким образом, $b(i+a)=b_2$ при $1 \leqslant a \leqslant i_1$;

(3) $$V_{i+i_1} = \bigcup_{q=1}^{s} P_{i_q}^{(i_1)} \cup \bigcup_{\tau=r-i_1+1}^{r} R_\tau$$

(Заметим, что при $i_1=0$ это равенство тоже верно.)

Пусть сначала $s>1$. Тогда $i_1<r$ и V_{i+i_1} содержит элемент $q_{r-i_1,j}$, для которого $j>l$, так что по свойству г)

$$b_j(V_{i+i_1}) \supseteq V_1 \quad \text{при} \quad t+3 \leqslant j \leqslant 2t+2.$$

Так как существует $q_{0\lambda} \in P_{i_1}^{(i_1)} \subseteq V_{i+i_1}$, то в силу б) $b_2(V_{i+i_1}) \supseteq V_1$. Далее, при $i_1>0$ $b_{2t+3}(V_{i+i_1}) \supseteq V_{i+i_1-1}$, а при $i_1=0$ $b_{2t+3}(V_{i+i_1}) \supseteq V_1$. При $2t+4 \leqslant j \leqslant 2t+l+3$ либо $b_j(V_{i+i_1}) \supseteq V_1$, либо $b_j(V_{i+i_1}) \supseteq V_{i+i_1}$. Поэтому остается лишь возможность $b(i+i_1+1)=b_j$ при $3 \leqslant j \leqslant t+2$. Пусть $P_{i_1}^{(i_1)}=\{q_{0k_1}, \ldots, q_{0k_\tau}\}$. Тогда $b(i+i_1+1)(P_{i_1}^{(i_1)})=P_0^* \subseteq Q_0$, причем $M(P_0^*) \geqslant M(P_{i_1}^{(i_1)})$ для всех j, кроме $j=k_1+2$, а при $j=k_1+2M(P_0^*)= =M(P_{i_1}^{(i_1)})-1$.

Итак,

(4) $$V_{i+i_1+1}=\{q\} \cup P_0^* \cup \bigcup_{\tau=r-i_1+1}^{r} R_\tau \cup \bigcup_{q=2}^{s} P_{i_q}^{(i_1)}.$$

Так как $q \in V_{i+i_1+1}$, то $b(i+i_1+1)$ есть либо b_{2t+3}, либо b_j, $2t+4 \leqslant j \leqslant 2t+l+3$, ибо в противном случае имели бы $V_{i+i_1+2} \supseteq V_1$. Если $i_1>0$, то V_{i+i_1+1} содержит $R_\tau=\{q_{\tau_1}, \ldots, q_{\tau l}\}$, так что для любого j, такого, что $2t+4 \leqslant j \leqslant 2t+l+3$, имеем $b_j(V_{i+i_1+1}) \supseteq V_1$. В этом случае, следовательно, $b(i+i_1+2)=b_{2t+3}$ и

$$V_{i+i_1+2}=\{q\} \cup P_1^* \cup \bigcup_{\tau=r-i_1+2}^{r} R_\tau \cup \bigcup_{q=2}^{s} P_{i_q}^{(i_1-1)} \cup Q_0,$$

где P_1^* состоит из всех q_{1i}, таких, что $q_{0i} \in P_0^*$.

Пусть для $a>0$ доказано:

$$V_{i+i_1+a+1}=\{q\} \cup \bigcup_{\tau=0}^{a-1} Q_\tau \cup P_a^* \cup \bigcup_{\tau=r-i_1+a+1}^{r} R_\tau \cup \bigcup_{q=2}^{s} P_{i_q}^{(i_1-a)},$$

где P_a^* состоит из всех q_{ai}, таких, что $q_{0i} \in P_0^*$. Пусть $i_1-a>0$. Так как $q \in V_{i+i_1+a+1}$, то $b(i+i_1+a+2)$ есть либо b_{2t+3}, либо b_j при некотором $j \in \{2t+4, \ldots, 2t+l+3\}$. Но $R_\tau \subseteq V_{i+i_1+a+1}$, так что $b(i+i_1+a+2)$ есть b_{2t+3} и V_{i+i_1+a+2} есть

$$\{q\} \cup P_{a+1}^* \cup \bigcup_{\tau=0}^{a} Q_r \cup \bigcup_{\tau=r-i_1+a+2}^{r} R_\tau \cup \bigcup_{q=2}^{s} P_{i_q}^{(i_1-a-1)}.$$

Таким образом, при $i_1>0$.

$$V_{i+2i_1+1}=\bigcup_{q=2}^{s} P_{i_q} \cup \bigcup_{\tau=0}^{i_1-1} Q_\tau \cup P_{i_1}^* \cup \{q\}.$$

При $i_1=0$ имеем из (4):

$$V_{i+1}=\{q\} \cup P_0^* \cup \bigcup_{q=2}^{s} P_{i_q}.$$

Так как $i_s=r$, $V_i \in K$, то P_{i_s} содержит α_{rj} при $j>l$. Следовательно, $b_{2t+3}(V_{i+2i_1+1}) \supseteq V_1$. Поэтому $b(i+2i_1+2)$ есть b_j при некотором $j \in \{2t+4, ..., 2t+l+3\}$. Так как $\{q_{r1}, \ldots, q_{rl}\} \setminus P_{i_s} \neq \varnothing$, то существует $\tau \leqslant l$: $\alpha_{r\tau} \notin P_r$. Для любого такого τ:

$$V_{i+2i_1+2} = b_{2t+3+\tau}(V_{i+2i_1+1}) = V_{i+2i_1+1} \setminus \{q\}.$$

Так как $s>1$ и $V_i \in K$, то $M(P_r) < 2^h-2$, т. е. $N(V_{i+2i_1+2}) < N(V_1)$ и $V_{i+2i_1+2} \in K$. Нетрудно проверить, что $N(V_{i+2i_1+2}) \geqslant N(V_i)$ при $M(\overset{*}{P}_{i_1}) = M(\overset{*}{P}_0) \geqslant M(P_{i_1})$, чего быть не может. Следовательно, $M(\overset{*}{P}_{i_1})$ должно быть меньше $M(P_{i_1})$, что возможно только при $b(i+2i_1+2) = b_{k_1+2}$, в этом случае $M(\overset{*}{P}_{i_1}) = M(P_{i_1})-1$ и $N(V_{i+2i_1+2}) = N(V_i)-1$. Очевидно, каждое V из K, такое, что $N(V) \geqslant N(V_{i+2i_1+2})$, есть V_j при некотором $j \leqslant i+2i_1+2$. Таким образом, если $V_i \in K$, $s>1$ (см. (2)), то существует $\delta \geqslant 2$, для которого $V_{i+\delta} \in K$; $N(V_{i+\delta}) = N(V_i)-1$.

Пусть теперь $s=1$. Из (3) находим:

$$V_{i+r} = P_r^{(r)} \cup \bigcup_{\tau=1}^{r} R_\tau.$$

Легко проверить, что $b(i+r+1)$ есть b_j $(3 \leqslant j \leqslant 2t+2)$. Пусть $P_r^{(r)} = \{q_{0k_1}, \ldots, q_{0k_\tau}\}$. При $3 \leqslant j \leqslant t+2$ $M(b_j(P_r^{(r)})) \geqslant M(P_r^{(r)})$, если $j \neq k_1+2$, и $M(b_{k_1+2}(P_r^{(r)})) = M(P_r^{(r)})-1$. Кроме того, при $t+3 \leqslant j \leqslant 2t+2$, $j \neq t+k_1+2$ также имеет место неравенство $M(b_j(P_r^{(r)})) \geqslant M(P_r^{(r)})$. При $k_1 \leqslant l$ $b_{t+k_1+2}(P_r^{(r)}) = b_{k_1+2}(P_r^{(r)})$, $M(b_{t+k_1+2}(P_r^{(r)}) = M(P^{(r)}_r)$. При $k_1 > l b_{t+k_1+2}(P_r^{(r)}) = \{q_{02}, \ldots, q_{0,k_1-1}, q_{0k_2}, \ldots, q_{0k_\tau}\}$, $M(b_{t+k_1+2}(P_r^{(r)}) = M(P_r^{(r)})-2$.

Итак, $V_{i+r+1} = b_j(V_{i+r})$ при $3 \leqslant j \leqslant 2t+2$, т. е.

$$V_{i+r+1} = \{q\} \cup \overset{*}{P}_0 \cup \bigcup_{\tau=1}^{r} R_\tau,$$

где $\overset{*}{P}_0 \subseteq Q_0$, $\overset{*}{P}_0 = b_j(P_r^{(r)})$, причем $M(\overset{*}{P}_0) < M(P_r^{(r)}) = M(P_r)$ только при $b(i+r+1) = b_{k_1+2}$ либо $b(i+r+1) = b_{t+k_1+2}$. Как и выше в случае $s>1$, можно показать:

$$V_{i+2r+1} = \{q\} \cup \overset{*}{P}_r \cup \bigcup_{\tau=0}^{r-1} R_\tau,$$

где $\overset{*}{P}_r$ состоит из всех q_{rj}, для которых $q_{0j} \in \overset{*}{P}_0$, причем $b(i+r+a+1)$ при $1 \leqslant a \leqslant r$ есть b_{2t+3}. Так как $N(V_i) > 2^{n-l-1} = N(\{q_{r,l+1}\})$, то либо $r>1$, $k_\tau \geqslant l+1$, либо $r=1$, $k_\tau > l+1$. В обоих случаях $\overset{*}{P}_r \setminus \{q_{r1}, \ldots, q_{rl}\} \neq \varnothing$. Поэтому $b(i+2r+2) \neq b_{2t+3}$. Предположим, что $\overset{*}{P}_0 \supseteq \{q_{01}, \ldots, q_{0l}\}$. Тогда $\overset{*}{P}_r \supseteq \{q_{r1}, \ldots, q_{rl}\}$. Как установлено, $b(i+2r+2)$ есть b_j для некоторого $j \in \{2t+4, ..., 2t+l+3\}$. Но для любого такого j имеем: $b_j(\{q_{r1}, \ldots, q_{rl}\}) \supseteq V_1$. Поэтому включение $\overset{*}{P}_0 \supseteq \{q_{01}, \ldots, q_{0l}\}$ невозможно, так что при $k_1 > l$

$b(i+r+1) \neq b_{k_1+2}$, а так как при $k_1 \leqslant l$ $b_{k_1+2}(V_{i+r}) = b_{k_1+t+2}(V_{i+r})$, то можно полагать $b(i+r+1) \neq b_{k_1+2}$ при любом K. Допустим, что $b(i+r+1) \neq b_{t+k_1+2}$. Тогда $M(P_r^*) = M(P_0^*) \geqslant M(P_r)$. Так как $\{q_{01}, \ldots, q_{0l}\} \setminus P_0^* \neq \varnothing$, то для каждого $j \in \{2t+4, \ldots, 2t+l+3\}$, такого, что $q_{0,j-2t-3} \notin P_0^*$, имеем:

$$V_{i+2r+2} = b_j(V_{i+2r+1}) = P_r^* \cup \bigcup_{\tau=0}^{r-1} R_\tau.$$

Заметим, что $P_r^* \setminus \{q_{r1}, \ldots, q_{rl}\} \neq \varnothing$; $\{q_{r1}, \ldots, q_{rl}\} \setminus P_r^* \neq \varnothing$. Очевидно, что либо $M(P_r^*) < 2^l - 2$, либо $P_r^* \supseteq V_1$. В первом случае $N(V_{i+2r+2}) < N(V_1)$, так что $V_{i+2r+2} \in K$ и $N(V_{i+2r+2}) \geqslant N(V_i)$, ибо $M(P_r^*) \geqslant M(P_r)$, чего быть не может. Во втором случае $V_{i+2r+2} \supseteq V_1$, чего тоже быть не может. Таким образом, необходимо $b(i+r+1) = b_{t+k_1+2}$.

При $k_1 \leqslant l$ имеем:

$$V_{i+2r+2} = \{q_{r1}, \ldots, q_{r,k_1-1}, q_{rk_2}, \ldots, q_{rk_\tau}\} \cup \bigcup_{\tau=0}^{r-1} R_\tau.$$

Нетрудно проверить, что $V_{i+2r+2} \in K$ и $N(V_{i+2r+2}) = N(V_i) - 1$. При $k_1 > l$

$$V_{i+2r+2} = \{q_{r2}, \ldots, q_{r,k_1-1}, q_{rk_2}, \ldots, q_{rk\tau}\} \cup \bigcup_{\tau=0}^{r-1} R_\tau,$$

т. е. V_{i+2r+2} есть элемент K с наибольшим номером, меньшим $N(V_i)$

$$N(V_{i+2r+2}) = N(V_i) - 2^{n-h-1} - 1.$$

Итак, из последовательности $V_0, V_1, \ldots, V_{k-1}$ можно выделить подпоследовательность $V_{i_1}, \ldots, V_{i_\nu}$, такую, что $\{V_{i_1}, \ldots, V_{i_\nu}\} = K$, причем V_{i_j+1} есть элемент K с наибольшим номером, меньшим $N(V_{i_j})$. Кроме того, $i_{j+1} \geqslant i_{j+2}$, так что $i_\nu \geqslant 2\nu - 1$; и $k-1 \geqslant 2\nu - 1$; $k \geqslant 2\nu$, откуда $k \geqslant 2^n(1-2^{1-l}) + 1 \geqslant 2^n(1-2^{1-l})$. Нами установлено, что если множество $B^* \setminus \mathscr{F}(\mathfrak{A})$ непусто, то длина любого слова из этого множества не меньше чем $2^n(1-2^{1-l})$. Для установления непустоты множества $B^* \setminus \mathscr{F}(\mathfrak{A})$ построим маршрут в $\bar{G}(\mathfrak{A})$, ведущий от V_0 к вершине, из которой не выходит ребро с некоторой отметкой. Мы уже установили, что в $\bar{G}(\mathfrak{A})$ существует маршрут от V_0 к вершине $\{q_{r,l+1}\}$. Имеем:

$$b_2^r(\{q_{r,l+1}\}) = \{q_{0,l+1}\}\, b_{t+l+3}(\{q_{0,l+1}\}) = \{q_{02}, \ldots, q_{0l}\};$$

$$\xi = b_{2t+3}^r(\{q_{02}, \ldots, q_{0l}\}) = \{q_{r2}, \ldots, q_{rl}\} \cup \bigcup_{\tau=0}^{r-1} R_\tau.$$

Пусть уже доказано существование пути из V_0 в $V \subseteq Q \setminus \{q\}$, причем $1 < N(V) \leqslant N(\xi)$. Пусть

$$V = \bigcup_{q=1}^{s} P_{i_q};\; P_{i_q} \neq \varnothing;\; P_{i_q} \subseteq Q_{i_q}.$$

Имеем:

$$b_2^i(V) = \bigcup_{q=1}^{s} P_{i_q}^{(i_1)} \cup \bigcup_{\tau=r-i_1+1}^{r} R_\tau,$$

сли $P_{i_1}^{(i_1)} = \{q_{0k_1}, \ldots, q_{0k_\tau}\}$, то $V' = b_{k_1+2}(b_2^{i_1}(V)) = P_0^* \cup \{q\} \cup \bigcup_{q=2}^{s} P_{i_q}^{(i_1)} \cup \bigcup_{\tau=r-i_1+1}^{r} R_\tau$, причем $M(P_0^*) = M(P_{i_1}) - 1$ и $V' \neq \varnothing$, так как $N(V) > 1$.

$$V'' = b_{2t+3}^{i_1}(V') = P_{i_1}^* \cup \bigcup_{q=2}^{s} P_{i_q} \cup \bigcup_{\tau=0}^{l-1} R_\tau \cup \{q\}.$$

Нетрудно проверить, что $N(V'' \setminus \{q\}) = N(V) - 1 < N(\xi)$, т. е. $\{q_{r1}, \ldots, q_{rl}\} \setminus V'' \neq \varnothing$ и существует $j \in \{2t+4, \ldots, 2t+l+3\}$, для которого

$$V''' = b_j(V'') = P_{i_1}^* \cup \bigcup_{q=2}^{s} P_{i_q} \cup \bigcup_{\tau=0}^{i_1=1} R_r \subseteq Q \setminus \{q\},$$

причем $N(V''') = N(V) - 1$. Итак, существует маршрут из V в $\{q_{01}\}$, но из $\{q_{01}\}$ не выходит ребро, помеченное b_3, что и требовалось. Таким образом, **автомат** $\mathfrak{A}$ не является генератором, и при m, n, p, удовлетворяющих условию теоремы, имеем

$$L(m, n, p) \geqslant l(\mathfrak{A}) > 2^n(1 - 2^{1-l}) = 2^n\left(1 - 2^{1-\left[\frac{p-3}{9}\right]}\right),$$

что и требовалось доказать.

УПРАЖНЕНИЯ

1. Построить конечный автомат $\mathfrak{A}$ с наименьшим возможным числом состояний, перечисляющий множество $((10)^* \cup (10)^* 1)^*$.
2. Является ли автоматно-перечислимым множество $(((10)^* \cup 1)^* . (01)^*)^*$?
3. Найти значение $L(2, 3, 2)$.
4. Пусть $L^*(m, n, p) = \max\limits_{|A|=m, |Q|=n, |B|=p} l\ \mathfrak{A}$, где максимум берется по всем автоматам Мура $\mathfrak{A} = (A, Q, B, \varphi, \psi)$. Существуют ли такие значения m, n, p, что $L^*(m, n, p) < L(m, n, p)$?

§ 3. ВЗАИМОДЕЙСТВИЕ КОНЕЧНЫХ АВТОМАТОВ И КОНЕЧНЫЕ АВТОМАТЫ В ЛАБИРИНТАХ

Пусть $\mathfrak{A} = (A, Q, B, \varphi, \psi, q_0)$ — произвольный инициальный конечный автомат и $\mathfrak{A}' = (B, Q', A, \varphi', \psi', q_0')$ — инициальный конечный автомат Мура, т. е. $\psi' = \psi'(q')$. **Взаимодействием автоматов** $\mathfrak{A}$ и $\mathfrak{A}'$ назовем последовательность (q_0, q_0', a_0, b_0), $(q_1, q_1', a_1, b_1) \ldots$, такую, что $a_0 = \psi'(q_0')$; $b_0 = \psi(q_0, a_0)$; $q_{i+1} = \varphi(q_i, a_i)$; $q_{i+1}' = \varphi'(q_i', b_i)$; $a_{i+1} = \psi'(q_{i+1}')$; $b_{i+1} = \psi(q_{i+1}, a_{i+1})$. Эта последовательность, как нетрудно заметить, описывает поведение системы, возникающей при соединении выхода автомата $\mathfrak{A}$ со входом автомата $\mathfrak{A}'$ и входа $\mathfrak{A}$ с выходом $\mathfrak{A}'$. Заметим, что если не требовать, чтобы автомат $\mathfrak{A}'$ был автоматом Мура, то при определении выходных сигналов автоматов $\mathfrak{A}$ и $\mathfrak{A}'$ в момент t возникает логический круг: выходной сигнал $\mathfrak{A}$ определяется в зависимости от выходного сигнала $\mathfrak{A}'$ в тот же момент и, наоборот, выходной сигнал $\mathfrak{A}'$ в момент t определяется в зависимости от выходного сигнала $\mathfrak{A}$ в момент t.

При рассмотрении взаимодействия двух автоматов естественным образом возникает следующее понятие **управления.** Пусть $S\subset A$. Скажем, что автомат $\mathfrak{A}$ S-управляет автоматом $\mathfrak{A}'$, если во взаимодействии этих автоматов на выходе автомата $\mathfrak{A}'$ в некоторый момент возникает сигнал из множества S. Автомат $\mathfrak{A}'$ назовем S-управляемым, если существует слово $\beta\in B^*$, такое, что $\psi'(q_0', \beta)\in S$.

Покажем, что взаимодействие автоматов $\mathfrak{A}$ и $\mathfrak{A}'$ можно представить как процесс прохождения автомата $\mathfrak{A}$ по некоторому лабиринту, а управление автоматом $\mathfrak{A}'$ — как отыскание автоматом $\mathfrak{A}$ выхода из этого лабиринта.

Пусть A и B — конечные непустые множества. Назовем **ориентированным** (A, B)**-лабиринтом** конечный орграф L с выделенной вершиной 0 и выделенным подмножеством $S'\subset A$, для которого выполнены следующие условия:

а) каждой вершине v сопоставлен символ $\rho(v)\in A$;

б) каждому ребру сопоставлен символ из B, причем различным ребрам, выходящим из вершины, сопоставлены различные символы;

в) множество $\theta(v)$ отметок ребер, выходящих из вершин v, однозначно определяется по отметке a этой вершины: $\theta(v)=\gamma(a)$;

г) существует путь от вершины 0 к вершине, отмеченной символом из множества S

Вершина 0 называется **началом лабиринта;** любая вершина, отмеченная символом из S, называется **выходом из лабиринта.**

Скажем, что конечный инициальный автомат $\mathfrak{A}=(A, Q, B, \varphi, \psi, q_0)$ является **допустимым для лабиринта** L, если выполняется условие

$$\forall q\in Q \quad \forall a\in A \quad (\psi(q, a)\in\gamma(a)).$$

Если автомат $\mathfrak{A}$ допустим для ориентированного лабиринта L, то **поведением** $\mathfrak{A}$ в L назовем бесконечную последовательность вида (q_0, v_0, a_0, b_0), (q_1, v_1, a_1, b_1).. , где $v_0=0$; $a_i=\rho(v_i)$; $b_i=\psi(q_i, a_i)$; $q_{i+1}=\varphi(q_i, a_i)$ и v_{i+1} есть вершина, к которой от v_i ведет ребро с отметкой b_i. Если хотя бы одна из вершин v_i в этой последовательности является выходом из L, то говорим, что $\mathfrak{A}$ **обходит** L.

Сопоставим произвольному управляемому инициальному автомату Мура $\mathfrak{A}=(B, Q', A, \varphi', \psi', q_0')$ с выделенным подмножеством S выходных символов ориентированный лабиринт $L(\mathfrak{A}')$, получающийся из диаграммы Мура автомата $\mathfrak{A}'$, если в ней у каждой стрелки оставить лишь отметку входного сигнала и каждой вершине приписать соответствующий выходной сигнал. Началом этого лабиринта служит вершина, соответствующая состоянию q_0', выходом — каждая вершина с отметкой из S.

Очевидно, взаимодействие любого автомата $\mathfrak{A}$ с автоматом $\mathfrak{A}'$ совпадает с поведением автомата $\mathfrak{A}$ в лабиринте $L(\mathfrak{A}')$, причем $\mathfrak{A}$ S-управляет автоматом $\mathfrak{A}'$ тогда и только тогда, когда $\mathfrak{A}$ обходит лабиринт $L(\mathfrak{A}')$ Обратно, если задан некоторый ориентированный (A, B)-лабиринт L, то сопоставим ему автомат Мура $\mathfrak{A}' = (B, Q', A, \varphi', \psi', 0)$, множеством состояний Q' которого служит множество вершин L; $\varphi'(q, b)$ определяется как вершина, в которую из q ведет ребро с отметкой b, если $b \in \theta(q)$, и $\varphi'(q, b) = q$ в противном случае; $\psi'(q)$ есть отметка вершины q и 0 — начало L. Очевидно, что любой автомат, обходящий L, S-управляет автоматом $\mathfrak{A}'$ и по любому автомату, S-управляющему автоматом $\mathfrak{A}'$, легко построить автомат, обходящий L.

Таким образом, задачи построения автомата, управляющего данным автоматом, и автомата, обходящего данный ориентированный лабиринт, оказываются в определенном смысле эквивалентными. Поведение автоматов в лабиринтах было впервые рассмотрено Шенноном [21] и изучалось затем в работах [22, 23]. В настоящем параграфе мы рассмотрим лишь одну из исследовавшихся задач, связанную с поведением автоматов в плоских прямоугольных лабиринтах. Приведем необходимые определения. Пусть $B = \{w, n, s, e\}$; положим $w^{-1} = e$, $e^{-1} = w$, $n^{-1} = s$, $s^{-1} = n$. Пусть A есть множество всех пар вида (M, μ), где M — непустое подмножество множества B и $\mu \in \{0, 1\}$. Лабиринтами далее будем называть лишь такие ориентированные (A, B)-лабиринты, для которых выполняются условия.

1) если из вершины v_1 к вершине v_2, ведет ребро с отметкой x, то из v_2 к v_1 ведет ребро с отметкой x^{-1};

2) если множество отметок ребер, выходящих из вершины v, есть $\theta(v)$, то отметка этой вершины v имеет вид $(\theta(v), \mu)$;

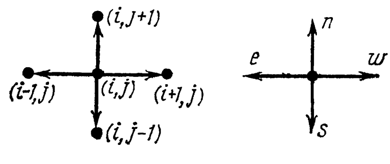

Рис 4 2

3) S есть множество отметок вида $(M, 1)$, причем в лабиринте существует единственная вершина, отмеченная символом из S. Эту вершину обозначим T и назовем выходом из лабиринта.

Лабиринт L называется плоским, если вершинами его являются точки плоскости с целыми координатами, причем ребро, выходящее из вершины (i, j) может вести лишь к одной из четырех вершин, указанных на рис. 4.2, и имеет своей отметкой символ соответствующего направления (рис. 4.2).

Плоский лабиринт назовем правильным, если существует путь, ведущий по ребрам целочисленной решетки, начинающейся с T, не пересекающийся далее с вершинами и ребрами L и уводящий сколь угодно далеко от L. Автомат, допустимый для лабиринтов рассматриваемого вида, называем **мышью.**

Имеет место следующая теорема, доказанная Л. Будахом [23]. В связи с тем, что изложенное в [23] доказательство теоремы занимает около 90 страниц, ниже приводится значительно упрощенный вариант ее доказательства, принадлежащий А. С. Подколзину [24].

Теорема 4.5. [23]. *Для любой мыши $\mathfrak{A}$ можно построить правильный лабиринт, который этой мышью не обходится.*

Доказательство. Введем сначала ряд вспомогательных понятий. Обозначим R множество всех непустых слов $p=x_1, ..., x_n$ над B, таких, что $\forall i \ (x_{i+1} \neq x_i^{-1})$. Положим $p^{-1}=x_n^{-1} \dots x_1^{-1}$. Конечный орграф L с выделенными вершинами 0 и T, ребрам которого сопоставлены слова из R, назовем **квазилабиринтом,** если выполнены следующие условия:

а) слова, сопоставленные различным ребрам, выходящим из одной вершины, начинаются с различных символов;

б) если из v_1 в v_2 ведет ребро, которому сопоставлено слово p, то из v_2 в v_1 ведет ребро, которому сопоставлено слово p^{-1};

в) существует путь от вершины 0 к вершине T. Как и в случае лабиринтов, 0 называется началом, T — выходом из L.

Пусть в квазилабиринте L от вершины u к вершине v ведет ребро, отмеченное словом $p=x_1 \dots x_n$, где $n>1$. Тогда от v к u ведет ребро, отмеченное словом p^{-1}. Удалим из L эти два ребра и вместо них присоединим к L цепочку, изображенную на рис. 4.3 ($w_1, ..., w_{n-1}$ — новые вершины).

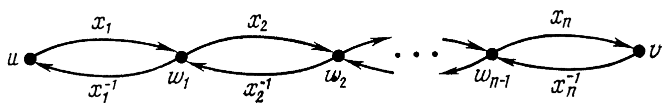

Рис. 4.3.

Проделав эту операцию над всеми ребрами L, а также сопоставив каждой вершине $v \neq T$ отметку $(\theta(v), 0)$, а вершине T — отметку $(\theta(T), 1)$, получим некоторый лабиринт, который обозначим $\Phi(L)$. Очевидно, множество вершин $\Phi(L)$ содержит множество вершин L. Пусть последовательность (s_0, v_0, a_0, b_0), $(s_1, v_1, a_1, b_1), \dots$ представляет собой поведение мыши $\mathfrak{A}$ в лабиринте $\Phi(L)$. Тогда **поведением мыши $\mathfrak{A}$ в квазилабиринте** L назовем подпоследовательность этой последовательности, соответствующую вершинам v_i квазилабиринта L (она может оказаться конечной).

Если (s_0, v_0, a_0, b_0), $(s_1, v_1, a_1, b_1), \dots$ — поведение мыши $\mathfrak{A}$ в лабиринте L, то будем говорить также, что мышь $\mathfrak{A}$ в момент $t=i$ находится в вершине v_i и имеет состояние s_i. Цепочки в лабиринтах вида, изображенного на рис. 4.3, будем называть **коридорами.**

Пусть p, $q \in R$ и $\mathfrak{A}$ — мышь. Скажем, что p и q **$\mathfrak{A}$-эквивалентны,** если для любого квазилабиринта L и любого ребра с отметкой p в нем при замене отметки p на q у этого ребра (вместе с заменой отметки p^{-1} противоположного ребра на q^{-1}) поведение $\mathfrak{A}$ в L не изменяется.

Лемма 4. 9. Для любого слова p из R и мыши $\mathfrak{A}$ существует такое натуральное l, что все слова вида p^{l_i}; $i=1, 2\ldots$ $\mathfrak{A}$-эквивалентны.

Доказательство. Пусть $p=x_1\ldots x_k$ и мышь $\mathfrak{A}$ в момент t находится в вершине u некоторого лабиринта L, из которой выходит коридор K, изображенный на рис. 4.4, и имеет состояние s.

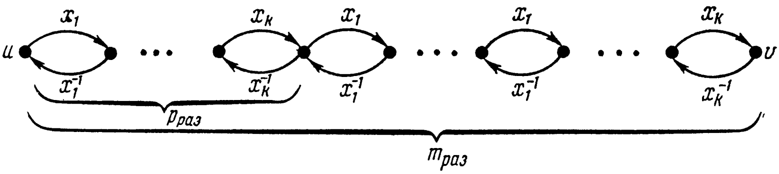

Рис 4.4.

Пусть отметка вершины u есть a. Покажем, что тогда существует такое m_0, что одна из следующих возможностей имеет место для всех $m=m_0i$; $i=1, 2, \ldots$.

1) $\mathfrak{A}$ не заходит в коридор K,

2) $\mathfrak{A}$ заходит в K и возвращается в u, не дойдя до вершины v,

3) $\mathfrak{A}$ заходит в K и не выходит из него,

4) $\mathfrak{A}$ проходит по K до вершины v и оказывается в состоянии s' (одном и том же для всех i).

Очевидно, что если для некоторого $m=m_0$ имеет место одна из ситуаций 1)—3), то она же имеет место и для всех $m>m_0$, т. е. и для $m=m_0i$; $i=1, 2, 3, \ldots$. Пусть ни для какого m ситуации 1)—3) места не имеют. Тогда рассмотрим бесконечный коридор Q вида, изображенного на рис. 4,5. Начальный отрезок этого коридора соответствующий слову p^m, обозначим Q_m. Мышь $\mathfrak{A}$ заходит в этот коридор и более не возвращается к u, причем выходит

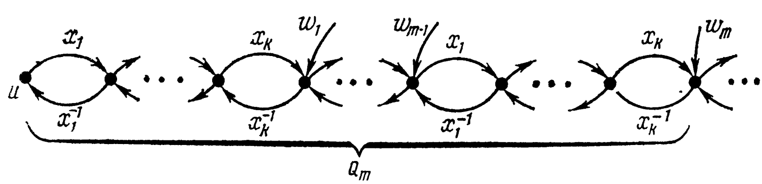

Рис. 4.5.

рано или поздно на конец любого отрезка Q_m. Пусть τ_m — момент, когда $\mathfrak{A}$ впервые попадает на конец отрезка Q_m. Выделим последовательность состояний $\mathfrak{A}$ в эти моменты: $\tau_1, \tau_2, \tau_3, \ldots$ $s_1, s_2, s_3, \ldots$. Тогда, так как число состояний мыши конечно, существуют n и r, такие, что $s_n=s_{n+r}$. В силу периодичности коридора мышь, находящаяся в состоянии s_n в конце отрезка Q_n, впервые выйдет на конец отрезка Q_{n+j} в том же состоянии, в котором мышь, находящаяся на конце отрезка Q_{n+r} в состоянии s_n, впервые выйдет на конец отрезка Q_{n+r+j}. Поэтому имеем: $s_{n+j}=s_{n+r+j}$; $j=0, 1, \ldots$ Отсюда получаем, что для любого j, $0 \leqslant j \leqslant r$, выполняется $s_{n+j+ir}=s_{n+j}$; $i=0, 1, 2, \ldots$. Выберем j так, чтобы $m_0=n+j$ делилось на r, тогда в конец каждого отрезка $Q_{m_0 i}$ $(i=1, 2, \ldots)$ $\mathfrak{A}$ будет впервые приходить в состоянии $s'=s_{n+j}$, что и завершает рассмотрение случая 4). Таким образом, для любых s и $\mathfrak{A}$, а также для случаев, когда мышь $\mathfrak{A}$ находится в начальный момент в вершине v, можно указать m_0, при котором одно из условий 1)—4) выполняется для всех $m=m_0 i$; $i=1, 2, \ldots$. Пусть l равно наименьшему общему кратному всех таких m_0; тогда в каждом из указанных случаев одно из условий 1)—4) выполняется для всех $m=li$; $i=1, 2, 3, \ldots$ Рассмотрим произвольный квазилабиринт L', у которого от вершины u к вершине v ведет ребро с отметкой p^m. В лабиринте $L=\Phi(L')$ от u к v будет вести коридор вида, изображенного на рис. 4.4. В силу вышесказанного, мышь $\mathfrak{A}$, находящаяся в вершине $u(v)$, для любого $m=li$ либо не заходит в коридор, либо заходит в него и, не дойдя до конца, возвращается к $u(v)$, либо остается в коридоре сколь угодно долго, либо, наконец, проходит до конца коридора и оказывается в состоянии $s'(s'')$, не зависящем от i. Это, очевидно, и означает, что поведения мыши $\mathfrak{A}$ в L' одинаковы при всех $m=li$; $i=1, 2, \ldots$. Лемма доказана.

Заметим, что если слова p и q $\mathfrak{A}$-эквивалентны, то, как легко проверить, любые слова вида XpY и XqY тоже $\mathfrak{A}$-эквивалентны.

Для заданной мыши $\mathfrak{A}$ применим лемму 4.9 к словам w, e, n, s; возьмем наименьшее общее кратное соответствующих значений l и обозначим его $\tilde{l}$. Обозначим: $\tilde{e}=e^{\tilde{l}}$, $\tilde{s}=s^{\tilde{l}}$, $\tilde{n}=n^{\tilde{l}}$, $\tilde{w}=w^{\tilde{l}}$; $\tilde{B}=\{\tilde{w}, \tilde{e}, \tilde{n}, \tilde{s}\}$. В силу леммы 1 все слова x, x^2, $x^3, \ldots$ для $x \in \tilde{B}$ $\mathfrak{A}$-эквивалентны. Квазилабиринт, у которого каждое приписанное ребру слово есть слово над $\tilde{B}$, назовем $\mathfrak{A}$-квазилабиринтом. Два слова p и q над $\tilde{B}$, назовем подобными, если одно получается из другого заменами вида $x \leftrightarrow xx$ $(x \in \tilde{B})$. Очевидно, подобные слова p и q $\mathfrak{A}$-эквивалентны. Каждому слову p над $\tilde{B}$ можно сопоставить подобное ему слово $\bar{p}=x_1 \ldots x_n$ над $\overline{\mathscr{D}}$, такое, что $\forall i (x_i \neq x_{i+1})$. Если $\mathfrak{A}$-квазилабиринт L_1 получен из $\mathfrak{A}$-квазилабиринта L_2 заменой отметок ребер на подобные им отметки, то скажем, что L_1 и L_2 подобны. Очевидно, что поведения $\mathfrak{A}$ в L_1 и в L_2 одинаковы.

Квазилабиринт L назовем **плоским**, если лабиринт $\Phi(L)$ плоский. $\mathfrak{A}$-квазилабиринт L назовем **планарным**, если существует подобный ему плоский квазилабиринт.

Предположим, что каждой вершине v $\mathfrak{A}$-квазилабиринта L сопоставлена взаимно-однозначно точка плоскости $\varphi(v)$, а ребру, ведущему от u к v, — ломаная, состоящая из горизонтальных и вертикальных отрезков и ведущая от $\varphi(u)$ и $\varphi(v)$, причем, если ребру приписано слово p и $\bar{p}=x_1 \ldots x_n$, то первый отрезок ломаной ведет в направлении x_1 (см. рис. 4.2), второй — в направлении x_2 и т. д. Пусть также (за исключением начал и концов) различные ломаные не пересекаются. Образованную всеми этими ломаными фигуру на плоскости назовем **укладкой** L.

Лемма 4.10. $\mathfrak{A}$-квазилабиринт L планарен тогда и только тогда, когда существует некоторая его укладка на плоскости.

Доказательство. Очевидно, достаточно показать, что если $\mathfrak{A}$-квазилабиринт обладает некоторой укладкой на плоскости, то он также обладает укладкой, у которой вершины расположены в узлах подрешетки целочисленной решетки с шагом $\tilde{l}$, а ломаные ведут по ребрам этой решетки. Пусть дана плоская укладка $\mathfrak{A}$-квазилабиринта L. Выделим все горизонтали, на которых расположена либо вершина, либо горизонтальный отрезок этой укладки (см. рис. 4.6). Эти горизонтали соединены между собой вертикальными отрезками укладки, и, растягивая эти отрезки, можно переместить горизонтали так, чтобы они пошли по линиям подрешетки целочисленной решетки с шагом $\tilde{l}$. Перемещая аналогичным образом вертикали, на которых расположены вершины и вертикальные отрезки укладки, получим искомую укладку $\mathfrak{A}$-квазилабиринта L. Лемма доказана.

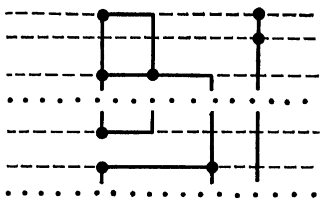

Рис 4 6

Лемма 4.11. Пусть L — $\mathfrak{A}$-квазилабиринт, у которого некоторое ребро r имеет отметку $\mathscr{P}xyxQ$ ($\mathscr{P}$, Q — слова над $\tilde{B}$; $x, y \in \tilde{B}$) и L' — $\mathfrak{A}$-квазилабиринт, полученный из L заменой этой отметки на $\mathscr{P}xQ$ (вместе с соответствующей заменой отметки противоположного ребра). Если L' планарный, то L тоже планарный.

Доказательство. Так как $\mathscr{P}xyxQ \in R$, то $x^{-1} \neq y$. Если $x = y$, то утверждение очевидно, ибо L' и L подобны. Пусть $x \neq y$. Без ограничения общности положим $x = \tilde{e}$, $y = \tilde{n}$. Пусть L' планарный. Рассмотрим ломаную, соответствующую в укладке L' ребру r, и выделим в ней горизонтальный отрезок ab, соответствующий рассматриваемому вхождению x в слово $\mathscr{P}xQ$. Пусть в укладке этот отрезок продолжается вправо и влево до концов c и d (см. рис. 4.7).

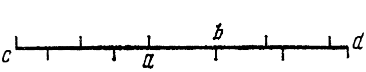

Рис 4 7

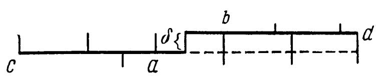

Рис. 4 8

Очевидно, что можно получить укладку L, изменив в укладке L' лишь часть, смежную с отрезком cd, так, как показано на рис. 4.8. Здесь δ — некоторая достаточно малая величина. Лемма доказана.

Квазилабиринт L **назовем деревом,** если граф, получающийся из него при замене каждой пары противоположных ребер одним неориентированным ребром, есть дерево Обозначим это дерево $t(L)$.

Лемма 4.12. $\mathfrak{A}$-квазилабиринт, являющийся деревом, планарен.

Доказательство. Каждому $\mathfrak{A}$-квазилабиринту L сопоставим $\mathfrak{A}$-квазилабиринт $\psi(L)$, получающийся из L при замене каждого ребра, отмеченного словом $x_1 \dots x_n$, где $n>1$ и $x_i \in \tilde{B}$, цепочкой вида, изображенного на рис. 4.3. Очевидно, L планарен тогда и только тогда, когда планарен $\psi(L)$. Поэтому лемму достаточно доказать для $\mathfrak{A}$-квазилабиринтов, у которых отметкой каждого ребра служит слово $x \in \tilde{B}$. Доказательство поведем индукцией по числу ребер дерева $t(L)$. Для одного ребра утверждение очевидно. Пусть оно доказано для всех деревьев, имеющих не более k ребер, и L — квазилабиринт, у которого дерево $t(L)$ имеет $k+1$ ребро. Пусть v — висячая вершина дерева $t(L)$, в которую ведет ребро r из вершины u. Рассмотрим укладку $\mathfrak{A}$-квазилабиринта, полученного из L удалением вершины v. В этой укладке к точке $\varphi(u)$ не примыкает отрезок, ведущий в направлении, определенном отметкой ребра r, и можно получить укладку L, если присоединить к $\varphi(u)$ такой отрезок, имеющий достаточно малую длину. Лемма доказана.

Лемма 4.13. Пусть L_1 — планарный $\mathfrak{A}$-квазилабиринт и v — вершина L_1. Пусть также L_2 — $\mathfrak{A}$-квазилабиринт, являющийся деревом и u — такая его вершина, что $\theta(u) \cap \theta(v) = \varnothing$. Тогда $\mathfrak{A}$-квазилабиринт, получающийся из L_1 и L_2 склеиванием вершин u и v, планарен.

Доказательство проводится индукцией по числу ребер в $t(L_2)$ аналогично доказательству леммы 4.

Произвольная укладка разбивает плоскость на одну внешнюю область и конечное число внутренних областей. Укладку $\mathfrak{A}$-квазилабиринта L назовем правильной, если из точки $\varphi(T)$ можно провести горизонтальный либо вертикальный отрезок, не пересекающийся с укладкой (за исключением точки $\varphi(T)$) и лежащий в ее внешней области $\mathfrak{A}$-квазилабиринт, обладающий правильной укладкой, назовем правильным. При помощи рассуждения, аналогичного рассуждению при доказательстве леммы 4.10, нетрудно убедиться, что для правильного $\mathfrak{A}$-квазилабиринта существует такой подобный ему $\mathfrak{A}$-квазилабиринт L, что лабиринт $\Phi(L)$ правильный. Поэтому для доказательства теоремы достаточно показать, что для любой мыши существует правильный $\mathfrak{A}$-квазилабиринт, не обходимый этой мышью.

Будем далее вместо $\tilde{e}$, $\tilde{n}$, $\tilde{w}$, $\tilde{s}$ писать e, n, w, s. Рассмотрим слова $enws$, $nwse$, $wsen$, $senw$ и для каждого найдем по лемме 4.9. соответствующее l. Наименьшее общее кратное всех этих l обозначим λ. Пусть, далее,

$$w_1 = (enws)^{\lambda+1}(wnes)^{\lambda},$$

$$w_2 = (wsen)^{\lambda+1}(eswn)^{\lambda}.$$

При изображении квазилабиринтов будем указывать лишь одно из двух противоположных ребер. Рассмотрим $\mathfrak{A}$-квазилабиринт L_0, изображенный на рис. 4.9. Очевидно, что для мыши $\mathfrak{A}$ помещенной в него, возможны следующие два случая:

а) через конечное число шагов $\mathfrak{A}$ заходит в один из коридоров и более из него не выходит.

б) Мышь $\mathfrak{A}$ бесконечное число раз возвращается в вершину 0.

В случае а) рассмотрим бесконечное дерево вида, изображенного на рис. 4.10. Поведение $\mathfrak{A}$ в нем воспроизводит поведение $\mathfrak{A}$ в L_0, т. е. через конечное число шагов $\mathfrak{A}$ заходит в один из коридоров дерева и более из него не выходит. При этом существует такое h, что $\mathfrak{A}$ никогда не достигает h-го яруса дерева. Рассмотрим $\mathfrak{A}$-квазилабиринт L_1, образованный первыми h ярусами дерева, и в качестве выхода T выберем произвольную вершину h-го яруса. По лемме 4.9 L_1 планарный и, как легко заметить, правильный, причем мышью $\mathfrak{A}$ не обходится

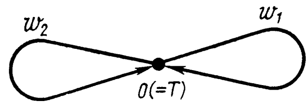

Рис. 4 9

В случае б) последовательность π проходимых коридоров периодична: $\pi=\varkappa_0\varkappa_1\varkappa_1\varkappa_1 \ldots$, где $\varkappa_0 = w_{i_1}^{\varepsilon_1}\ldots w_{i_s}^{\varepsilon_s}$ — предпериод и $\varkappa_1 = w_{j_1}^{\tau_1}\ldots w_{j_m}^{\tau_m}$ — период. Проделав в $\varkappa_0$ и $\varkappa_1$ всевозможные замены вида $w_i w_i^{-1} \to \Lambda$, получим приведенные предпериод p и период q. Возможны следующие случаи:

А. $q=\Lambda$. В этом случае $\mathfrak{A}$ в дереве рис. 4.10 будет периодически возвращаться к корню поддерева, соответствующего предпериоду p, и снова найдется такое h, что $\mathfrak{A}$ никогда не достигает

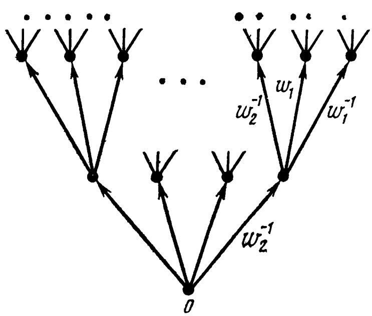

Рис. 4.10.

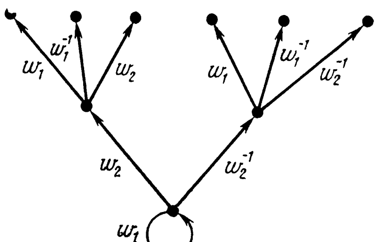

Рис. 4 11

h-го яруса. Как и в случае а), в качестве правильного квазилабиринта, не обходимого мышью $\mathfrak{A}$, берем квазилабиринт, образованный первыми h ярусами дерева рис. 4.10.

Б. $q\neq\Lambda$. Тогда возможны три подслучая:

1. $q=w_1^{n_1}$;

2. $q=w_2^{n_2}$;

3. $q=w_1^{n_1}w_2^{m_1}\ldots w_1^{n_t}w_2^{m_t}$ (очевидно, можем считать, что q начинается именно с $w_1^{n_1}$).

В подслучае 1 рассмотрим бесконечное дерево с петлей в корне, изображенное на рис. 4.11. Пусть 0 есть вершина этого дерева, к которой от корня ведет путь p^{-1}. Тогда мышь из вершины O придет к корню дерева и будет далее возвращаться к нему периодически, так что найдется такое h, что $\mathfrak{A}$ никогда не достигает h-го яруса дерева. Как и в случае а), рассмотрим $\mathfrak{A}$-квазилабиринт L_2, образованный первыми h ярусами дерева, и в качестве выхода T выберем произвольную вершину h-го яруса. Докажем, что L_2 планарный. По лемме 4.13 это достаточно доказать для квазилабиринта L_3 (см. рис. 4.12, а), причем по лемме 4.11 последний квазилабиринт можно сначала преобразовывать, заменяя в w_1 все вхождения вида xyx на x. Имеем:

$$w_1=(enws)^{\lambda+1}(wnes)^{\lambda},$$

$$(enws)(wnes)\to es,$$

$$(enws)es(wnes)\to es,$$

т. е.

$$w_1\to(enws)es\to enws=w_1'.$$

Квазилабиринт, соответствующий w_1', имеет укладку, изображенную на рис. 4.12, б, т. е. является планарным. Как видно из доказательства леммы 4.11,, укладку L_3 можно получить из укладки рис. 4.12, б путем последовательного «изгибания» ребер, причем так, чтобы полученная в результате ломаная располагалась внутри области, заштрихованной на рис. 4.12, в. Для получения укладки L_2 к точке $\varphi(Q)$ достаточно присоединить укладку дерева высоты h, которая, как видно из рис. 4.12, в, располагается вне замкнутой ломаной, т. е. полученная укладка L_2 правильная.

Аналогичным образом поступаем в подслучае 2. Отметим, что

$$w_2\to wsen,\quad w_1^{-1}\to nesw,\quad w_2^{-1}\to swne.$$

В подслучае 3 выделим два подслучая:

3.1. Существует либо n_i, либо m_i, отличное от ±1.

3.2. Все n_i и m_i равны ±1.

Построение правильного квазилабиринта, не обходимого мышью $\mathfrak{A}$, во всех этих подслучаях осуществляется следующим образом. Задается некоторый квазилабиринт L, ребрам которого приписаны слова вида $w_{i_1}^{\varepsilon_1},\ldots,w_{i_\tau}^{\varepsilon_\tau}$, причем существует начинающийся из вершины α замкнутый маршрут M, соответствующий некоторой степени периода q. Каждое ребро L, которому приписано слово $x=x_1x_2\ldots x_n$, $n>1$, где каждое x_i есть $w_j^{\pm1}$, заменим цепочкой вида, изображенного на рис. 4.3. При этом любому началу $x'=x_1\ldots x_k$ слова x соответствует некоторая вершина $\xi(x')$ цепочки. Полученный квазилабиринт обозначим L_1. К каждой вершине v квазилабиринта L_1 присоединим бесконечное дерево вида, изображенного на рис. 4.13, где $w_{j_1}^{\tau_1},\ldots,w_{j_k}^{\tau_k}$ — все слова вида $w_i^{\pm1}$, для которых из v не выходит ребро, отмеченное этим словом. Обозначим полученный квазилабаринт L_2. Пусть O есть вершина

L_2, к которой от вершины α ведет путь p^{-1}. Тогда мышь $\mathfrak{A}$ из вершины 0 придет к вершине α и будет далее перемещаться по цепочкам, соответствующим ребрам замкнутого маршрута M (быть мо-

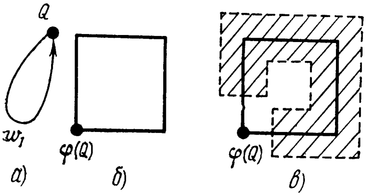

Рис 4 12

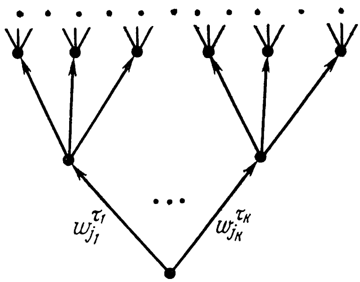

Рис 4 13

жет, выходя при этом в присоединенные к L_1 деревья). При этом существует такое h, что $\mathfrak{A}$ никогда не достигает h-го яруса присоединенных деревьев. Ограничиваясь первыми h ярусами этих деревьев, получим конечный квазилабиринт L_3. Если взять в качестве выхода из него произвольную вершину h-го яруса любого из присоединенных деревьев, то L_3 не будет обходиться мышью $\mathfrak{A}$.

Заметим, что в силу выбора λ следующие слова $\mathfrak{A}$-эквивалентны:

$$w_1 \underset{\mathfrak{A}}{\sim} (enws)^{\lambda x} w_1; \quad w_1 \underset{\mathfrak{A}}{\sim} w_1 (wnes)^{\lambda x}; \quad w_2 \underset{\mathfrak{A}}{\sim} (wsen)^{\lambda x} w_2;$$

$$(*) \qquad w_2 \underset{\mathfrak{A}}{\sim} w_2 (eswn)^{\lambda x}; \quad w_1^{-1} \underset{\mathfrak{A}}{\sim} w_1^{-1} (nesw)^{\lambda x};$$

$$w_1^{-1} \underset{\mathfrak{A}}{\sim} (nwse)^{\lambda x} w_1^{-1}; \quad w_2^{-1} \underset{\mathfrak{A}}{\sim} w_2^{-1} (swne)^{\lambda x}; \quad w_2^{-1} \underset{\mathfrak{A}}{\sim} (senw)^{\lambda x} w_2^{-1}$$

(x — натуральное).

Заменяя в соответствии с этими соотношениями входящие в отметки ребер квазилабиринта L слова вида $w_i^{\pm 1}$, преобразуем эти отметки к $\mathfrak{A}$-эквивалентным им отметкам так, чтобы полученный в результате квазилабиринт L' оказался планарным. При этом квазилабиринт L' преобразуется в некоторый квазилабиринт L_1', отличающийся от L_1 лишь тем, что вместо слов $w_i^{\pm 1}$ некоторые ребра имеют своими отметками $\mathfrak{A}$-эквивалентные им в силу указанных соотношений слова. Соответствующий квазилабиринт L_3' планарен и не обходится мышью $\mathfrak{A}$. В каждом из рассматриваемых ниже подслучаев будет установлено, что укладка одного из присоединяемых к L_1' деревьев располагается во внешней области укладки L_1': выбирая выход из L_3 на h-м ярусе этого дерева, получим правильный квазилабиринт L_3'.

Для установления планарности квазилабиринтов в соответствии с леммой 3 нам понадобится преобразовывать слова над $\bar{B}$, используя замены $xyx \to x$, $xx \to x$ к виду, не содержащему вхождений xyx и x. Результат такого приведения слова p обозначим $\hat{p}$. Если слова p и q могут быть получены друг из друга заменами вида $xyx \leftrightarrow x$ и $xx \leftrightarrow x$ (т. е. двусторонними заменами), то они называются эквивалентными: $p \sim q$. Нетрудно проверить, что в этом случае $\hat{p} = \hat{q}$.

Произвольное слово приводится либо к виду $\delta_1 (enws)^x \delta_2$, либо к виду $\delta_3 (eswn)^x \delta_4$, где δ_1, δ_3 — концы, а δ_2, δ_4 — начала слов $enws$ и $eswn$ соответственно. Первая и последняя буквы у слова $\hat{p}$ такие же, как у p.

Перейдем к рассмотрению подслучая 3.1. Пусть подстановка ρ на множестве B есть подстановка $(ns)(we)$. Рассмотрим мышь $\mathfrak{A}^*$, отличающуюся от $\mathfrak{A}$ лишь функцией выходов: $\psi^*(s, a) = \rho(\psi(s, \rho(a)))$. Нетрудно проверить, что если мышь $\mathfrak{A}$ проходит в квазилабиринте L_0 некоторую последовательность коридоров, то $\mathfrak{A}^*$ проходит последовательность коридоров, отличающуюся от нее заменой w_1 на w_2, и наоборот. Кроме того, если построен правильный лабиринт L, не обходимый мышью $\mathfrak{A}$ ($\mathfrak{A}^*$), то мышь $\mathfrak{A}$ ($\mathfrak{A}^*$) в лабиринте L^*, полученном из L поворотом на 180°, будет воспроизводить повернутое на 180° поведение $\mathfrak{A}$ ($\mathfrak{A}^*$) в L и, следовательно, не будет обходить L^*. Поэтому, переходя, при необходимости к мыши $\mathfrak{A}^*$, можно добиться, чтобы в подслучае 3.1 отличной от ± 1 была степень при w_1. Начало периода можно выбрать так, чтобы эта была степень при первом вхождении w_1 в q: $|n_1| > 1$. Рассмотрим сначала случай $n_1 > 1$. Пусть $q' = w_2^{m_1} w_1^{n_2} \dots w_1^{n_t} w_2^{m_t}$; $q_1 = w_1 q' q^{\lambda-1} w_1$; $q_2 = q' q^{\lambda-1}$. В качестве L возьмем квазилабиринт, изображенный на рис. 4.14. Покажем, как преобразовать слова q_1 и q_2 при помощи соотношений (*) в слова $\tilde{q}_1$ и $\tilde{q}_2$ так, чтобы полученный при этом квазилабиринт L' был планарным. Легко проверить, что имеют место следующие эквивалентности:

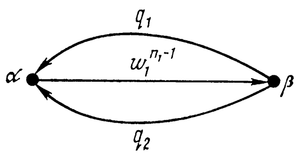

Рис. 4.14

$$q_1 \sim (eswn)^{n_1-1} q^\lambda w_1; \quad q_2 \sim \delta_1 (wnes)^{n_1} q^\lambda,$$

где $\delta_1 = 1$ при $m_1 < 0$; $\delta_1 = \Lambda$ при $m_1 > 0$.

Возможны следующие случаи:

а) $\hat{q} = (enws)^x \delta_2$, где $\delta_2 = en$ при $m_t > 0$ и $\delta_2 = l$ при $m_t < 0$;

б) $\hat{q} = (eswn)^x \delta_3$, где $\delta_3 = \Lambda$ при $m_t > 0$ и $\delta_3 = l$ при $m_t < 0$.

В случае а) имеем:

$$q_2 \sim \delta_1 (wnes)^{n_1} (enws)^{\lambda x} \delta_2;$$

$$q_1 \sim (eswn)^{n_1-1} (enws)^{\lambda x} (enws) \sim (eswn)^{n_1-1} (enws)^{\lambda x+1}.$$

Положим $\tilde{q}_1 = q_1(wnes)^{\lambda x}$ (очевидно, $\tilde{q}_1$ получено из q_1 заменой вида (*)). Тогда $\tilde{q}_1 \sim (eswn)^{n_1-1}(enws)^{\lambda x+1}(wnes)^{\lambda x}$, откуда находим $\hat{\tilde{q}} = es(wnes)^{n_1-2}$. При $m_t>0$ положим $\tilde{q}_2 = q_2(eswn)^{\lambda x}$, а при $m_t<0$ $\hat{q}_2 = q_2(swne)^{\lambda x}$. Впервом случае находим $\hat{\tilde{q}}_2 = \delta_1(wnes)^{n_1-1}wn$, а во втором случае $\hat{\tilde{q}}_2 = \delta_1(wnes)^{n_1-1}wne$.

В случае б)

$$q_1 \sim (eswn)^{n_1-1}(eswn)^{\lambda x}\,enws \sim (eswn)^{\lambda x+n_1-2}\,es;$$

$$q_2 \sim \delta_1(wnes)^{n_1}(eswn)^{\lambda x}\,\delta_3 \sim \delta_1(wnes)^{\lambda x+n_1-1}\,wn\delta_3.$$

Положим $\tilde{q}_1 = (enws)^{\lambda x}q_1$. Тогда снова получаем $\hat{\tilde{q}}_1 = es(wnes)^{n_1-2}$. При $m_1>0$ положим $\tilde{q}_2 = (wsen)^{\lambda x}q_2$, а при $m_1<0$ $\tilde{q} = (senw)^{\lambda x}q_2$. В первом случае находим $\hat{\tilde{q}}_2 = (wnes)^{n_1-1}\,wn\delta_3$, а во втором случае $\hat{\tilde{q}}_2 = s(wnes)^{n_1-1}\,wn\delta_3$.

Таким образом, всегда $\hat{\tilde{q}}_1 = es(wnes)^{n_1-2}$ и $\hat{\tilde{q}}_2 = \delta(wnes)^{n_1-1}\delta'$, где $\delta \in \{\Lambda, s\}$ и $\delta' \in \{wn, wne\}$. Кроме того, $\hat{w}_1^{n_1-1} = (enws)^{n_1-1}$.

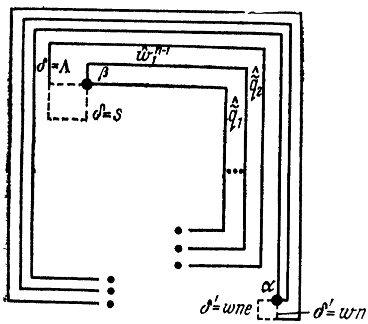

Рис. 4.15.

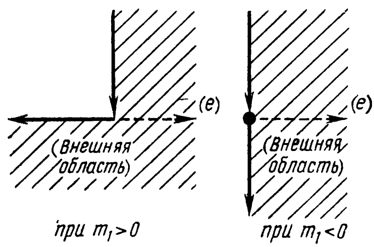

Рис 4 16.

Для лабиринта вида, изображенного на рис. 4.14, у которого отметки ребер q_1, q_2 и $w_1^{n_1-1}$ заменены отметками $\hat{\tilde{q}}_1$, $\hat{\tilde{q}}_2$ и $\hat{w}_1^{n_1-1}$, существует укладка на плоскости, указанная на рис. 4.15. Укладка L' получается из нее в соответствии с леммой 4.11 путем «изгибания» ребер, а укладка L_1' — введением новых вершин на полученных ломаных. Заметим, что при перемещении от точки β к точке α вдоль ломаной, соответствующей на рис. 4.15 слову $\hat{\tilde{q}}_2$, внешняя область укладки остается слева. Очевидно, это же будет выполняться и для полученной из нее «изгибанием» ребер ломаной, соответствующей слову $\tilde{q}_2$. На последней ломаной рассмотрим вершину v квазилабиринта L_1', соответствующую началу $q'w_1^{n_1}$ слова q_2. Так как слово w_1 кончается буквой s, а $w_2^{m_1}$ — начинается либо с w, либо с s, то окрестность точки v

имеет либо вид, изображенный на рис. 4.16, а, либо вид, изображенный на рис. 4.16, б, и укладка дерева, присоединяемая к v в направлении e, расположена во внешней области укладки L_1'. Выбирая выход из L_3' на h-м ярусе этого дерева, получим правильный квазилабиринт L_3', не обходящийся мышью $\mathfrak{A}$, что и завершает рассмотрение случая $n_1>1$. При $n_1<-1$ полагаем $q_1=w_1^{-1}q'q^{\lambda-1}w_1^{-1}$; $q_2=q'q^{\lambda-1}$ и в квазилабиринте L на рис. 4.14 заменяем отметку $w_1^{n_1-1}$, ребра, ведущего из α в β, на $w_1^{n_1+1}$. В остальном рассуждения совершенно аналогичны случаю $n_1>1$. Перейдем к рассмотрению подслучая 3.2. Пусть $\pi=n_1, m_1, n_2, \dots, n_t, m_t$ — последовательность степеней слов w_1 и w_2, входящих в q. Возможны следующие подслучаи:

3.2.1. $n_1=m_1=\dots=n_t=m_t=n_0$.

3.2.2. Найдется член последовательности π, у которого оба соседних члена (считаем, что член n_1 соседний с m_t) имеют противоположный знак. Переходя, при необходимости, к мыши $\mathfrak{A}^*$ и изменяя начало периода q, можно добиться, чтобы q в этом случае имело вид $w_2^i w_1^j w_2^{\varepsilon_1} \dots w_2^{\varepsilon_2} w_1^j$, где $i\neq j$.

3.2.3. В π можно выделить кусок вида $1, \overbrace{-1, \dots, -1}^{s}, \overbrace{1, \dots, 1}^{r}, -1, \dots$, где $s>1$, $r>1$. Переходя по необходимости к мыши $\mathfrak{A}^*$, можно добиться, чтобы при $s\geqslant r$ левая единица массива единиц, а при $s<r$ — правая единица массива минус-единиц соответствовала степени при w_2. Тогда окрестность этой степени w_2 в q будет иметь вид: $w_{j'}^{-i} w_j^{-1} \dots w_1^{-1} w_2^i w_1 \dots w_j w_{j'}^{-i}$. Изменяя начало периода q, можно привести q к виду $(w_j^{-1} \dots w_1^{-1} w_2^i w_1 \dots w_j) w_{j'}^{-i} \dots w_{j'}^{-i}$.

В подслучае 3.2.1. можем считать, что $q=w_1w_2$. Рассмотрим лишь случай $n_0=1$; случай $n_0=-1$ аналогичен. Возьмем в качестве L квазилабиринт, изображенный на рис. 4.17, где $q_1=q^{\lambda-1}$. Пусть L' получен из L заменой q_1 на $\tilde{q}_1=q_1(eswn)^{\lambda}$. Имеем

$$\tilde{q}_1 \sim en(wsen)^{\lambda-1}(eswn)^{\lambda} \sim eswn,$$

т. е. $\hat{q}_1=eswn$, и квазилабиринт, полученный из L заменой q_1 на $\hat{q}_1$, имеет укладку, изображенную на рис. 4.18. Укладка L_1' получается из нее «изгибанием» ребер и добавлением новых вершин.

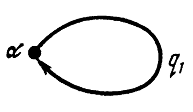

Рис. 4.17.

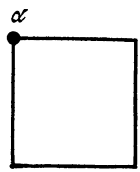

Рис. 4.18.

Видно, что укладка дерева, присоединяемого к α в направлении n, расположена во внешней области укладки L_1'. В подслучае 3.2.2, положим $i=-1$, $j=1$; случай $i=1$, $j=-1$ аналогичен. Обозначим $q'=w_1w_2^{\varepsilon_1}\dots w_2^{\varepsilon_2}w_1$ и выберем в качестве L квазилабиринт, изображенный на рис. 4.19. Для получения планарного квазилабиринта L' преобразуем сначала слово $q_1=q(q')^{\lambda-1}$, используя соотношение (*), к такому слову $\tilde{q}_1$, чтобы цикл c, соответствующий этому слову, был планарен. Так как q' начинается с e, q и q' кончаются на s, w_2^{-1} начинается с s и кончается на e, к укладке цикла c можно присоединить укладки циклов, соответствующих w_2^{-1} как указано на рис. 4.20, что и даст укладку L'. Возможны следующие случаи:

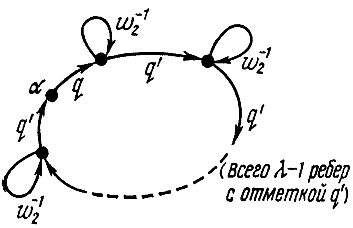

Рис 4 19

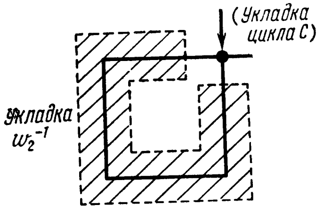

Рис 4 20

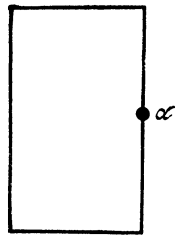

Рис 4.21

а) $\hat{q}'=(enws)^x$;
б) $\hat{q}'=(eswn)^x es$.

В случае а) находим $q(q')^{\lambda-1}\sim swn(enws)^{\lambda x}\sim s(enws)^{\lambda x-1}$. Положим $\tilde{q}_1=q_1(wnes)^{\lambda x}$, тогда $\hat{\tilde{q}}_1=swnes$. В случае б) $q(q_1)^{\lambda-1}\sim$ $\sim(swne)^{\lambda x+1}s$, и, полагая $\tilde{q}_1=(senw)^{\lambda x}q_1$, имеем $\hat{\tilde{q}}=swnes$. Укладка цикла, соответствующего слову $\hat{\tilde{q}}_1$, указана на рис. 4 21 Укладка L_1' получается из нее «изгибанием» ребер, присоединением укладок циклов, соответствующих словам w_2^{-1}, и добавлением новых вершин. Видно, что укладка дерева, присоединенного к вершине α в направлении e, расположена во внешней области укладки L_1'.

В подслучае 3.2.3. положим $i=j=1$; остальные случаи рассматриваются аналогично. Обозначим $\underbrace{w_1^{-1}\ldots w_1^{-1}}_{k}w_2\underbrace{w_1\ldots w_1}_{k}=q_2$; тогда q запишется в виде q_2q', где q' начинается и кончается словом w_2^{-1}. Обозначим также $w_1^{-1}w_2^{-1}\ldots w_1^{-1}=q_3$. В качестве L возьмем квазилабиринт, изображенный на рис. 4.22. Как и в случае 3.2.2, для получения планарного квазилабиринта L' преобразуем слово $q(q')^{\lambda-1}=q_1$ к такому слову $\tilde{q}_1$, чтобы соответствующий $\tilde{q}_1$ цикл был планарным. Укладка L' получится тогда присоединением к этому циклу ломаных, соответствующих слову q_3, и присоединением к концам ломаных циклов, соответствующих слову w_2. Возможны следующие случаи:

а) $\hat{q}_1=(swne)^x$;
б) $\hat{q}_1=(swne)^x se$.

Заметим, что $\hat{q}_2=nws$, $q\sim nwsq'$. В случае а) находим: $q(q')^{\lambda-1}\sim nws(swne)^{\lambda x}\sim nw(swne)^{\lambda x}$. Положим $\tilde{q}_1=(nwse)^{\lambda x}q_1$. Тогда $\hat{\tilde{q}}=nwse$. В случае б) $q(q')^{\lambda-1}\sim nw(senw)^{\lambda x}se$; будем иметь $\hat{\hat{q}}_1 = nwse$. Таким образом, $\hat{\hat{q}}_1 = nwse$, и укладка цикла для $\tilde{q}_1$ получается из укладки рис. 4.23 «изгибанием» ребер. Видно, что дерево, присоединяемое к вершине α в направлении s,

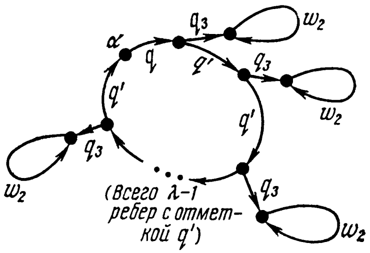

Рис. 4 22.

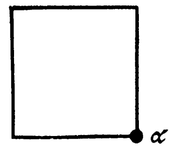

Рис. 4 23.

располагается во внешней области укладки L_1', так что получаемый квазилабиринт правильный. Теорема доказана.

УПРАЖНЕНИЯ

1. Построить автомат $\mathfrak{A}$ с наименьшим возможным числом состояний, $\{1\}$-управляющий любым $\{1\}$-управляемым сильно связным автоматом Мура $\mathfrak{A}'$ вида $(\{0, 1\}, \{q_1, q_2\}, \{0, 1\}, \varphi', \psi', q_1)$.
2. Построить автомат $\mathfrak{A}$ с наименьшим возможным числом состояний, обходящий произвольный правильный лабиринт без циклов.
3. Плоский (необязательно правильный) лабиринт назовем выпуклым, если вершинами его являются все целочисленные точки, расположенные внутри некоторой выпуклой области, причем любые две смежные (как точки целочисленной решетки) вершины соединены ребром. Построить автомат $\mathfrak{A}$, обходящий все выпуклые лабиринты.

ЛИТЕРАТУРА

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Элементы теории автоматов. М.: Изд-во Моск. ун-та, 1978.
2. Бёркс А. В., Райт Д. Б. Теория логических сетей. — В кн.· Кибернетический сборник, вып. 4. М.: ИЛ, 1962, 33—57.
3. Кобринский Н. Е., Трахтенброт Б. А. Введение в теорию конечных автоматов М.· Физматгиз, 1962.
4 Мур Э. Ф. Умозрительные эксперименты с последовательными машинами.— В кн Автоматы. М.· ИЛ, 1956, 179—210.
5. Грунский И С., Пономаренко Г. Г. Критерий конечности класса автоматов, неотличимых простым экспериментом. — Дискретный анализ, 1981. вып. 35, 3—15.
6. Карацуба А. А. Решение одной задачи из теории конечных автоматов. — УМН, 1960, **15**, № 3.
7 Василевский М. П. О распознавании неисправности автоматов. — Кибернетика, 1973, № 4, 98—108.
8. Василевский М. П. О расшифровке автоматов. — Кибернетика, 1974, № 2, 19—23.
9. Трахтенброт Б А., Барздинь Я. М Конечные автоматы (поведение и синтез). М. Наука, 1970
10. де Брёйн Н Г Одна комбинаторная задача — В кн. Кибернетический сборник (новая серия), вып. 6 М ИЛ, 1969.
11. Клини С. К. Представление событий в нервных сетях и конечных автоматах — В кн Автоматы М.· ИЛ, 1956, 15—67.
12. Копи И М, Элгот К. С. Райт Д. Б Реализация событий логическими сетями. — В кн Кибернетический сборник, вып 3, М ИЛ, 1961, 147—166.
13. Арбиб М А. Мозг, машина и математика М.· Наука, 1968.
14. Глушков В. М. Синтез цифровых автоматов. М.: Физматгиз, 1962.
15. Ушчумлич Ш М. О некоторых свойствах алгоритмов анализа и синтеза автоматов — В кн: Методы и системы технической диагностики, т 1 Саратов. Изд-во Саратовского ун-та, 1980.
16. Ушчумлич Ш. М. Об эффективности некоторых алгоритмов анализа и синтеза автоматов — В кн · Методы и системы технической диагностики, т 3. Саратов Изд-во Саратовского ун-та, 1984.
17. Ушчумлич Ш. М. Исследование некоторых алгоритмов анализа и синтеза автоматов. — ДАН СССР, 1979, **247**, № 3, 561—565.
18 Храпченко В М. Об одном методе получения нижних оценок сложности П-схем — Матем заметки, 1971, **10**, № 1, 83—92.
19. Mc Naughton R. Testing and generating infinite sequences by a finite automation. — Inform. and Control, **9**, № 5, 1966, 521—530.
20. Подколзин А. С. О сложности распознавания автоматов — генераторов.— Дискретный анализ, 1972. вып. 21, 31—61.
21. Шеннон К Сообщение о машине, решающей лабиринтную задачу. — В кн.: К Шеннон. Работы по теории информации и кибернетике. М.: ИЛ, 1963, 223—231.
22. Döpp K Automaten in labyrinthen. — EIK, 1971, **7**, № 2, 79—94.
23. Budach L. Automata and labirinths. — Math. Nachrichten, 1978, **86**, 195—282.
24. Будах Л. Лабиринты и автоматы. — Проблемы кибернетики, 1978, вып. 34, 83—94.

Валерий Борисович Кудрявцев,
Александр Сергеевич Подколзин,
Шчепан Ушчумлич

ВВЕДЕНИЕ В ТЕОРИЮ АБСТРАКТНЫХ АВТОМАТОВ

Зав редакцией *С. И. Зеленский*
Редактор *А. А. Локшин*
Художественный редактор *Ю. М. Добрянская*
Технический редактор *Г. Д. Колоскова, К. С. Чистякова*
Корректоры *Н В Картышева, Л А Кузнецова*

ИБ № 1929

Сдано в набор 22 08.84
Подписано к печати 10 07.85
Л-103090 Формат 60×90/16 Бумага тип № 3
Гарнитура литературная. Высокая печать
Усл печ л 11,0 Уч.-изд л. 11,6
Тираж 2925 экз. Заказ 471
Цена 40 коп Изд № 3240

Ордена «Знак Почета» издательство Московского университета 103009, Москва, ул. Герцена, 5/7.
Типография ордена «Знак Почета» изд-ва МГУ. 119899, Москва, Ленинские горы