ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

МОСКОВСКИЙ ИНЖЕНЕРНО-ФИЗИЧЕСКИЙ ИНСТИТУТ
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

С.Д. Кулик, А.В. Берков, В.П. Яковлев

ВВЕДЕНИЕ В ТЕОРИЮ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

(методы квантовой механики в кибернетике)
Книга 1

Рекомендовано УМО "Ядерные физика и технологии"
в качестве учебного пособия
для студентов высших учебных заведений

Москва 2008

УДК 530.145:007(075)
ББК 22.31я7+32.81я7
К 90

Кулик С.Д., Берков А.В., Яковлев В.П. Введение в теорию квантовых вычислений (методы квантовой механики в кибернетике): учебное пособие.– В 2 кн.– Кн. 1. – М.: МИФИ, 2008.–212 с.

Изложены основные понятия и методы теории квантовых вычислений — новой дисциплины, сформировавшейся на стыке квантовой механики и кибернетики. Представлены начальные основы квантовой схемотехники. На многочисленных примерах детально рассмотрены основные идеи, а также даны решения задач прямого и обратного анализа квантовой схемы и задачи синтеза квантовой схемы, удовлетворяющей требуемым условиям.

Пособие в основном ориентировано на студентов МИФИ кафедр “Теоретическая ядерная физика” и “Управляющие интеллектуальные системы”, изучающих не только квантовую механику, но и теорию принятия решений, и схемотехнику вычислительных устройств.

В первой книге представлены начала волновой кибернетики, отражающие важные сведения из классической кибернетики, необходимые для понимания квантовых вычислений.

Во второй книге представлены основы квантовых вычислений.

Пособие подготовлено в рамках Инновационной образовательной программы.

Рецензент
д-р физ.-мат. наук, проф. С. Г. Рубин

ISBN 978-5-7262-0976-0
ISBN 978-5-7262-0996-8 (кн. 1)

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Главная цель представленной работы — ознакомить читателя с основными понятиями *квантовой механики*, и в частности, дать предварительное введение в *теорию квантовых вычислений* (ТКВ) и приобрести навык в решении некоторых простейших задач в этой области.

При работе над книгой учитывался тот факт, что при изучении дисциплины, связанной с квантовыми вычислениями читатель, уже знаком с теорией *информации,* с теорией *множеств*, теорией *вероятностей* (ТВ), *математической статистической* (МС), *линейной алгеброй*, *с алгеброй Буля*, с основами *построения цифровых схем* (регистров, триггеров, комбинационных схем), *аналоговых схем*, а также владеет методами *математического моделирования и математического анализа*. При этом он владеет элементами *программирования* и знаниями по *физике* (в объеме традиционного курса университета) и хотя бы в небольшом объеме — знаниями по *квантовой механике.* Поэтому сведения по этим дисциплинам приведены достаточно кратко и, как правило, неполно.

Часть приведенных в работе примеров связана с *автоматизированными фактографическими информационно-поисковыми системами* (АФИПС), являющимися одной из разновидностей *автоматизированных систем обработки информации и управления* (АСОИУ). В состав АФИПС входит *фактографическая база данных* (БД), содержащая большое число записей. Размер баз данных поисковых систем сети Интернет очень большой. Квантовая БД, построенная на квантовых элементах, потенциально может содержать число записей больше, чем атомов во вселенной. Современные вычислительные средства заведомо обречены на неудачу при попытке реализовать на практике такую огромную базу данных.

Применяемые в настоящее время многопроцессорные системы позволяют создавать достаточно эффективные по быстродействию вычислительные системы. Однако квантовые вычислительные устройства, реализованные на квантовых элементах, потенциально могут обеспечить несравнимо большее быстродействие, чем существующие классические вычислительные системы.

Изучение теории квантовых вычислений невозможно без введения определений. Многие используемые далее определения связаны с прикладными задачами, поэтому они могут не содержать некоторых деталей, важных с точки зрения формальной теории.

Важно отметить, что для любого заданного определения или термина (из рассматриваемых далее) практически всегда можно подобрать *контрпример*, т.е. найти такое **нечто**, что, с одной стороны, это **нечто** удовлетворяет определению, а с другой — это **нечто** не удовлетворяет определению.

В процессе разработки аналогичной дисциплины и при написании лекционных материалов были широко использованы подходящие источники многих авторов (приведенные в конце каждой главы).

Сейчас, к сожалению, достаточно часто нарушаются права авторов, поэтому каждый раз, где это необходимо, даны ссылки на источник заимствования. Не всегда это заимствование было дословным. Иногда текст подвергался изменению, переработке и дополнению без прямого указания по тексту об этом.

Авторы благодарны студентам кафедры “Теоретическая ядерная физика” и кафедры “Управляющие интеллектуальные системы” МИФИ, которые, с одной стороны, были первыми слушателями, и на них апробировалась часть материалов, представленных в пособии, а с другой стороны, оказали техническую помощь в оформлении рукописи.

В пособии в книге 2 главу 1 написал *А.В. Берков*, главы 2, 3, 4 — *В.П. Яковлев,* главу 5 (и главу 1 в книге 1) — *С.Д. Кулик*.

Авторы

Во многих источниках есть ошибки, опечатки, упущения и т.п. дефекты. Конечно, и эта работа не исключение. В любом случае будем рады информации об обнаруженных опечатках и неточностях.

Авторы

sedmik@mail.ru
sedmik@hotmail.com

ВВЕДЕНИЕ

Современное общество уже нельзя представить без активного и широкого применения вычислительных средств, а также без эффективного применения *информационных систем* (ИС) и, в частности, *автоматизированных систем обработки информации и управления* (АСОИУ).

Применяемые в настоящее время технические системы позволяют решать многие специальные задачи в различных областях знаний: медицине, военном деле, криминалистике и др.

Однако созданные и проектируемые ИС и, в частности АСОИУ, во многих случаях не удовлетворяют растущим требованиям пользователей. К основным факторам, которые влияют на эффективность применения информационных систем, и которые до настоящего времени еще не удалось в достаточной степени учесть при создании ИС, следует отнести:

- противоречие между необходимостью увеличивать объем информации, хранимой в ИС, и требованием сокращать время ее обработки (например, время поиска);
- сложный и противоречивый характер связи между требованиями к точности обслуживания информационных запросов, увеличением объема хранимой информации и сокращением времени ее обработки.

Кроме этих общих проблем, при решении специальных задач в таких областях, как, например, медицина, военное дело или криминалистика, важное значение приобретает разработка различных алгоритмов (вычислительных схем), эффективных, например, с точки зрения временных затрат, и выработка на их основе алгоритмов принятия решений.

Возможность создания этих алгоритмов связана с фундаментальными исследованиями в квантовой механике, в теории принятия решений и в теории нейронных сетей. О важности этих исследований свидетельствуют многочисленные публикации различных ученых, так или иначе сталкивающихся на практике с проблемой повышения эффективности ИС и вычислительных средств.

В методическом плане изложение материала ведется в двух направлениях.

С одной стороны, представлен подход к проблемам квантовых вычислений (и к проблемам разработки квантовых алгоритмов), отталкивающийся от важных результатов, полученных в кибернетике, при этом эмпирическим образом вводится аппарат квантовой механики, выступающий именно как формальная математическая структура (это безусловно поможет кибернетику, не владеющему соответствующим разделом физики, как можно быстрее и с меньшими затратами понять азы квантовой механики).

С другой стороны, фундаментальные результаты кибернетики излагаются, по возможности опираясь на квантовую механику как физическую теорию реального квантового мира (это позволит физику, не владеющему соответствующим разделом кибернетики, освоить начала кибернетики, необходимые для понимания квантовых вычислений).

Изучение *теории квантовых вычислений* и, в частности, начал *волновой кибернетики* невозможно без введения определений. В данной работе приводится много определений, что позволяет читателю взглянуть на предмет с разных сторон и рассмотреть тонкие моменты.

Опыт создания ИС показал, что современный специалист в области информационных систем (и в частности АСОИУ) неизбежно столкнется с проблемой принятия решения, а также с необходимостью разрабатывать эффективный алгоритм для решения заданной технической задачи. Ему следует быть готовым к этому. А для того чтобы разрабатывать эффективные алгоритмы, он должен знать, как это можно сделать.

Современные исследования убедительно показывают, что элементная база вычислительных средств, построенная на квантовых объектах, должна обеспечить возможность реализовывать не просто эффективные, а очень эффективные алгоритмы для решения практических задач. Инструментарий квантовых вычислений предоставляет широкие возможности эффективного решения очень важных задач для практики, решение которых пока еще не под силу классическим алгоритмам. Квантовая механика открыла возможность разработки квантовых алгоритмов для выполнения квантовых вычислений.

Именно основам квантовых вычислений и посвящено данное пособие.

«Сто раз прочти, сто раз напиши, и смысл сам войдет в тебя.»
(*Китайская пословица)* [**36**]

«…По мере того, как электронные устройства становятся все меньше и меньше, в их функционирование постепенно вмешиваются квантовые эффекты.»
М. Нильсен, И. Чанг [**17**, с.23]

Начала волновой кибернетики

Г л а в а 1

НАЧАЛА ВОЛНОВОЙ КИБЕРНЕТИКИ

Изначально данная глава имела другое название. Однако когда работа над книгой была практически завершена, стало ясно, что в ней содержится нечто большее, чем было задумано ранее. К тому же, как было выяснено, имеется ряд публикаций, которые показывают, что имеют место быть следующие самостоятельные научные направления:

- квантовая информация [**17**, **18**, **25**];
- квантовые алгоритмы [**17**, **98**, **99**];
- квантовая теория проверки гипотез и оценивания [**47**];
- квантовая статистика [**52**];
- квантовые игры и квантовые стратегии [**100**];
- квантовые нейронные сети [**86**].

При этом в классической кибернетике уже давно имеют самостоятельное и важное значение такие научные разделы, как:

- теория информации [**3**, **4**, **6**]; теория алгоритмов [**91**, **92**];
- теория проверки гипотез и оценивания [**44**, **49**];
- математическая статистика [**51**, **60**];
- теория игр (стратегии) [**101**]; нейронные сети [**82**].

Возникла идея ввести в название главы именно термин *волновая кибернетика*.

Под *волновой кибернетикой* авторы понимают все то, что связано с *классической кибернетикой,* но с учетом законов *квантовой механики.* Авторы не отрицают и тот факт, что квантовая механика, возможно, привнесет в этот раздел науки и что-то сугубо свое, именно присущее только квантовой механике. Возможно, когда-то термин *волновая кибернетика* будет заменен на какой-то другой (более подходящий) термин.

Волновая кибернетика возникла не на пустом месте. До нее существовала и активно развивалась классическая кибернетика, опирающаяся на законы классической физики.

Данная глава, по сути, содержит именно начала *волновой кибернетики*, именно то, от чего она отталкивается и с чего собственно и начинается.

1.1. Единица информации

> «Информация – не просто математическое понятие, она всегда имеет физическое воплощение, которое в традиционной теории информации следует законам классической физики, а в квантовой информатике – законам квантового мира.»
>
> *М. Нильсен* [**19**]

Содержание

Понятие информации. Понятие данных. Понятие базы данных (БД). Энтропия. Измерение информации. Квантовая информация.

Информация и данные

Важнейшим слагаемым нашего мира являются ***энергия***, ***вещество***, а также ***информация***.

Исследователи считают, что информация [**6**, с.9] "*является более трудным для исследования понятием, чем, скажем, энергия, занимающая определенное, давно выясненное место в физике*".

Термин *информация* (англ. – *information,* лат. – *informatio* (разъяснение, осведомление) [**12**, с.14]) появился (см. [**5**]) около 2.5 тысяч лет назад в латинском языке, а затем и в большинстве других языков. Огромное число людей в мире стало активно применять этот термин. Как правило, они вкладывали в этот термин практически одинаковый смысл [**5**]: "*сообщение, осведомляющее о положении дел, о состоянии чего-нибудь*".

Специалисты полагают [**5**], что "*источником всей информации является окружающий нас материальный мир*".

Информация – понятие в некотором смысле простое, а самое главное, практически не определяемое.

Специалистами принято, что есть (см. [**8**, с.12]) ***определения*** и есть ***понятия***. Определения, как правило, даются однозначно. Понятия обычно не даются однозначно, а вводятся с помощью примеров. Если в какой-то научной области необходимо ввести какое-то новое понятие, то делается это по-своему, т.е. так, как это наиболее удобно. Часть исследователей дают именно понятие об информации.

Однако в некоторых случаях делаются попытки дать все-таки определение, что такое информация.

Хорошо известно, что в любой области науки имеются свои простые, неопределяемые понятия, на которых данная наука основывается. Так, важным понятием науки информатики является *информация*. На данном этапе развития современной науки точное определение, что же такое *информация*, пока еще отсутствует.

Например, понятие множества относится к числу первоначальных математических понятий [**69**, с.759] и может быть пояснено только на примерах.

Определение термина *информация* много, они сложны и противоречивы. Из философии следует, что *информация* — это одно из основных, универсальных свойств материи, связанное с понятием отражения.

Для других областей науки *информацию* можно кратко определить как все те сведения, знания, сообщения, которые помогают решить ту или иную задачу (т.е. уменьшение неопределенности ее исходов).

В дальнейшем разумно использовать понятия, термины и различные определения в соответствии с различными нормативными документами, например ГОСТ 7.0-99 [**10**], ГОСТ 7.73-96 [**11**] и другие источники. Дадим некоторые определения информации.

Определение 1.1

Информация [**5**] — это отражение того разнообразия, которое существует во Вселенной.

Определение 1.2

Информация [**8**, с.13] — это продукт взаимодействия *данных* и адекватных им методов.

Определение 1.3

Информация [**10**] — это сведения, воспринимаемые человеком и(или) специальными устройствами как отражение **фактов** материального или духовного мира в процессе коммуникации (см. **ГОСТ 7.0-99**).

Определение 1.4

Информация [**16**] — это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления (см. **ГОСТ Р 51275-99**).

Определение 1.5

Информация [**12**, с.17] — это данные, необходимые и полезные тому, кому они передаются.

Определение 1.6

Информация [**12**, с.14] — содержание какого-либо сообщения, сведения о чем-либо, рассматриваемые в аспекте их передачи в пространстве и времени.

Определение 1.7

Информация [**12**, с.14] — сведения, подлежащие передаче.

Определение 1.8

Информация [**12**, с.14] — это значение, вкладываемое человеком в данные на основе известных соглашений, используемых для их представления.

Определение 1.9

Информация [**12**, с.14] — содержание, значение данных, которое видят в них люди. Обычно данные состоят из *фактов*, которые становятся информацией в определенном контексте и понятны людям.

Определение 1.10

Информация [**14**] — это сведения о чем-либо, рассматриваемые в процессе их передачи.

Определение 1.11

Информация [**12**, с.15] — это то, что сокращает степень неопределенности (у *К. Шеннона* — энтропии) у ее адресата о каком-либо объекте.

Определений термина *данные* (англ. *data*) также много и они различны. Понятие *информация* близко к понятию *данные*. Однако между ними есть различие. Не всегда эти термины используются как синонимы.

Определение 1.12
Данные [**8**, с.11] — это зарегистрированные *сигналы*.

Определение 1.13
Данные [**10**] — это *информация*, обработанная и представленная в *формализованном* виде для дальнейшей обработки (см. **ГОСТ 7.0-99**).

Определение 1.14
Данные [**12**, с.13] — некоторый факт, то, на чем основан вывод или любая интеллектуальная система.

Определение 1.15
Данные [**12**, с.13] — факт, понятие или инструкции, представленные в условной форме, удобной для пересылки, интерпретации и обработки человеком или автоматизированными средствами.

Для понимания, что же такое информация, очень важен следующий пример.

Пример 1.1, где есть (см. [**8**, с.13]) данные и методы (автор *Н. Винер* [**9**, с.237-238]).
“Допустим, я нахожусь в лесах вдвоем со **смышленым** дикарем, который не может говорить на моем языке, и на языке которого я тоже не могу говорить. Даже без какого-либо условного языка знаков, известного нам обоим, я могу многое узнать от него. Мне нужно лишь **быть особенно внимательным** в те моменты, когда он обнаруживает признаки волнения или интереса. Тогда я должен **посмотреть** вокруг, особенно в направлении его взгляда, и **запомнить** все, что увижу или услышу. Не пройдет много времени, как я **открою**, какие предметы представляются важными для него, – не потому, что он сообщил мне о них словами, но потому, что я сам их заметил.

Иначе говоря, сигнал, лишенный внутреннего содержания, может приобрести для моего спутника смысл по тому, что наблюдает он в данный момент, и может приобрести для меня смысл по тому, что наблюдаю я в данный момент. Способность дикаря замечать моменты моего особенно активного внимания сама по себе образует язык, возможности которого столь же разнообразны, как и диапазон впечатлений, доступных нам обоим" (выделения полужирным сделаны авторами) ■

ОТМЕТИМ [**8**, с.13]. В рассмотренном выше примере легко выделить набор *методов* (наблюдение и анализ) и *алгоритм* (посмотреть, запомнить, открыть), а также необходимость адекватности методов (дикарь должен быть смышленым, а наблюдатель — быть особенно внимательным).

Опыт показывает, что передача информации происходит посредством *сигналов*. На практике информация может передаваться в форме *сообщений* от источника к приемнику с помощью некоторого *канала связи* между ними. Сначала источник формирует сообщение. Это сообщение кодируется в сигнал. Затем этот сигнал посылается по каналу связи. После этого в приемнике может появиться принимаемый сигнал. Если он появился, то принятый сигнал **декодируется** и уже после этого становится принимаемым сообщением.

При всех трактовках понятия *информация* она предполагает существование ДВУХ объектов (рис. 1.1):

- *источника* информации;
- *приемника* информации.

Рис. **1.1.** Передача информации от *источника* к *приемнику*

ОТМЕТИМ. **Данные** — это *сигналы,* из которых еще надо извлечь информацию.

ОТМЕТИМ (см. [**8**, с.11]). Специалисты полагают, что все виды энергообмена сопровождаются появлением *сигналов*. Все сигналы имеют в своей основе материальную энергетическую природу. Если происходят взаимодействия сигналов с физическими телами, то в этих телах происходит возникновение определенных изменений свойств (которое называют *регистрацией сигналов*).

ОТМЕТИМ. Обработка данных — процесс приведения их к пригодному для этого виду (т.е. пригодному для извлечения информации).

Сам процесс передачи **ДАННЫХ** от *источника* к *потребителю* и восприятия в качестве **ИНФОРМАЦИИ** может быть представлен как прохождение ТРЕХ фильтров (рис. 1.2):

- *физического*;
- *семантического*;
- *прагматического*.

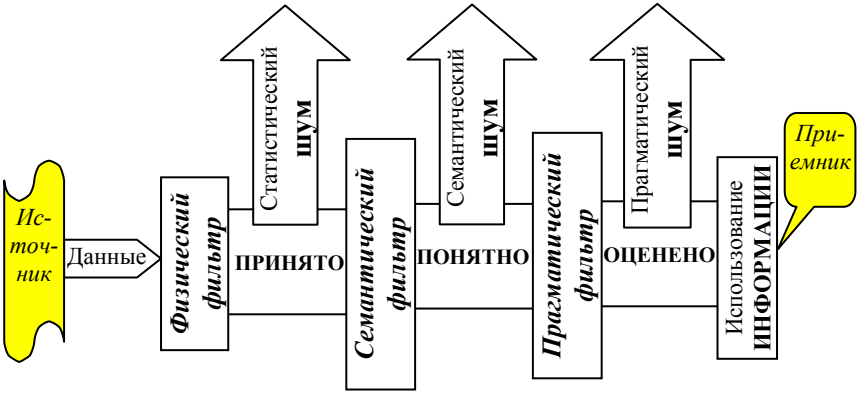


Рис. **1.2.** Процесс передачи и восприятия информации [**13**]

Для того чтобы быть **воспринятыми** и стать **информацией**, эти **данные** проходят как бы тройной фильтр (см. рис. 1.2):

- ***физический*** (через который поступают данные и, как правило, не все из-за ограниченности *пропускной способности канала*);
- ***семантический*** (где идет отбор тех данных, которые понятны получателю, т.е. соответствуют тезаурусу его знаний);
- ***прагматический*** (где оценивается полезность данных, т.е. отбор тех сведений, что полезны для решения данной задачи).

Поясним суть этих фильтров на следующем простом примере.

Пример 1.2. Есть Петя (*источник*), находящийся не дома и посылающий СООБЩЕНИЕ (СВЕДЕНИЯ о том, когда он будет дома) Маше (*приемнику*) по КАНАЛАМ сети Internet в виде E-mail. Маша при этом решает для себя ЗАДАЧУ (ответом на нее является ЗНАНИЕ (т.е. **ИНФОРМАЦИЯ**) о том, придет ли Петя домой или нет).

Тогда **ДАННЫЕ** — это файл письма на диске для передачи его Маше по E-mail:

"**Маша, я буду обязательно дома завтра! /Петя/.**"

При передаче СИГНАЛОВ по каналам сети Internet, т.е. пройдя ***физический фильтр***, было получено СООБЩЕНИЕ:

"**Маша, я буду об#56fgyj(0[]sdo дома за#154uув* /Петя/.**",

т.е. часть символов была потеряна и при этом появились другие символы.

Далее Маша пытается сделать ОТБОР тех **ДАННЫХ**, что ей понятны (***семантический фильтр***), и ей это удается. Она понимает часть фразы:

"**Маша, я буду об…о дома за… /Петя/.**"

После этого Маша пытается оценить (***прагматический фильтр***) ПОЛЕЗНОСТЬ **ДАННЫХ,** т.е. делает ОТБОР тех СВЕДЕНИЙ, что полезны ей для решения данной ЗАДАЧИ, и получает (оставляет, отбирает):

"**Маша, я буду дома /Петя/.**",

т.е. Маша ПОЛУЧИЛА необходимую ей **ИНФОРМАЦИЮ**, что содержалась в **ДАННЫХ**, переданных ей Петей по каналам связи. Тогда СВЕДЕНИЕ о том, что ***Петя будет дома*** — есть **ИНФОРМАЦИЯ**, полученная Машей■

Информация обладает следующими важными особенностями [**8**, с.14]:

- **динамический характер информации** (информация — не статичный объект, так как информация существует только в момент взаимодействия данных и методов (в момент передачи данных от источника к приемнику); информация пребывает в состоянии данных, т.е. она содержится в данных и лишь только в момент протекания информационного процесса информация существует) [**8**, с.14];
- **адекватность методов** (из одних и тех же данных можно получить разную информацию в зависимости от адекватности взаимодействующих с ними методов) [**8**, с.14];
- **диалектический характер взаимодействия данных и методов** (данные — объективны, так как они есть результат регистрации объективно существующих сигналов, а методы субъективны; *информация возникает и существует в момент диалектического взаимодействия объективных данных и субъективных методов*) [**8**, с.14].

Основополагающим и фундаментальным для информатики является понятие *информации*, используемое в теории информации, и понятие *данных*, используемое в теории баз данных.

В настоящее время ГОСТ 7.73-96 [**11**] определил понятия *информационно-поисковый массив* и *фактографическая база данных*. В вычислительной технике большую роль играют достаточно специфическая информация и данные, которые специалисты стали называть *фактографическими*. Опираясь на [**10** и др.] и используя принятые термины *информация* и *данные*, дадим следующие определения.

Определение 1.16

Фактографическая информация (ФИ) — информация, содержащая конкретные фактические сведения (сообщения) о конкретных фактах, о фактических событиях, характеризующие некоторый объект и позволяющие провести сопоставление его с аналогами.

ОТМЕТИМ. В качестве примера фактографической информации можно привести сведения о конкретном человеке: его фамилия, имя, место и дата рождения, телефон, E-mail, адрес прописки, рост, особые приметы, описание внешности.

Определение 1.17

Фактографические данные (ФД) — фактографическая информация, обработанная и представленная в формализованном виде для дальнейшей обработки.

ОТМЕТИМ [**12**, с.16]. Чтобы стать информацией, данные должны правильно *отражать* объект описания (иначе это уже будет так называемая ДЕЗинформация).

ОТМЕТИМ [**12**, с.17]. Данные, переданные не по назначению, не *своевременно* или не представляющие *новизну*, есть информационный шум.

ВАЖНО ПОМНИТЬ [**12**, с.16]. Чтобы стать информацией, данные должны быть *интересны* субъекту информирования и должны обладать *новизной*. Такие данные должны быть связаны с необходимостью решения некоторых *задач* и сокращать степень *неопределенности* о самом объекте интереса.

ВАЖНО [**12**, с.15]. Очень кратко признаки информации можно сформулировать следующим образом: "*Информация — это сведения или данные, объективно отражающие различные стороны и элементы окружающего мира и деятельности человека на определенном этапе развития общества, представляющие для него какой-либо интерес и материализованные в форме, удобной для использования, передачи, хранения и/или обработки (преобразования) человеком или автоматизированными средствами*".

Что можно делать с информацией (данными)?

Практика показала, что информацию можно:

- архивировать [**8**, с.18], хранить;
- защищать [**8**, с.18];
- создавать;
- уничтожать;
- копировать;
- восстанавливать;
- транспортировать [**8**, с.18], распространять, передавать, пересылать;
- принимать;
- обрабатывать;
- уменьшать, терять;
- находить, собирать [**8**, с.18], искать, накапливать;
- оценивать, измерять;
- использовать, воспринимать, пропускать;
- преобразовывать [**8**, с.18], изменять, искажать;
- продавать, покупать, обменивать;
- сортировать [**8**, с.18];
- фильтровать [**8**, с.18];
- формализовать [**8**, с.18];
- др.

Какими свойствами может обладать информация (данные)?

- Полнота [**8**, с.15];
- достоверность [**8**, с.15], точность;
- своевременность;
- краткость, избыточность;
- непрерывность, дискретность [**31**, с.14];
- адекватность [**8**, с.15];
- доступность [**8**, с.14];
- актуальность [**8**, с.14];
- ценность, важность;
- объективность (субъективность) [**8**, с.15];
- понятность;
- др.

Технические специалисты, например *Дж. Мартин* и др., определяют ***базу данных*** *"...как совокупность взаимосвязанных хранящихся вместе данных при наличии такой минимальной избыточности, которая допускает их использование оптимальным образом для одного или нескольких приложений; данные запоминаются так, чтобы они были независимы от программ, использующих эти данные; для добавления новых или модификации существующих данных, а также для поиска данных в базе данных применяется общий управляемый способ..."* [**15**, с.28].

Согласно ГОСТ 7.73-96 база данных — это несколько другой объект.

Определение 1.18

База данных (**БД**) [**11**] — это набор данных, который достаточен для установленной цели и представлен на *машинном носителе* в виде, позволяющем осуществлять *автоматизированную* переработку содержащейся в нем *информации* (см. **ГОСТ 7.73-96**).

ОТМЕТИМ. Наряду с *классической* БД специалисты в работах [**86**, **75-78**] рассматривают и *квантовую* БД, реализованную на *квантовых* элементах (объектах).

Информация определяет многие процессы, происходящие в вычислительном устройстве. На практике различают *непрерывную* информацию и *дискретную* информацию [**31**, с.14].

Единицы измерения данных. Наименьшей единицей измерения данных является *бит*, так на практике именно в *триггере* может храниться один бит данных. Следующей единицей является *байт*, содержащий 8 бит данных. Более крупной единицей является килобайт, содержащий 1024 байт данных. Более крупные единицы измерения образуются с использованием следующих префиксов: *мега-*, *гига-*, *тера-*.

Информация и энтропия

В 40-х гг. XX в. **ИНФОРМАЦИЯ** была определена через меру уменьшения НЕОПРЕДЕЛЕННОСТИ ЗНАНИЯ о совершении какого-либо СОБЫТИЯ. Такая мера была названа ЭНТРОПИЕЙ. У истоков науки об **ИНФОРМАЦИИ** стояли такие ученые как *Н.Винер, К. Шеннон, А.Н. Колмогоров, В.А. Котельников* и др.

ОТМЕТИМ [**1**, с.298]. Специалисты полагают, что наличие некоторой неопределенности связано с наличием некоторого беспорядка (или разупорядоченности). Устранение неопределенности связано с упорядочиванием. Причем энтропию можно рассматривать как саму меру беспорядка (или разупорядоченности).

Информационный объем сообщения на практике может быть измерен в ***битах,*** что соответствует числу двоичных цифр (нуля и единицы), которыми может быть закодировано это сообщение.

Слово *бит* — это [**1**, с.200] сокращение от английского словосочетания *binary digit* — двоичная цифра.

ОТМЕТИМ [**7**]. Неоднократные попытки численного измерения информации предпринимались давно, например, *Р. Фишером* (1921 г.), *Х. Найквист* (1924 г.), *Р. Хартли* (1928 г.), *К. Шенноном* (1948 г.) и др. Наиболее убедительные результаты были получены *К. Шенноном*. После этого началось интенсивное развитие теории информации.

Определение 1.19
Бит [**1**, с.200] — количество информации, которое содержится в ответе на вопрос, допускающий два равновероятных ответа.

ОТМЕТИМ [**1**, с.206]. Количество бит информации, необходимое для выбора определенного варианта из N равновероятных вариантов, равно $\log_2 N$.

Следующий наглядный пример (построенный по аналогии, как в работе [**1**, с.201]), представленный на рис. 1.3, достаточно наглядно демонстрирует понятие *бита информации*.

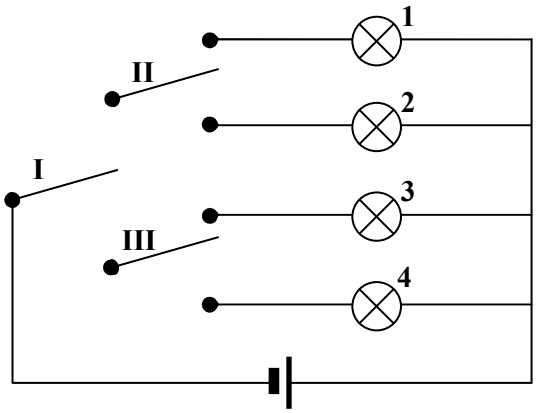


Рис. **1.3.** Пояснение понятия *бита информации*

На рис. 1.3 изображены 3 переключателя, источник питания и 4 лампочки, соединенные проводами с источником и с выключателями. Человек-оператор (или просто оператор) может поставить любой переключатель либо в верхнее положение, либо в нижнее, замыкая тем самым какую-то цепь. С помощью переключателя **I** можно подать сигнал либо на вход **II**, либо на вход переключателя **III**. С помощью переключателя **II** можно подать сигнал либо на лампу **1**, либо на лампу **2**. Аналогично с помощью переключателя **III** можно подать сигнал либо на лампу **3**, либо на лампу **4**. Каждый переключатель может быть установлен только в одном из двух положений: верхнее или нижнее (промежуточные положения недопустимы).

Закодируем сигнал, формируемый оператором посредством установки переключателя в верхнее положение как 0, а в нижнее положение как 1. Поставив в соответствующее положение каждый из переключателей, оператор тем самым сформирует сигнал, который включит одну из 4-х лампочек.

Например, сигнал 01 (рис. 1.4) включит лампочку 2, а сигнал 11 включит лампочку 4 и т.п.

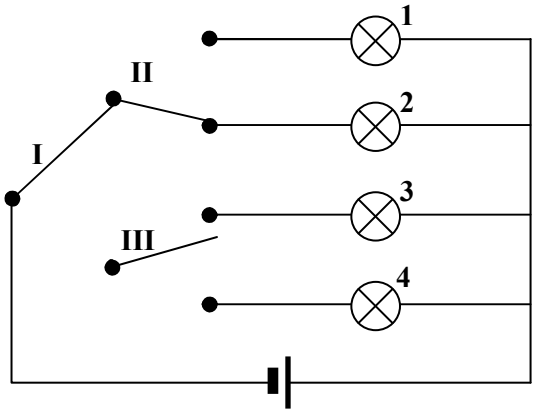


Рис. **1.4.** Сигнал 01 включает лампочку 2

Оператор, устанавливая переключатель в одно из двух положений, формирует сигнал (1 или 0), который содержит 1 бит информации.

Следующую формулу принято называть формулой *Хартли* [**1**, с.204; **2**, с.9,10,18]:

$$H=\log_2 N.$$

Формула *Хартли* позволяет вычислить количество информации, необходимое для выбора определенного варианта из N равновероятных вариантов.

Другую формулу

$$H=-\sum_{i=1}^{N} p_i \log_2 p_i \text{ , где } \sum_{i=1}^{N} p_i = 1$$

называют в теории информации формулой *Шеннона* [**1**, с.211; **2**, с.35]. Формула *Шеннона* позволяет вычислить количество информации, необходимое для выбора определенного варианта из N

НЕравновероятных вариантов, характеризующихся вероятностями p_1, p_2,… p_i,…, p_N (т.е. количество информации, произведенной одним выбором). В табл. 1.1 приведены вероятности p_i встречаемости символов в тексте на русском языке.

ОТМЕТИМ [**1**, с.299]. Неравновероятность вариантов снижает степень неопределенности и, как следствие этого, уменьшает количество информации.

ОТМЕТИМ [**1**, с.299]. В общем случае от того, какое множество вероятностей p_i количество информации H в битах может принимать значение от 0 до $\log_2 N$. Если p_7=1, а p_i=0, i=1, 2, 3, 4, 5 ,6, **8**, 9,…, N; то H=0 бит. Если p_i=1/N, i=1,…, N; то H=$\log_2 N$.

Таблица 1.1. Символы и их вероятности [**1**, с. 236; **4**, с. 238]

Символ	Вероятность p_i	Символ	Вероятность p_i
пробел	0.174	я	0.018
о	0.090	ы	0.016
е, ё	0.072	з	0.016
а	0.062	ь,ъ	0.014
и	0.062	б	0.014
т	0.053	г	0.013
н	0.053	ч	0.012
с	0.045	й	0.010
р	0.040	х	0.009
в	0.038	ж	0.007
л	0.035	ю	0.006
к	0.028	ш	0.006
м	0.026	ц	0.004
д	0.025	щ	0.003
п	0.023	э	0.003
у	0.021	ф	0.002

Поясним понятие энтропии на следующем интересном примере.

Пример 1.3 случайных предложений (автор *Р.Л. Добрушин*), “смысл” которых постепенно появляется [**1**, с.301-310; **4**, с.236-248].

№**1**. Вероятности p_i=1/32, i=1,…, N=32; H_1=$\log_2$32=5 бит, т.е. вероятности появления всех букв и пробела **равны**:

СУХЕРРОБЬДЩ ЯЫХВЩИЮАЙЖТЛФВНЗАГФОЕНВШТЦР ПХГБКУЧТЖЮРЯПЧЬКЙХРЫС

№**2**. Вероятности p_i взяты из табл. 1.1, H_2=4.35 бит, т.е. вероятности появления всех букв и пробела **не** равны (так как в текстах на русском языке):

ЕЫНТ ЦИЯЬА ОЕРВ ОДНГ ЬУЕМЛОЛЙК ЗБЯ ЕНВТША

№**3**. H_3 =3.52 бит, т.е. вероятности появления всех букв и пробела учитывают **1** предшествующую букву:

УМАРОНО КАЧ ВСВАННЫЙ РОСЯ НЫХ КОВКРОВ НЕДАРЕ

№**4**. H_4 =3.01 бит, т.е. вероятности появления всех букв и пробела учитывают **2** предшествующие буквы:

ПОКАК ПОТ ДУРНОСКАКА НАКОНЕПНО ЗНЕ СТВОЛОВИЛ СЕ ТВОЙ ОБНИЛЬ

№**5**. H_5 ≈2.5 бит, т.е. вероятности появления всех букв и пробела учитывают **3** предшествующие буквы:

ВЕСЕЛ ВРАТЬСЯ НЕ СУХОМ И НЕПО И КОРКО

№**6**. H_6 =0 бит, т.е. (см. [**1**, с.310])

$$H = 1\cdot\log_2 1 + \sum_{i=2}^{32} 0\cdot\log_2\frac{1}{0} = 0\,,$$

т.е. вероятность появления одной какой-то буквы (например, буквы А) есть p_m=1, а остальные есть p_i=0, i=1, 2,…, $\boldsymbol{m}$–1, $\boldsymbol{m}$+1, …, 32:

АААААААААААААААААААААААААААААААА

Некоторые оценки показывают [**1**, с.305], литературный текст обладает тем свойством, что энтропия буквы есть $H_{лит}$≈1 бит■

ВАЖНО (см. [**1**, с.310]). При сравнивании текстов №1-6 видно, что *плохо, когда энтропии очень много, и плохо, когда ее очень мало.*

По сравнению (см. [**1**, с.301-310]) с текстом №1 текст №2 более похож на осмысленный текст, выполненный на русском языке. Энтропия буквы в тексте №2 меньше, чем энтропия буквы в тексте №1. Для текста №3 характерно то, что он достаточно уже упорядочен, а его слова — почти легко произносимы в отличие от текста №1 и №2. Текст №4 все более приближается к реальным текстам (есть даже почти правильные слова). Текст №5 очень похож на осмысленный текст. Продолжая дальнейшие исследования в том же направлении, можно в итоге придти к тексту №6 с предельно большой дифференциацией вероятностей букв. Такой текст №6 соответствует ситуации абсолютного порядка (в то время как текст №1 соответствует ситуации наибольшего БЕСпорядка [**1**, с.302]). Специалисты полагают [**1**, с.309], что при уменьшении энтропии меньше 1-го бита на букву произойдет переход от *литературного текста* к некоторому специализированному тексту, который будет понятен соответствующим специалистам (более непонятным для непосвященных потребителей такого текста). Если рассмотреть обратный процесс [**1**, с.306] от литературного текста к тексту №1, то будет видно, что энтропия возрастает (растет беспорядок в тексте, уменьшается информация в нем).

ОТМЕТИМ [**1**, с.307]. Если выполнен переход от текста №1 к тексту литературному, то энтропия буквы уменьшится с 5 бит до 1 бита, а значит, получилось накопление информации в тексте в количестве 5 – 1=4 бит.

ВАЖНО (см. [**1**, с.306]). Все значения энтропии от H_1 до $H_{лит}$ могут быть получены с помощью формулы *Шеннона*.

ОТМЕТИМ [**5**]. Существуют две возможности для увеличения передаваемой информации. Одна — это необходимым образом изменить вероятность сообщения. Вторая — это увеличить число альтернатив или компонент, из которых набирается сообщение.

ВАЖНО (см. [**1**, с.298]). Можно полагать, что процесс получения информации соответствует некоторому процессу упорядочивания, что в итоге и означает процесс понижения энтропии.

ОТМЕТИМ [**5**]. Сама *природа информации*, а также возможность *измерения ценности* информации есть важная и интересная область дальнейших ее изучений.

ВАЖНО ПОМНИТЬ (см. [**1**, с.298]). Специалисты полагают, что можно рассматривать H, с одной стороны, как количество информации, которое устраняет неопределенность, а с другой стороны, как меру степени этой неопределенности.

Специалисты полагают [**20**, с.469], что любое *сообщение* в области теории информации — это некоторый "набор сведений о некоторой физической системе".

В качестве примера для физической системы можно привести **состояние** *автоматизированной фактографической информационно-поисковой системы* (АФИПС), в состав которой входит *фактографическая база данных* (ФБД). Современные АФИПС снабжены, как правило, средствами самоконтроля за состоянием ФБД. В случае несанкционированного изменения (удаления) записей ФБД (например, хакером-злоумышленником) эти средства самоконтроля посылают человеку-оператору (например, администратору АФИПС) специальное **текстовое** *сообщение* о текущем состоянии ФБД, например о нарушении целостности данных или о несанкционированном доступе к закрытым для посторонних пользователей данным. Такое текстовое сообщение содержит сведения о состоянии физической системы — ФБД в АФИПС.

Отметим следующее. Если администратору АФИПС уже известно, что ФБД несанкционированно изменена, то специальное текстовое *сообщение* только об этом не несет никакой дополнительной информации (т.е. не содержит интересующих администратора сведений).

В качестве другого примера физической системы можно привести персональный компьютер (ЭВМ).

При начальной загрузке ЭВМ выполняется тестирование аппаратуры, например оперативной памяти.

В случае обнаружения неисправностей человеку-оператору (например, пользователю) посылается специально закодированное **звуковое** *сообщение* в виде серии коротких и длинных гудков. Такое звуковое сообщение содержит сведения о состоянии физической системы (ЭВМ).

Отметим следующее. Если пользователю уже известно состояние ЭВМ, например, что ЭВМ неисправна, то специальное звуковое *сообщение* только об этом не несет никакой дополнительной информации для этого пользователя (т.е. не содержит интересующих пользователя сведений о состоянии ЭВМ).

В том случае, когда состояние *физической системы* (ФС) известно заранее получателю информации, то у него нет необходимости в ней, а значит, и нет необходимости в самой передаче *сообщения* от источника, содержащего сведения о состоянии ФС.

Для исследователей важно было понять, что значит *большая* или *меньшая* неопределенность и, самое главное, в чем ее можно на практике измерять.

Следуя работе [**20**, с.470], будем сравнивать две ФС, обозначенные как F_1 и F_2, каждая из которых обладает некоторой неопределенностью.

Предполагается, что каждая такая ФС может именно **случайно** оказаться в некотором состоянии — такой физической системе присуща *степень неопределенности*.

Поскольку состояния рассматриваемых систем случайны, то таким состояниям систем поставим во взаимно однозначное соответствие некоторые случайные события и некоторую *случайную величину* (**СВ**), например, системе F_1 — случайные события Z_i и случайную величину X, а системе F_2 — случайные события D_i и случайную величину Y.

Под $x_1,\ldots,x_m$ будем понимать конкретные числовые значения случайной величины X, а под $y_1,\ldots,y_n$ — конкретные числовые значения случайной величины Y.

Пример 1.4. Игральная кость (кубик) и монета [**20**, с.470].

Игральная кость на рис. 1.5**а** (правильная, т.е. симметричная) после подбрасывания может находиться только в равновозможных 6 состояниях:

1. Выпала цифра 1 (т.е. на верхней грани кубика цифра 1).
2. Выпала цифра 2 (т.е. на верхней грани кубика цифра 2).
3. Выпала цифра 3 (т.е. на верхней грани кубика цифра 3).
4. Выпала цифра 4 (т.е. на верхней грани кубика цифра 4).
5. Выпала цифра 5 (т.е. на верхней грани кубика цифра 5).
6. Выпала цифра 6 (т.е. на верхней грани кубика цифра 6).

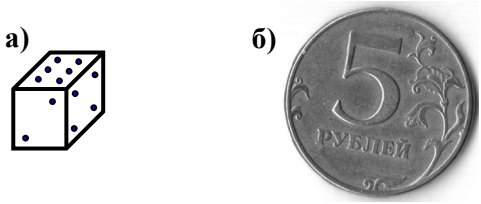


Рис. **1.5.** Игральная кость (кубик) и монета

Так как игральная кость правильная, то в априори (т.е. до получения сведений о результатах подбрасывания) вероятность каждого из 6 событий есть 1/6. В этом случае почти невозможно предсказать состояние такой физической системы (игральной кости).

Монета на рис. 1.5**б** (правильная, т.е. симметричная) после подбрасывания может, как и игральная кость, также находиться только в двух равновозможных состояниях: лежать *орлом* вниз или *решкой* (*решеткой*, т.е. цифрой) вниз.

Пусть в априори (т.е. до получения сведений) вероятность события, что монета лежит *решкой* вниз, есть 1/2, а вероятность события, что монета лежит *орлом* вниз, есть также 1/2.

Интуиция подсказывает, что неопределенность в первом случае с игральной костью значительно больше, чем в случае с монетой. У игральной кости больше возможных состояний, чем у монеты■

ОТМЕТИМ [**20**, с.470]. Степень неопределенности определяется числом возможных состояний системы. Однако этого еще недостаточно, так как важно еще что-то нечто другое.

Пример 1.5. Лампочка и монета.

Лампочка на рис. 1.6**а** после включения выключателя может находиться только в следующих двух состояниях:

лампочка исправна; лампочка перегорела.

а) **б)**

Рис. **1.6.** Лампочка и монета

Пусть в априори (т.е. до получения сведений) вероятность события, что лампочка исправна, есть 0.997, а вероятность события, что лампочка неисправна (перегорела), есть 0.003 . В этом случае можно почти наверняка предсказать состояние такой физической системы (лампочки) — ФС находится в исправном состоянии, т.е. лампочка исправна (принимая такое решение, только в 3 случаях из 1000 в среднем будет допущена ошибка). Такая ФС имеет достаточно малую степень неопределенности.

Монета на рис. 1.6**б** после подбрасывания может, как и лампочка, также находиться только в двух следующих состояниях:

монета лежит *орлом* вниз; монета лежит *решкой* вниз.

Пусть в априори (т.е. до получения сведений) вероятность события, что монета лежит *решкой* вниз, есть 0.5, а вероятность события, что монета лежит *орлом* вниз, есть также 0.5 .

В этом случае почти невозможно предсказать состояние такой физической системы (монеты) — ФС находится в состоянии, когда монета лежит *решкой* вниз (принимая такое решение, только в половине случаев из рассматриваемых в среднем будет допущена ошибка). Такая ФС уже имеет достаточно большую степень неопределенности по сравнению с другой ФС — лампочкой■

ВАЖНО ПОМНИТЬ [**20**, с.470]. Специалисты полагают, что в общем случае степень неопределенности определяется не только числом возможных состояний системы, но и вероятностью этих состояний.

Пример 1.6. Отгадывание числа (см. и ср. [**1**, с.200-203]).

Задумано некоторое целое число ***L*** от 0 до 7. Можно задавать вопросы в ответ, на которые можно получать ответы типа ДА или НЕТ. Сколько и какие вопросы следует задать, чтобы наверняка выяснить (отгадать) задуманное число ***L***?

Представим число ***L*** в двоичной системе счисления (табл. 1.2).

Таблица 1.2. Представление числа ***L***

Число ***L*** в десятичной системе счисления	Число ***L*** в двоичной системе счисления
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Таблица 1.3. Список вопросов для отгадывания числа ***L***

№ п/п	Текст вопроса
1	*Верно ли, что в двоичной записи загаданного числа равна единице 1-я слева цифра?*
2	*Верно ли, что в двоичной записи загаданного числа равна единице 2-я слева цифра?*
3	*Верно ли, что в двоичной записи загаданного числа равна единице 3-я слева цифра?*

Каждый вариант возможного числа ***L*** в двоичной системе счисления представлен однозначно трехзначным двоичным числом из нулей и единиц.

Поскольку такая двоичная запись неизвестного числа ***L*** является однозначной, то, определив число этих нулей и единиц, а также порядок их записи, можно однозначно восстановить и загаданное число ***L***. Для этого необходимо получить ответы на 3 вопроса (табл. 1.3), причем их можно задать все одновременно и получить затем все ответы сразу. Зная, какая двоичная цифра стоит на каком месте, можно однозначно выяснить, какое число ***L*** было задумано■

Пусть F — это некоторая физическая система (или техническая система), имеющая конечное множество состояний $\boldsymbol{s_1},\ldots, \boldsymbol{s_m}$. Такая физическая система с вероятностью $\boldsymbol{p_i}$ может находиться в $\boldsymbol{s_i}$–м состоянии. Таким образом, между множеством состояний $\boldsymbol{s_1},\ldots, \boldsymbol{s_m}$ и множеством вероятностей $\boldsymbol{p_1},\ldots, \boldsymbol{p_m}$ имеется взаимно однозначное соответствие (см. табл. 1.4), причем $\sum_{k=1}^{m} p_k = 1$.

ОТМЕТИМ [**20**, с.470]. Вероятность $\boldsymbol{p_i}=P(F\sim\boldsymbol{s_i})$ есть вероятность того, что физическая система F примет состояние $\boldsymbol{s_i}$. Здесь введено обозначение события $F\sim\boldsymbol{s_i}$, состоящего в том, что физическая система F находится в состоянии $\boldsymbol{s_i}$.

ОТМЕТИМ. Будем полагать, что событие $Z_{\boldsymbol{i}}$ ($\boldsymbol{i}=1,\ldots, \boldsymbol{m}$) есть $F\sim\boldsymbol{s_i}$, т.е. $Z_{\boldsymbol{i}}$ это событие, состоящее в том, что физическая система F находится в состоянии $\boldsymbol{s_i}$. Так как все события $Z_{\boldsymbol{i}}$ образуют полную группу событий, а их число $\boldsymbol{m}$ конечно, то событие, состоящее в объединении всех этих событий $\bigcup_{i=1}^{m} Z_i = \Omega$, есть достоверное событие и $\sum_{k=1}^{m} p_k = 1$.

Таблица 1.4. Состояния ФС F, события, вероятности и СВ

Состояние $\boldsymbol{s_k}$	Событие $Z_{\boldsymbol{k}}$	Вероятность p_k	Значения $x_{\boldsymbol{k}}$ случайной величины X
$\boldsymbol{s_1}$	Z_1	$\boldsymbol{p_1}$	x_1
$\boldsymbol{s_2}$	Z_2	$\boldsymbol{p_2}$	x_2
$\boldsymbol{s_3}$	Z_3	$\boldsymbol{p_3}$	x_3
⋮	⋮	⋮	⋮
$\boldsymbol{s_i}$	Z_i	$\boldsymbol{p_i}$	x_i
⋮	⋮	⋮	⋮
$\boldsymbol{s_{m-1}}$	Z_{m-1}	$\boldsymbol{p_{m-1}}$	x_{m-1}
$\boldsymbol{s_m}$	Z_m	$\boldsymbol{p_m}$	x_m

Если содержимое табл. 1.4 переписать в виде табл. 1.5, то можно заметить [**20**, с.471], что между физической системой $\boldsymbol{F}$, которая

может находиться в конечном числе m состояний, и **прерывной** случайной величиной X есть много общего.

Таблица 1.5. Ряд распределения случайной величины X

Вероятность события, что $X \sim x_k$	Значения x_k случайной величины X
p_1	x_1
p_2	x_2
p_3	x_3
⋮	⋮
p_i	x_i
⋮	⋮
p_{m-1}	x_{m-1}
p_m	x_m

ВАЖНО ПОМНИТЬ [**20**, с.471]. Совершено не важно, какие именно значения $x_1,\ldots, x_m$ записаны в правом столбце табл. 1.5, при этом важно именно количество этих значений m и величины вероятностей p_i.

Определение 1.20

Энтропией физической системы F [**20**, с.471] называется сумма произведений вероятностей различных состояний F, умноженная на логарифм этих вероятностей, взятых с обратным знаком:

$$H(F) = -\sum_{i=1}^{N} p_i \log_K p_i \ , \text{ где } \sum_{i=1}^{N} p_i = 1 \ ,$$

а выбор величины K основания логарифма соответствует выбору единицы измерения энтропии ($\lim\limits_{p\to 0}\left(-p\log_2 p\right) = 0$ [**4**, с.70, 72]).

ОТМЕТИМ. Под физической системой F можно понимать (т.е. поставить в соответствие) случайную величину X, где под $x_1,\ldots,x_N$ будем понимать конкретные числовые значения случайной величины X, а p_i — вероятность реализации случайного значения x_i.

ОТМЕТИМ [**1**, с.189, 258; **2**, с.7, 13]. Для обозначения энтропии обычно принят символ H, который был введен еще в работах (1868-1871 гг.) австрийского физика *Л. Больцмана*. Немецкий физик *Р. Клаузис* обозначал энтропию символом S (1865 г.).

Пример 1.7 (см. и ср. задачу №16 из [**4**, с. 76-77])

Имеются две урны (рис. 1.7), содержащие по 20 шаров.

В первой урне (рис. 1.7**а**) содержится 10 белых, 5 черных и 5 красных шаров. На рис. 1.7, 1.8, 1.9 приняты следующие обозначения для:

белых шаров — ○;
черных шаров — ●;
красных шаров — ⊗;
неизвестного шара — ⓘ.

Во второй урне (рис. 1.7**б**) содержится 8 белых, 8 черных и 4 красных шаров.

Из каждой урны наудачу (случайно) извлекли по одному шару (т.е. проводятся два опыта: первый опыт — извлечение шара из первой урны, а второй опыт — извлечение шара из второй урны).

Исход какого из этих двух опытов следует считать более неопределенным?

Рис. **1.7.** Исходное состояние 1-й и 2-й урны с 20 шарами

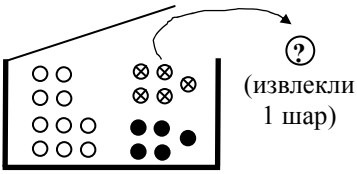


Рис. **1.8.** Из 1-й урны взяли 1 какой-то шар

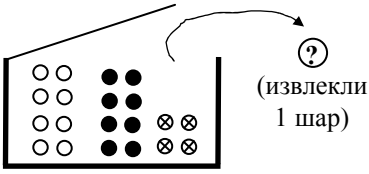


Рис. **1.9.** Из 2-й урны взяли 1 какой-то шар

Решение

1). Вычислим вероятности p_i, i=1, 2, … , N=3 для каждого из опытов и результаты расчетов запишем в две таблицы (табл. 1.6, 1.7):

Для первого опыта справедливо

$$p_1 = \frac{10}{20};\ p_2 = \frac{5}{20} = \frac{1}{4};\ p_3 = \frac{5}{20} = \frac{1}{4}.$$

Таблица 1.6. Первый опыт

Цвет вынутого шара	белый	черный	красный
Вероятность p_i	1/2	1/4	1/4
i	1	2	3

Для второго опыта справедливо

$$p_1 = \frac{8}{20} = \frac{2}{5};\ p_2 = \frac{8}{20} = \frac{2}{5};\ p_3 = \frac{4}{20} = \frac{1}{5}.$$

Таблица 1.7. Второй опыт

Цвет вынутого шара	белый	черный	красный
Вероятность p_i	2/5	2/5	1/5
i	1	2	3

2). Вычислим энтропию H_1 и H_2 для каждого из двух опытов:

$$H_1 = -\left\{\frac{1}{2}\log_2\frac{1}{2}\right\} - \left\{\frac{1}{4}\log_2\frac{1}{4}\right\} - \left\{\frac{1}{4}\log_2\frac{1}{4}\right\} = 1.50$$

$$H_2 = -\left\{\frac{2}{5}\log_2\frac{2}{5}\right\} - \left\{\frac{2}{5}\log_2\frac{2}{5}\right\} - \left\{\frac{1}{5}\log_2\frac{1}{5}\right\} \approx \frac{4}{5}\cdot 1.32 + \frac{1}{5}\cdot 2.32 \approx 1.52$$

3). Так как $H_2 > H_1$, то исход второго опыта является более неопределенным, чем исход первого опыта.

4). И тем самым задача решена■

Определение 1.21

Под объединением двух физических систем F_1 и F_2 [**20**, с.475] понимается сложная система $\boldsymbol{W}=(F_1, F_2)$, состояния которой представляют собой все возможные комбинации состояний $\boldsymbol{s_{1i}}$, $\boldsymbol{s_{2j}}$ систем F_1 и F_2 (причем $\boldsymbol{s_{1i}}$ — возможные состояния системы F_1, а $\boldsymbol{s_{2i}}$ — возможные состояния системы F_2, где i=1, 2,…, N1; j=1, 2,…, N2).

ОТМЕТИМ. Под двумя физическими системами F_1 и F_2 можно понимать (поставить в соответствие) две случайные величины X и Y, где под $\boldsymbol{x_1}$,…, $\boldsymbol{x_{N1}}$ будем понимать конкретные числовые значения X, а под $\boldsymbol{y_1}$,…, $\boldsymbol{y_{N2}}$ — конкретные числовые значения случайной величины Y. Система (X, Y) имеет распределение P_{ij} , где P_{ij} — вероятность реализации пары случайных значений ($\boldsymbol{x_i}$, $\boldsymbol{y_j}$).

Определение 1.22

Энтропией сложной системы $\boldsymbol{W}=(F_1, F_2)$ (см. и ср. [**20**, с.476]) называется сумма произведений вероятностей различных состояний такой сложной системы, умноженная на логарифм этих вероятностей, взятых с обратным знаком:

$$H\left(W\right)=H(F_1,F_2)=-\sum_{i=1}^{N1}\sum_{j=1}^{N2}\left\{P_{ij}\cdot\log_K\left(P_{ij}\right)\right\},$$

где $\sum_{i=1}^{N1}\sum_{j=1}^{N2}\left\{P_{ij}\right\}=1$, а выбор величины $\boldsymbol{K}$ основания логарифма соответствует выбору единицы измерения энтропии.

ОТМЕТИМ. Для случайных величин X и Y справедливо аналогичное выражение:

$$H_{X,Y}=H(X,Y)=-\sum_{i=1}^{N1}\sum_{j=1}^{N2}\left\{P_{ij}\cdot\log_K\left(P_{ij}\right)\right\}.$$

Определение 1.23

Условная энтропия $H(Y|X)$ случайных величин X и Y или систем F_1, F_2 (см. и ср. [**20**, с.478]) есть:

$$H(Y \mid X) = -\sum_{i=1}^{N1}\sum_{j=1}^{N2}\left\{P_{ij}\cdot\log_K\left(P\left(y_j \mid x_i\right)\right)\right\}.$$

ОТМЕТИМ. Вероятности P_{ij} событий ($X\sim \boldsymbol{x_i}$, $Y\sim \boldsymbol{y_j}$), вероятности p_i событий ($X\sim\boldsymbol{x_i}$) и вероятности r_j событий ($Y\sim\boldsymbol{y_j}$) представлены в табл. 1.8, т.е. [**20**, с.475-480] $P_{ij}=P((X\sim\boldsymbol{x_i})\ (Y\sim\boldsymbol{y_j}))$, $p_i=P(X\sim\boldsymbol{x_i})$, $r_j=P(Y\sim\boldsymbol{y_j})$, $P_{ij}= p_i\cdot P(\boldsymbol{y_j}|\ \boldsymbol{x_i})$, $P_{ij}= r_j\cdot P(\boldsymbol{x_i}|\boldsymbol{y_j})$.

Таблица 1.8. Вероятности P_{ij} для (X, Y)

Y	X						r_k
	$\boldsymbol{x_1}$	$\boldsymbol{x_2}$	…	$\boldsymbol{x_i}$	…	$\boldsymbol{x_{N1}}$	
$\boldsymbol{y_1}$	P_{11}	P_{21}	…	P_{i1}	…	P_{N11}	$\boldsymbol{r_1}$
$\boldsymbol{y_2}$	P_{12}	P_{22}	…	P_{i2}	…	P_{N12}	$\boldsymbol{r_2}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$\boldsymbol{y_j}$	P_{1j}	P_{2j}	…	P_{ij}	…	P_{N1j}	$\boldsymbol{r_j}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$\boldsymbol{y_{N2}}$	P_{1N2}	P_{2N2}	…	P_{iN2}	…	$P_{N1\,N2}$	r_{N2}
p_k	$\boldsymbol{p_1}$	$\boldsymbol{p_2}$	…	$\boldsymbol{p_i}$	…	$\boldsymbol{p_{N1\,N2}}$	—

Основные свойства *энтропии* приведены в табл. 1.9.

Таблица 1.9. Основные формулы и свойства энтропии

№ п/п	Свойство	Примечание
1	$H=\log_2 N$	Формула *Хартли* [**1**, с.204; **2**, с.9,10,18]
2	$H=-\sum_{i=1}^{N} p_i \log_2 p_i$, где $\sum_{i=1}^{N} p_i = 1$	Формула *Шеннона* (при $p_i = 1/N$ формула *Шеннона* превращается в формулу *Хартли*). Если для некоторого значения i вероятность $\boldsymbol{p_i}=0$, то следует принять, что $(-\boldsymbol{p_i}\log_2\boldsymbol{p_i})=0$, т.е. если дополнить множество возможных значений СВ, включив в него произвольное число значений с нулевыми вероятностями, то энтропия СВ останется без изменения [**2**, с.14]
3	$H\geq 0$	Энтропия СВ неотрицательна [**2**, с.14]
4	$H=0$	Энтропия СВ равна нулю только тогда, когда одно из ее значений имеет вероятность, равную 1 (т.е СВ фактически является детерминированной) [**2**, с.14]
5	$H=f(\boldsymbol{p_i})$	Энтропия является непрерывной функцией $f(\boldsymbol{p_i})$ своих аргументов $\boldsymbol{p_i}$, $i=1, 2,\ldots, N$ [**2**, с.14]
6	$\max_{p_i,\, i=1,2,\ldots,N} f(p_i)=\log_2 N$ $f(p_i)=\left\{-\sum_{i=1}^{N} p_i \log_2 p_i\right\}$	Среди всех СВ, у которых конечное число возможных значений равно N, максимальную энтропию имеет равномерно распределенная на этом множестве случайная величина [**2**, с.14]

Таблица 1.9 (окончание)

7	$H(X, Y) = H(X) + H(Y)$ $H(X \mid Y)=H(Y)$	При объединении независимых систем X и Y (случайных величин) их энтропии складываются [**20**, с.476]
8	$H(X, Y) = H(X) + H(Y \mid X)$ $H(X, Y) = H(Y) + H(X \mid Y)$	При объединении систем X и Y (случайных величин) энтропия объединенной системы (X, Y) равна энтропии одной из ее составных частей плюс условная энтропия второй части относительно первой [**20**, с.479; **2**, с.46]
9	$H(X,Y) = -\sum_{i=1}^{N1}\sum_{j=1}^{N2}\{f_{ij}\}$ $f_{ij} = P_{ij} \cdot \log_K\left(P_{ij}\right)$	Расчетная формула для $H(X, Y)$
10	$H(X \mid Y)=0$	Состояние одной системы Y (т.е. СВ) полностью определяет собой состояние другой системы X [**20**, с.480]
11	$H(X, Y) = H(X) = H(Y)$	Системы X и Y (т.е. СВ) эквивалентны, т.е. состояния каждой из систем X, Y однозначно определяет состояние другой [**20**, с.480]
12	$H(X \mid Y) \le H(X)$	Условная энтропия не может превосходить безусловную энтропию [**2**, с. 40]
13	$H(X \mid Y_1 Y_2 \ldots Y_M) \le \ldots \le H(X \mid Y_1) \le$ $\le H(X)$	Каждое дополнительное условие к уже имеющимся не увеличивает энтропии СВ (системы) [**2**, с. 41]

Представленные сведения дают только общее представление о проблемах, связанных с энтропией. Однако это дает возможность далее ввести численный показатель о количестве информации. Перейдем к его краткому рассмотрению.

Количество информации

Пусть имеются две физические системы

$$F_1$$

и

$$F_2$$

и соответствующие им две случайные величины

$$X$$

и

$$Y.$$

Если СВ X имеет известное априорное распределение вероятностей, то эта СВ X характеризуется энтропией (в битах) [**20**, с.471]:

$$H\left(X\right) = H_X = -\sum_{i=1}^{N} p_i \log_2 p_i \ .$$

Далее, если проводится эксперимент (опыт о случайным исходом), в результате которого измеряют значение СВ X и получают ее конкретное значение $\boldsymbol{x_i}$, то вполне допустимо, что исходная неопределенность, характеризующаяся величиной H_X, не будет полностью снята, т.е. она будет не увеличена (а вполне возможно, что и уменьшена).

Определение 1.24

Количество информации [**2**, с.53] об X, содержащееся в случайной величине Y, есть разность энтропий X

до (H_{Xapr}=H_X)

и

после (H_{Xaprs}= $H_{X|Y}$= $H(X\,|Y)$)

проведения эксперимента (опыта)

$$I_{X|Y} = H_X - H_{X|Y} \ .$$

Основные свойства $I_{X|Y}$ приведены в табл. 1.10.

Таблица 1.10. Основные свойства $\boldsymbol{I_{X|Y}}$ (см. [**2**, с.53-60])

№ п/п	Свойство	Примечание
1	$I_{X\|Y}=0$	Если СВ X и Y независимы
2	$I_{X\|Y}\geq 0$	Количество информации неотрицательно
3	$I_{X\|Y}=I_{Y\|X}$	Количество информации о СВ X, содержащееся в случайной величине Y, равно количеству информации об Y, содержащемуся в случайной величине X
4	$\max\limits_{Y}\left\{I_{X\|Y}\right\}=H_X$	Максимальное количество информации об X, которое может быть извлечено из эксперимента над СВ Y, равно энтропии H_X
5	$I_{X\|Y}=H_X-H_{X\|Y}$	Первая расчетная формула для $I_{X\|Y}$
6	$I_{X\|Y}=H_X+H_Y-H_{X,Y}$	Вторая расчетная формула для $I_{X\|Y}$. Если две ФС (или две СВ X и Y) объединяются в одну, то [**20**, с.479] энтропия объединенной системы есть $H_{X,Y}$
7	$I_{X\|Y,Z}=H_X-H_{X\|Y,Z}$	Расчетная формула для $I_{X\|Y,Z}$
8	$I_{X\|Y}\leq I_{X\|Y,Z}$ $I_{X\|Z}\leq I_{X\|Y,Z}$	Дополнительный эксперимент к ранее проведенным не уменьшает количества извлеченной информации о СВ

Рассмотрим важный пример, связанный с расчетом количества информации.

Пример 1.8 (см. и ср. [**2**, с. 60-61])

Контроль знаний студентов по курсу “Основы квантовых вычислений” проводится по двухбалльной системе: зачет — незачет. Имеется только две группы студентов: ***A*** и ***B***.

При оценке знаний студентов преподаватель может допускать следующие ошибки:

- если студент владеет предметом (т.е. действительно заслуживает оценку “зачет”), то преподаватель ошибается с вероятностью 0.05**;**
- если студент не владеет предметом (т.е. действительно заслуживает оценку “незачет”), то преподаватель ошибается с вероятностью 0.1 **.**

В группе ***A*** только 80 % студентов действительно заслуживают оценку “зачет”, а в группе ***B*** таких студентов только 30 %.

В какой из групп оценка преподавателя дает большую информацию о знаниях студента?

Решение

1). Введем две случайные величины ***X*** и ***Y*** следующим образом:

$$X = \begin{cases} 0, & \textit{если студент не владеет предметом}; \\ 1, & \textit{если студент владеет предметом}; \end{cases}$$

$$Y = \begin{cases} 0, & \textit{если преподаватель ставит "незачет"}; \\ 1, & \textit{если преподаватель ставит "зачет"}. \end{cases}$$

Требуется вычислить $I_{X|Y}$ для группы ***A*** (т.е. $I^{A}_{X|Y}$) и $I_{X|Y}$ для группы ***B*** (т.е. $I^{B}_{X|Y}$) и затем определить, что больше — $I^{A}_{X|Y}$ или $I^{B}_{X|Y}$.

2). Воспользуемся свойством $I_{X|Y} = I_{Y|X}$ и будем вычислять $I_{Y|X}$, (поскольку так будет удобнее) следующим образом:

$$I_{Y|X} = H_Y - H_{Y|X},$$

$$H_Y = -\sum_{i=0}^{1} p_i \ln p_i \ ,$$

$$H_{Y|X} = H(Y \mid X) = -\sum_{i=0}^{1}\sum_{j=0}^{1}\left\{P_{ij}\cdot \ln\left(P\left(y_j \mid x_i\right)\right)\right\},$$

где $\boldsymbol{p_i}$ — вероятность реализации случайного значения $\boldsymbol{i}$ для $\boldsymbol{Y}$ (т.е. $\boldsymbol{i}$=0 или $\boldsymbol{i}$=1), а $P_{ij}= p^{\boldsymbol{A}}{}_i \cdot P(\boldsymbol{y_j}|\boldsymbol{x_i})$ или $P_{ij}= p^{\boldsymbol{B}}{}_i \cdot P(\boldsymbol{y_j}|\boldsymbol{x_i})$, $p^{\boldsymbol{A}}{}_i$, $p^{\boldsymbol{B}}{}_i$ — вероятность реализации значения $\boldsymbol{i}$ случайной величины $\boldsymbol{X}$ для группы $\boldsymbol{A}$ и $\boldsymbol{B}$ соответственно.

Найдем вероятности $\boldsymbol{p_i}$, а затем и H_Y:

$\boldsymbol{p_0}$=0.8·0.05+0.2·0.9=0.22 (для “незачет”);

$\boldsymbol{p_1}$=0.8·0.95+0.2·0.1=0.78 (для “зачет”);

$$H_Y = -\sum_{i=0}^{1} p_i \ln p_i = \left[0.22\cdot \ln 0.22\right] + \left[0.78\cdot \ln 0.78\right] = 0.5269 \text{ нат.}$$

Найдем вероятности $P(\boldsymbol{y_j}|\boldsymbol{x_i})$, $\boldsymbol{P_{ij}}$, а и затем $H_{Y|X}$:

$P(\boldsymbol{y_j}=0|\boldsymbol{x_i}=0)=0.9$; $P(\boldsymbol{y_j}=0|\boldsymbol{x_i}=1)=0.05$;

$P(\boldsymbol{y_j}=1|\boldsymbol{x_i}=0)=0.1$; $P(\boldsymbol{y_j}=1|\boldsymbol{x_i}=1)=0.95$.

Найдем вероятности $\boldsymbol{P_{ij}}$, а затем и $H_{Y|X}$ для группы $\boldsymbol{A}$:

$p^{\boldsymbol{A}}{}_0=0.2$; $p^{\boldsymbol{A}}{}_1=0.8$;

$\boldsymbol{P_{00}}= p^{\boldsymbol{A}}{}_0 \cdot P(\boldsymbol{y_j}=0|\boldsymbol{x_i}=0)=0.2\cdot 0.9=0.18$;

$\boldsymbol{P_{01}}= p^{\boldsymbol{A}}{}_0 \cdot P(\boldsymbol{y_j}=1|\boldsymbol{x_i}=0)=0.2\cdot 0.1=0.02$;

$\boldsymbol{P_{10}}= p^{\boldsymbol{A}}{}_1 \cdot P(\boldsymbol{y_j}=0|\boldsymbol{x_i}=1)=0.8\cdot 0.05=0.04$;

$\boldsymbol{P_{11}}= p^{\boldsymbol{A}}{}_1 \cdot P(\boldsymbol{y_j}=1|\boldsymbol{x_i}=1)=0.8\cdot 0.95=0.76$;

$$H_{Y|X} = -\sum_{i=0}^{1}\sum_{j=0}^{1}\left\{P_{ij}\cdot \ln\left(P\left(y_j \mid x_i\right)\right)\right\} = 0.2238 \text{ нат.}$$

Вычислим информацию $I^{\boldsymbol{A}}{}_{X|Y}$ для группы $\boldsymbol{A}$:

$$I^{\boldsymbol{A}}{}_{X|Y}=I_{Y|X}= H_Y - H_{Y|X} =0.5269\text{-}0.2238=0.303 \text{ нат.}$$

Проводя аналогичные вычисления, можно получить, что [**2**, с. 90]:

$$I^{\boldsymbol{B}}{}_{X|Y} =0.333 \text{ нат.}$$

3). Сравнение $I^{\boldsymbol{A}}{}_{X|Y}$ с $I^{\boldsymbol{B}}{}_{X|Y}$ показывает, что больше $I^{\boldsymbol{B}}{}_{X|Y}$, а значит оценка преподавателя дает большую информацию о знаниях студента группы $\boldsymbol{B}$.

4). И тем самым задача решена■

Определение 1.25

Количество информации от события к событию [**20**, с.492] — частная информация о событии, получаемая в результате сообщения о другом событии, равна логарифму отношения вероятности первого события после сообщения к его же вероятности до сообщения (априори):

$$I_{y_j \to x_i} = \log_K \left\{ \frac{P\left(x_i \mid y_j\right)}{p_i} \right\}.$$

ОТМЕТИМ [**20**, с.492]. Информация *от события к событию* обладает неожиданным свойством — она может быть как положительной, так и отрицательной.

Рассмотрим следующий достаточно простой пример с урной и шарами, связанный с наблюдением одного события по отношению к другому событию, где требуется вычислить количество информации.

Пример 1.9 (см. [**20**, с. 493])

В урне 3 белых и 4 черных шара (рис. 1.10). Из урны вынуто 4 шара, три из них оказались черными, а один — белым (рис. 1.11).

Определить информацию, заключенную в наблюдаемом событии ***B***, по отношению к событию ***A*** — следующий вынутый из урны шар будет черным (рис. 1.12).

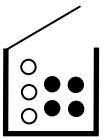


Рис. **1.10.** Исходное состояние урны и шаров

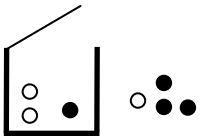


Рис. **1.11.** Состояние урны после извлечения 4-х шаров

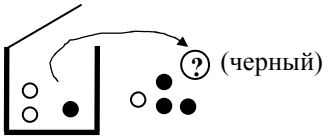


Рис. **1.12.** Событие ***A*** — следующий вынутый шар будет черным

Решение

1). Событие ***B*** состоит в том, что из урны случайно было вынуто 4 шара, три из них оказались черными, а один — белым:

$$\boldsymbol{B} = \{\textit{вынуто 4 шара: 3 черных и 1 белый шар}\},$$

а событие ***A*** есть

$$\boldsymbol{A} = \{\textit{следующий вынутый из урны шар будет черным}\}.$$

2). Найдем условную вероятность $P(\boldsymbol{A}|\boldsymbol{B})$, а затем и $P(\boldsymbol{A})$:

$$P(\boldsymbol{A}|\boldsymbol{B})=1/3;\ \ P(\boldsymbol{A})=4/7.$$

3). Вычислим количество информации от события ***B*** к событию ***A***:

$$I_{B\to A} = \log_K \left\{ \frac{P(A\,|\,B)}{P(A)} \right\} = \log_{K=2} \left\{ \frac{1/3}{4/7} \right\} = \log_2 \left\{ \frac{7}{12} \right\} \approx -0.778 \text{ бит.}$$

4). И тем самым задача решена■

ОТМЕТИМ [**2**, с.9; **20**, с.570]. Для перевода одних логарифмов в другие можно воспользоваться формулой $\log_K x = \log_K M \cdot \log_M x$; $\log_2 10 \approx 3.32193$.

В вычислительной технике бит *информации* хранится в наименьшем элементе памяти ЭВМ, необходимом для хранения одного из двух двоичных знаков 1 и 0, которые используются для представления *данных* и команд. На практике обычно таким элементами памяти являются *триггеры,* из которых собирается *регистр*, содержащий, как правило, 8 триггеров.

Двоичный канал связи без помех

Для передачи информации от источника к приемнику применяют специальное техническое средство, называемое *каналом связи*. На практике при реализации различных технических систем используются разнообразные каналы связи. Принято полагать [**1**, с.221], что одним из главных элементов канала связи является *линия связи*. В качества примера линии связи можно привести оптическое волокно для сети Интернет, телефонный кабель, а также некоторое пространство [**1**, с.221], разделяющее отправителя и получателя. В процессе передачи по линии связи сигнал обычно

как-то *искажается* (может ослабевать). Искажения происходят вследствие возникновения помех (различных шумов). Полагают, что эти помехи имеют статистический характер.

Специалистами разработаны различные методы, позволяющие бороться с возникающими искажениями в процессе передачи сигнала. Обычно (рис. 1.13) на входном конце канала связи расположен блок кодирующего устройства, а на выходном конце канала связи находится блок декодирующего устройства.

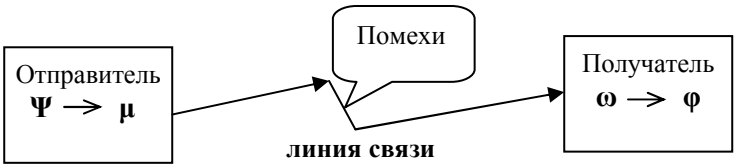


Рис. **1.13.** Передача по каналу связи

Задача кодирующего устройства — преобразовать входное сообщение (сигнал) **Ψ** в последовательность **μ** некоторых так называемых *элементарных сигналов*, например, в закодированную последовательность нулей и единиц. Такая последовательность нулей и единиц поступает в линию связи.

При передаче по линии связи в идеальных условиях (при отсутствии помех (искажений)) на выходе линии связи на вход декодирующего устройства поступает сигнал **ω.**

Так как условия передачи идеальные, то **ω** в точности повторяет сигнал **μ**, т.е. на вход декодирующего устройства поступает тот же набор нулей и единиц, который и был передан в линию связи. В случае наличия помех эти двоичные наборы могут уже не совпадать. На выход декодирующего устройства в общем случае поступает сообщение (сигнал) **φ**. В случае отсутствия помех при исправности самого декодирующего устройства сообщение **φ** должно в точности соответствовать сообщению **Ψ**.

Тот, кто передает сообщение (*отправитель*), применяет для формирования самого сообщения на входе канала связи некоторый набор символов (букв) или другими словами — *алфавит*. Сообщение представляет собой некоторый набор символов, причем сам выбор какого-либо символа привносит какую-то информацию в количестве ***H***, которое называют энтропией (*энтропией символа*

сообщения). Для получателя сообщения сама степень неопределенности отнесения к символу и есть ***H***.

Вернемся к рис. 1.13: получателю сообщения известен алфавит, однако несмотря на это получатель не знает отправленный текущий символ (и естественно весь набор символов) по линии связи, т.е. сам получатель находится в некоторой неопределенности. После принятия получателем сообщения неопределенность изменяется (т.е. получатель получит информацию в расчете на один символ сообщения в количестве ***H***).

Пусть ***C*** — это пропускная способность (или, как принято говорить, емкость) канала связи, которая измеряется в *бит/с*, т.е. в количестве битов данных, переданных за одну секунду.

Здравый смысл подсказывает, что на практике, чтобы не терять данные при передаче их по каналу связи, максимальная скорость ***v*** ввода данных (информации) в канал связи должна быть как-то согласована с самой пропускной способностью этого канала связи, т.е. с ***C*** и ***H***. Эта согласованность определяется следующим простым соотношением:

$$v \le C/H.$$

Если скорость ***v*** больше величины ***C/H***, то неизбежны потери данных (информации) при передаче их по такому каналу связи.

К. Шеннон доказал следующую замечательную теорему.

Основная теорема Шеннона [**1**, с.253]

Для любой линии связи с помехами всегда можно подобрать специальный код, позволяющий передавать сообщения по этой линии с заданной скоростью, сколь угодно близкой к максимально возможной скорости $v=C/H$, так, чтобы вероятность ошибки в определении каждой переданной буквы оказалась меньше любого заранее заданного числа ε ■

Важно заметить, что сама теорема не дает ответа на вопрос о том, что это за помехоустойчивые коды. Эта теорема показывает, что такие коды существуют. Действительно, впоследствии такие коды были найдены, и в науке появилась *теория кодирования*. Основная идея этих кодов состоит [**1**, с.253] в кодировании не отдельных символов, а сразу достаточно длинных последовательностей (блоков) из большого числа символов.

Пример 1.10 помехоустойчивого кода (см. [**1**, с. 253-254]).

Пусть некоторый блок данных состоит из следующих 16 двоичных цифр (т.е. нулей и единиц):

1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1.

Для того чтобы закодировать такой блок, надо добавить к этой двоичной последовательности еще одну двоичную последовательность из следующих 8 проверочных двоичных цифр:

0 1 1 0 1 1 0 0.

Таким образом, в линию связи будет передана следующая более длинная последовательность из 24 двоичных цифр:

1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 **0 1 1 0 1 1 0 0**.

Первые 16 цифр содержат сведения (передаваемое сообщение), следующие 8 цифр являются проверочными, т.е. служат для проверки передаваемого сообщения.

В случае наличия помех, если при передаче по линии связи возникнет ошибка, например какая-то цифра будет передана неправильно (т.е. вместо нуля будет передана единица или вместо единицы будет передан нуль), то проверочные коды позволят установить наличие искажения в переданном сигнале.

Для этого запишем внутри квадратной таблицы четыре четверки информационных цифр с указанием проверочных кодов, разделенных на две четверки таким образом, как показано на рис. 1.14, 1.15.

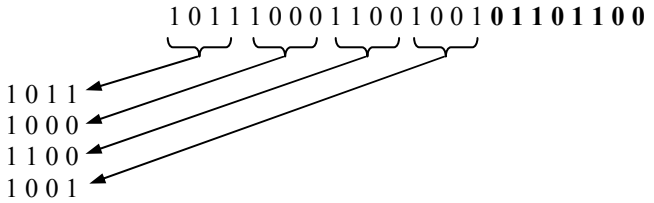


Рис. **1.14.** Информационные коды в квадратной таблице

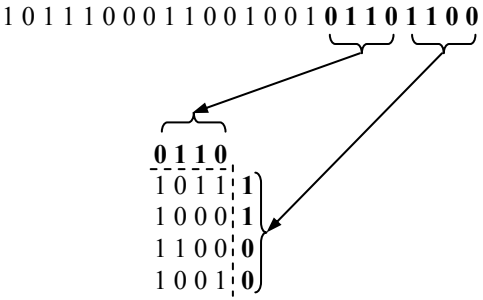


Рис. **1.15.** Проверочные коды в квадратной таблице

Получатель (в блоке приемника) выполняет подсчет суммы цифр для каждой строки и столбца, включая и цифры проверочного кода (рис. 1.15).

Для выяснения наличия ошибки применяется следующее достаточно простое правило:

- если окажется, что каждая из 8-ми сумм будет четная, то это означает, что все цифры последовательности из 24 двоичных цифр переданы без ошибок (это и изображено на рис. 1.15);
- если окажется, что для одного из 4-х столбцов и для одной из 4-х строк сумма получилась нечетной, то это означает, что передана неправильно та информационная цифра, которая стоит на пересечении данного столбца и данной строки;
- если окажется, что только для одного столбца сумма получилась нечетной, то это означает, что передана неправильно та информационная цифра, которая стоит в данном столбце;
- если окажется, что только для одной строки сумма получилась нечетной, то это означает, что передана неправильно та информационная цифра, которая стоит в данной строке.

Важно заметить, что в данном примере предполагается, что в каждом блоке только одна из 24 цифр может оказаться неправильной ■

Квантовая информация

> «…интересным может быть следующий вопрос: сколько информации представляет кубит, *если мы не измеряем его*? Ответить на него не так просто, поскольку нельзя определить количество информации, не выполняя соответствующего измерения…. Природа прячет массу скрытой информации…. Понимание этой скрытой *квантовой информации* является той задачей, которую мы пытаемся решать…»
>
> *М. Нильсен, И. Чанг* [**17**, с.36-37]

> «…разрыв между ненаблюдаемым состоянием кубита и доступными нам наблюдениями лежит в основе квантовых вычислений и квантовой информации.»
>
> *М. Нильсен, И. Чанг* [**17**, с.34]

На практике специалисты активно используют достаточно новые термины, такие как *квантовая информатика* [**25**] и *квантовая информация* [**17**, **18**, **26**].

Существуют следующие определения термина *квантовая информация.*

Определение 1.26

Квантовая информация [**17**, с.78-80] — общее название для всех видов деятельности, связанных с обработкой информации на основе *квантовой механики*.

Определение 1.27

Квантовая информация [**17**, с.78-80] обозначает изучение элементарных задач по обработке *квантовой информации* (т.е. сюда не входит построение квантовых алгоритмов, поскольку детали этих алгоритмов выходят за рамки «элементарных»).

Определение 1.28

Квантовая информация [**26**, с.507] — новое направление физики, возникло на стыке квантовой механики, оптики, теории информации и программирования, дискретной математики, лазерной физики и спектроскопии и включает в себя вопросы квантовых вычислений, квантовых компьютеров, квантовой телепортации и кванто-

вой криптографии, проблемы декогеренции и спектроскопии одиночных молекул и примесных центров.

Специалисты полагают [**19**], что целью *квантовой теории информации* является определение общих **принципов**, лежащих в основе управления поведением квантовых систем, например квантовых вычислителей — компьютеров (законы квантовой механики — это правила игры, а искомые принципы — эвристика опытного игрока).

Теория *квантовой информации* и *квантовых вычислений* пока еще находится в стадии своего развития и далека от своего завершения. Далее будем использовать пока более удобный термин *квантовая теория информации.*

Определение 1.29

Квантовая теория информации (см. и ср. [**18**, с.78-80]) обозначает раздел науки, определяющий специализированную область по аналогии с термином *классическая теория информации*, используемый для описания соответствующей классической области.

Определение 1.30

Теория информации (*классическая теория информации*) — это (см. [**20**, с.468]) наука, изучающая количественные закономерности, связанные с получением, передачей, обработкой и хранением информации.

ВАЖНО ПОМНИТЬ [**17**, с.659]. Специалисты полагают, что *квантовая теория информации* имеет принципиальную особенность, состоящую в том, что сами квантовые состояния рассматриваются именно как *информация* и при этом изучаются с теоретико-информационной точки зрения.

ОТМЕТИМ [**18**, с.79]. Специалисты полагают, что *квантовая теория информации* шире *классической теории информации*.

В развитии понятия энтропии выделяют три этапа [**1**, с.257-258], кратко представленные в табл. 1.11. К трем существующим этапам (в табл. 1.11) добавлен еще один — *текущий*, который непосредственно связан с развитием (см. [**17**, с.28, 640, 735; **24**]) нового направления квантовых вычислений.

Таблица 1.11. Этапы развития понятия энтропии

Этап	Название этапа	Дата (годы)	Примечание
Первый	*Термодинамический*	1865	*Р. Клаузис* ввел само понятие энтропии и ее обозначение как ***S***
Второй	*Статистический*	1877	*Л. Больцман* ввел вероятностную трактовку понятия энтропии и ее обозначение как ***H***
Третий	*Информационный*	40-е годы прошлого столетия	Работы *К. Шеннона* и *Н. Винера*. Энтропия становится мерой неопределенности, можно измерить количество информации
Текущий	*Квантовый*	1932, 1983, 1995	Работы *Дж. фон Неймана*, *Д. Дойча*, *Б. Шумахера* и др. Получен квантовый аналог классической формулы для энтропии. Сделано обобщение энтропии на квантовые состояния и доказан аналог теоремы о кодирование для канала без шума

Энтропию квантового состояния *Дж. фон Нейман* определил следующим образом.

Определение 1.31

Энтропией квантового состояния [**17**, с.621, 639, 694] называется $S(\boldsymbol{\rho})$, определяемое следующим образом[1]:

$$S(\rho) \equiv -tr\left(\rho \cdot \log_a(\rho)\right),$$

где **ρ** — матрица плотности (оператор плотности); $0 \cdot \log_a 0 \equiv 0$; a=2.

ОТМЕТИМ [**17**, с.83]. Энтропия *Дж. фон Неймана* совпадает с энтропией *К. Шеннона* тогда и только тогда, когда состояния $|\psi_j\rangle$ ортогональны. В противном случае энтропия *Дж. фон Неймана*

[1] Необходимые элементы квантовой механики приведены в книге 2.

для источника p_j, $|\psi_j\rangle$ в общем случае строго меньше, чем энтропия *К. Шеннона — **H***.

Определение 1.32

Относительной энтропией квантового состояния [**17**, с.622, 639] называется $S(\boldsymbol{\rho}\|\boldsymbol{\sigma})$, определяемое следующим образом:

$$S(\rho\|\sigma) \equiv tr\left(\rho \cdot \log_a(\rho)\right) - tr\left(\rho \cdot \log_a(\sigma)\right),$$

где **ρ** и **σ** — матрицы плотности (операторы плотности); a=2.

ОТМЕТИМ [**17**, с.622]. Относительная энтропия $S(\rho\|\sigma) \geq 0$, причем равенство достигается тогда и только тогда, когда **ρ=σ**.

Определение 1.33

Условной энтропией составной квантовой системы [**17**, с.625-626, 639] называется $S(\boldsymbol{A}|\boldsymbol{B})$, определяемое следующим образом:

$$S(A \mid B) \equiv S(A,B) - S(B),$$

где $S(A,B)$ — совместная энтропия для составной системы из двух компонент (систем) ***A*** и ***B***; $S(A,B) = -tr\left(\rho^{AB} \cdot \log_a\left(\rho^{AB}\right)\right)$, a=2.

Определение 1.34

Взаимной информацией [**17**, с.625-626, 639] называется $S(\boldsymbol{A}:\boldsymbol{B})$, определяемое следующим образом:

$$S(A:B) \equiv S(A) + S(B) - S(A,B),$$

где ***A*** и ***B*** — компоненты (или системы).

ОТМЕТИМ [**17**, с.681]. Такая важная проблема, как определение пропускной способности квантового канала для квантовой информации, исследователями пока еще изучена хуже, чем другая тоже важная проблема — определение пропускной способности того же квантового канала с **шумом** для классической информации.

Дополнительные и важные сведения, связанные с квантовой механикой, более подробно представлены в книге 2.

Выводы (резюме) по разделу 1.1

1. Определение термина *информация* много, они сложны и противоречивы.

   Информация — это

   - сведения, воспринимаемые человеком и(или) специальными устройствами как отражение **фактов** материального или духовного мира в процессе коммуникации;
   - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

2. Определений термина *данные* также много и они различны. Понятие *информация* близко к понятию *данные*. Однако между ними есть различие. Не всегда эти термины используются как синонимы.

   Данные — это

   - *информация*, обработанная и представленная в *формализованном* виде для дальнейшей обработки;
   - *сигналы,* из которых еще надо извлечь информацию.

   Передача информации происходит посредством *сигналов*. Информация может передаваться в форме *сообщений* от источника к приемнику с помощью некоторого *канала связи* между ними.

3. Чтобы стать *информацией*, данные должны быть *интересны* субъекту информирования и должны обладать *новизной*. Такие данные должны быть связаны с необходимостью решения некоторых *задач* и сокращать степень *неопределенности* о самом объекте интереса.

4. Сам процесс передачи **данных** от *источника* к *потребителю* и восприятия в качестве **информации** может быть представлен как прохождение трех фильтров: *физического, семантического, прагматического.*

5. Физическая система может **случайно** оказаться в некотором состоянии — такой системе присуща *степень неопределенности*. Наличие некоторой неопределенности связано с наличием некоторого беспорядка (или разупорядоченности).

Устранение неопределенности связано с упорядочиванием. Энтропию можно рассматривать как меру беспорядка.

6. Информационный объем сообщения на практике может быть измерен в ***битах***, что соответствует числу двоичных цифр (нуля и единицы), которыми может быть закодировано это сообщение. **Бит** — количество информации, которое содержится в ответе на вопрос, допускающий два равновероятных ответа. **Количество информации** измеряется энтропией (например, в битах).
7. Специалистами разработаны различные методы, позволяющие бороться с возникающими искажениями в сигналах. Существуют помехоустойчивые коды, позволяющие исправлять ошибки.
8. **Квантовая информация** — общее название для вех видов деятельности, связанных с обработкой информации на основе *квантовой механики*, и обозначает изучение элементарных задач по обработке *квантовой информации*.
9. **Квантовая теория информации** обозначает раздел науки, определяющий специализированную область по аналогии с термином *классическая теория информации*, используемый для описания соответствующей классической области.
10. **Квантовая теория информации** имеет принципиальную особенность, состоящую в том, что сами квантовые состояния рассматриваются именно как *информация* и при этом изучаются с теоретико-информационной точки зрения.
11. Далее для рассматриваемых квантовых вычислений важным является то, что информация — это не просто математическое понятие. На практике информация всегда имеет физическое воплощение, которое для *классической информации* подчиняется законам классической физики, а для *квантовой информации* — законам *квантовой механики.*
12. Информация определяет многие процессы, происходящие в вычислительном устройстве. Различают информацию *непрерывную* и *дискретную*.

1.2. Алгебра Буля и цифровые элементы

«Мало знать, надо и применять, мало хотеть, надо и делать.»
И. Гете [**29**, с.46]

«К сожалению или нет, но логику можно проверять экспериментально.»
Р. Фейнман [**21**, с.128]

Содержание

Высказывание. Логическая (булева) переменная. Логическая функция. Логическая операция. Таблица истинности. Законы алгебры высказываний. Совершенная дизъюнктивная нормальная форма (СДНФ). Совершенная конъюнктивная нормальная форма (СКНФ). Алгоритм получения СКНФ. Базис. Вычислительный базис. Смена вычислительного базиса. Логический элемент. Цифровой сигнал. Логическая схема. Комбинационная схема. Анализ и синтез комбинационной схемы. Цифровая вычислительная машина (ЦВМ). Сумматоры. Триггеры и регистры. RS триггер. Некоторые черты квантового вычислителя. Операция "контролируемое НЕ" (CNOT — controlled not). Вентиль Тоффоли.

В кибернетике при разработке вычислительных устройств рассматриваются вопросы *анализа* и *синтеза* цифровых схем, в основе которых лежат логические элементы. Подходящим математическим аппаратом для анализа и синтеза цифровых схем является *алгебра Буля*, названная в честь [**31**, с.164] английского математика *Дж. Буля* (1815-1864). Важными понятиями этой алгебры являются *высказывание* и *логическая* переменная.

Определение 1.35
Высказывание [**31**, с.164] — некоторое предложение, о котором можно утверждать, что оно *истинно* или *ложно*.

Определение 1.36
Логическая (булева) переменная [**31**, с.164] — такая величина $\boldsymbol{x}$, которая может принимать только два значения: **0** или **1**; $\boldsymbol{x}=\{0,1\}$.

На практике любое высказывание можно обозначить, например, символом $\boldsymbol{x}$ или $\boldsymbol{y}$ или каким-то еще другим символом. При этом можно полагать, что если это высказывание *ложно*, то $\boldsymbol{x}=\mathbf{0}$, а если высказывание *истинно*, то $\boldsymbol{x}=\mathbf{1}$ (где 1 — *логическая единица*,

0 — *логический нуль*). Для удобства оперирования такими высказываниями используют логические (или булевы) переменные.

Значения 0 или 1 связаны с тем, *истинно* или *ложно* высказывание, следующим образом.

Определение 1.37

Высказывание абсолютно истинно [**31**, с.164], если соответствующая ему логическая величина принимает значение x=**1** при любых условиях.

Определение 1.38

Высказывание абсолютно ложно [**31**, с.164], если соответствующая ему логическая величина принимает значение x=**0** при любых условиях.

На базе логических переменных вводят *логические функции* (или функции алгебры логики).

Определение 1.39

Логическая функция (ЛФ) [**31**, с.164] — функция $f(x_1, x_2,\ldots, x_n)$, принимающая значение, равное **0** или **1**, на наборе логических переменных $x_1, x_2,\ldots, x_n$.

Известно [**30**, с.42-43], что общее число различных логических функций от n переменных есть $M=2^{2^n}$. ЛФ удобно представлять в табличной форме в виде **таблицы истинности** (например, как в табл. 1.12), где возможным наборам аргументов ставятся в соответствие значения функции. В табл. 1.12 приведены логические функции от 1-й переменной (при n=1, M=4). Так функция $f_3(x)$ повторяет значение своего аргумента, а $f_4(x)$ является логическим отрицанием логической переменной x. Пример функции, которая абсолютно истинная, есть $f_1(x)$, а абсолютно ложная — $f_4(x)$.

Таблица 1.12. Логические функции от 1-й переменной [**31**, с.166]

Функция f_i	x		Примечание
	0	**1**	
f_1	1	1	$f_1(x)$ =**1** (константа единицы)
f_2	0	0	$f_2(x)$ =**0** (константа нуля)
f_3	0	1	$f_3(x) \equiv x$ (тождественная функция)
f_4	1	0	$f_4(x) = \overline{x}$ (логическое отрицание)

В табл. 1.13 приведены ЛФ от двух переменных, определяющих различные операции над булевыми переменными (при n=2 число ЛФ есть M=16). Так функция $f_7(x_1,x_2)$ определяет операцию сложения по модулю 2, $f_2(x_1,x_2)$ — операцию конъюнкции (логическое умножение), $f_8(x_1,x_2)$ — операцию дизъюнкции (логическое сложение), $f_9(x_1,x_2)$ — операцию ИЛИ-НЕ (стрелка Пирса), $f_{15}(x_1,x_2)$ — операцию И-НЕ (штрих Шеффера), повторяет значение своего аргумента, а $f_4(x)$ является логическим отрицанием логической переменной x. Примером ЛФ, которая абсолютно истинная, является $f_1(x)$, а абсолютно ложная — $f_4(x)$.

Таблица 1.13. Логические функции от 2-х переменных [**31**, с.166]

Функция f_i	x_1 x_2				Примечание
	00	**01**	**10**	**11**	
f_1	0	0	0	0	$f_1(x_1,x_2)$=**0** (константа нуля)
f_2	0	0	0	1	$x_1 \& x_2$ (конъюнкция, И)
f_3	0	0	1	0	$x_1 \& \overline{x}_2$ (запрет x_2)
f_4	0	0	1	1	$x_1\overline{x}_2 \vee x_1x_2 = x_1$
f_5	0	1	0	0	$\overline{x}_1 \& x_2$ (запрет x_1)
f_6	0	1	0	1	$\overline{x}_1x_2 \vee x_1x_2 = x_2$
f_7	0	1	1	0	$x_1 \oplus x_2$ (сложение по модулю 2)
f_8	0	1	1	1	$x_1 \vee x_2$ (дизъюнкция, ИЛИ)
f_9	1	0	0	0	$\overline{x_1 \vee x_2} = x_1 \downarrow x_2$ (функция Пирса)
f_{10}	1	0	0	1	$x_1 \leftrightarrow x_2$ (равнозначность)
f_{11}	1	0	1	0	$\overline{x}_1\overline{x}_2 \vee x_1\overline{x}_2 = \overline{x}_2$
f_{12}	1	0	1	1	$x_2 \rightarrow x_1$ (импликация)
f_{13}	1	1	0	0	$\overline{x}_1\overline{x}_2 \vee \overline{x}_1x_2 = \overline{x}_1$
f_{14}	1	1	0	1	$x_1 \rightarrow x_2$ (импликация)
f_{15}	1	1	1	0	$\overline{x_1 \& x_2} = x_1 \mid x_2$ (функция Шеффера)
f_{16}	1	1	1	1	$f_{16}(x_1,x_2)$=**1** (константа единицы)

ОТМЕТИМ. В алгебре высказываний существуют 3 основные логические операции: *конъюнкция*, *дизъюнкция* и *отрицание*.

Определение 1.40

Логическая операция [**39**, с.35] — способ построения сложного высказывания из данных высказываний, при котором значение истинности сложного высказывания полностью определяется значениями истинности исходных высказываний.

При вычислении значений логических выражений (формул) логические операции (используемые для записи формулы (выражения)) вычисляются (в соответствии с их приоритетом) в следующем порядке [**39**, с.43]:

1) инверсия (логическое отрицание);
2) конъюнкция;
3) дизъюнкция;
4) импликация и эквивалентность (равнозначность).

При наличии операций одного приоритета они выполняются слева направо. На практике, чтобы изменить порядок выполнения операции, используют (как это обычно принято) скобки. В табл. 1.14 приведены условные обозначения типовых логических операций.

Таблица 1.14. Принятые обозначения для некоторых операций

Операция	Возможные обозначения
Инверсия	НЕ x; NOT x; $\overline{x}$; $\neg x$;
Конъюнкция (логическое умножение)	y И x; y AND x; $y \wedge x$; $y \cdot x$; yx; y & x;
Дизъюнкция (логическое сложение)	y ИЛИ x; y OR x; $y \vee x$; $y + x$;
Импликация	$y \to x$; $y \Rightarrow x$;
Эквивалентность	$y \leftrightarrow x$; $y \Leftrightarrow x$; $y \sim x$; $y \equiv x$
Стрелка Пирса	$y \downarrow x$
Штрих Шеффера	$y \mid x$
Исключающее ИЛИ (сложение по модулю 2)	y XOR x; $y \oplus x$;

Определение 1.41

Простое высказывание [**39**, с.40] — высказывание, которое не содержит в себе других высказываний.

***Пример* 1.11** простых высказываний [**39**, с.40]:

Идет дождь.

Нам живется весело■

Определение 1.42

Сложное высказывание [**39**, с.40] — высказывание, которое получено путем объединения нескольких простых высказываний в одно с помощью логических операций и скобок.

***Пример* 1.12** сложных высказываний [**39**, с.40]:

Идет дождь, а у меня нет зонта.

Когда живется весело, то и работа спорится.

Идет налево — песнь заводит, направо — сказку говорит■

В рамках формальной логики выделяют следующие 4 закона [**39**, с.52]:

I. Закон тождества: в процессе определенного рассуждения всякое понятие и суждение должны быть тождественны сами себе.

II. Закон непротиворечия: невозможно, чтобы одно и то же в одно и то же время было и не было присуще одному и тому же в одном и том же отношении. То есть невозможно что-либо одновременно утверждать и отрицать.

III. Закон исключения третьего: из двух противоречащих суждений одно истинно, другое ложно, а третьего не дано.

IV. Закон достаточного основания: всякая истинная мысль должна быть достаточно обоснована.

Отметим, что появление трех первых законов связывают с *Аристотелем*, а последний закон — с *Г. Лейбницем*.

В алгебре логики (алгебре высказываний) выделяют особо законы, которые содержат одну переменную [**39**, с.53]:

I. Закон тождества: $x = x$.

II. Закон непротиворечия: $\overline{x \& \overline{x}} = 1$ или $x \,\&\, \overline{x} = 0$.

III. Закон исключения третьего: $x \vee \overline{x} = 1$.

IV. Закон достаточного основания: $\overline{\overline{x}} = x$.

Выделяют также следующие законы и свойства [**39**, с.60]:

V. Закон идемпотентности: $x \vee x = x$ и $x \,\&\, x = x$.

VI. Закон поглощения: $x \vee (x \,\&\, y) = x$ и $x \,\&\, (x \vee y) = x$.

VII. Закон для импликации (правило замены операции импликации):

$$(x \to y) = (\overline{x} \vee y) \text{ и } (x \to y) = (\overline{x} \to \overline{y}).$$

VIII. Закон для эквивалентности (правило замены операции эквивалентности):

$$(x \leftrightarrow y) = (x \,\&\, y) \vee (\overline{x} \,\&\, \overline{y});$$

$$(x \leftrightarrow y) = (x \vee \overline{y}) \,\&\, (\overline{x} \vee y);$$

$$(x \leftrightarrow y) = (x \to y) \,\&\, (y \to x).$$

IX. Свойства констант:

$\overline{0} = 1$ и $\overline{1} = 0$; $x \vee 0 = x$ и $x \,\&\, 0 = 0$; $x \vee 1 = 1$ и $x \,\&\, 1 = x$.

В алгебре логики имеются 4 основных закона [**30**, с.44]:

I. Переместительный закон

$x_1 \vee x_2 = x_2 \vee x_1$ (для дизъюнкции);

$x_1 \,\&\, x_2 = x_2 \,\&\, x_1$ (для конъюнкции);

II. Сочетательный закон

$(x_1 \vee x_2) \vee x_3 = x_1 \vee (x_2 \vee x_3)$ (для дизъюнкции);

$(x_1 \,\&\, x_2) \,\&\, x_3 = x_1 \,\&\, (x_2 \,\&\, x_3)$ (для конъюнкции);

III. Распределительный закон

$(x_1 \vee x_2) \,\&\, x_3 = x_1 \,\&\, x_3 \vee x_2 \,\&\, x_3$ (для дизъюнкции);

$(x_1 \,\&\, x_2) \vee x_3 = (x_1 \vee x_3) \,\&\, (x_2 \vee x_3)$ (для конъюнкции);

IV. Закон общей инверсии (формула *де Моргана*)

$\overline{x_1 \vee x_2} = \overline{x}_1 \,\&\, \overline{x}_2$ или $x_1 \vee x_2 = \overline{\overline{x}_1 \,\&\, \overline{x}_2}$ (для дизъюнкции);

$\overline{x_1 \,\&\, x_2} = \overline{x}_1 \vee \overline{x}_2$ или $x_1 \,\&\, x_2 = \overline{\overline{x}_1 \vee \overline{x}_2}$ (для конъюнкции).

Важно отметить, что указанные выше законы справедливы для любого конечного числа переменных.

На практике требуется выполнить упрощение сложных высказываний путем замены их на равносильные на основе законов алгебры логики с целью получения высказываний более простой формы.

***Пример* 1.13** упрощения сложного высказывания [**39**, с.64].

Пусть требуется упростить $F(x,y) = x \vee \overline{x}\ \&\ y$.

Решение

1). Найдем то, что можно вынести за скобки, которых пока нет. Для этого представим x как следующее выражение:

$$x = x\ \&\ 1,$$

а **1** представим в соответствии с Законом исключения третьего следующим образом:

$$1 = y \vee \overline{y}.$$

В итоге получим следующее выражение:

$$F(x,y) = x \vee \overline{x}\ \&\ y = (x\ \&\ 1) \vee \overline{x}\ \&\ y = \left(x\ \&\ (y \vee \overline{y})\right) \vee \overline{x}\ \&\ y =$$

$$= (x\ \&\ y \vee x\ \&\ \overline{y}) \vee \overline{x}\ \&\ y = x\ \&\ y \vee x\ \&\ \overline{y} \vee \overline{x}\ \&\ y,$$

т.е. можно полагать, что $F(x,y) = x\ \&\ y + x\ \&\ \overline{y} + \overline{x}\ \&\ y$.

2). Далее будем группировать элементы получившегося выше выражения. Однако не хватает одного элемента выражения (слагаемого). Для этого в соответствии с Законом идемпотентности добавим в получившееся выражение одно из его слагаемых $(x\ \&\ y)$ следующим образом:

$$F(x,y) = x\ \&\ y + x\ \&\ \overline{y} + \overline{x}\ \&\ y + (x\ \&\ y)$$

или

$$F(x,y) = (x\ \&\ y + x\ \&\ \overline{y}) + (\overline{x}\ \&\ y + (x\ \&\ y)) =$$

$$= x\ \&\ (y + \overline{y}) + y\ \&\ (\overline{x} + x) = x\ \&\ 1 + y\ \&\ 1 = x + y.$$

3). Таким образом, окончательно получаем следующее более простое выражение:

$$F(x,y) = x \vee y.$$

4). И тем самым задача решена■

Определение 1.43

Элементарная конъюнкция (ЭК) [**39**, с.107] — конъюнкция нескольких переменных, взятых с отрицанием или без отрицания, причем среди переменных могут быть одинаковые.

Определение 1.44

Элементарная дизъюнкция (ЭД) [**39**, с.107] — дизъюнкция нескольких переменных, взятых с отрицанием или без отрицания, причем среди переменных могут быть одинаковые.

Определение 1.45

Дизъюнктивная нормальная форма (ДНФ) [**39**, с.107] — всякая дизъюнкция *элементарных конъюнкций*.

Определение 1.46

Конъюнктивная нормальная форма (КНФ) [**39**, с.107] — всякая конъюнкция *элементарных дизъюнкций*.

Логические функции на практике можно представить в следующих двух различных формах [**39**, с.107]:

1) *дизъюнктивная нормальная форма* (ДНФ);
2) *конъюнктивная нормальная форма* (КНФ).

В случае ДНФ логическая функция записывается в виде дизъюнкции элементарных конъюнкций, образованных из переменных и их отрицаний.

В случае КНФ наоборот, т.е. конъюнкции элементарных дизъюнкций, образованных из переменных и (или) их отрицаний.

Кроме ДНФ и КНФ рассматривают еще и совершенную ДНФ и совершенную КНФ.

Определение 1.47

Совершенная дизъюнктивная нормальная форма (СДНФ) [**39**, с.107] — всякая ДНФ, в которой нет одинаковых *элементарных конъюнкций* и все конъюнкции состоят из одного и того же набора переменных, в который каждая переменная входит только один раз (возможно, с отрицанием).

Определение 1.48

Совершенная конъюнктивная нормальная форма (СКНФ) [**39**, с.107] — всякая КНФ, в которой нет одинаковых *элементарных дизъюнкций* и все дизъюнкции состоят из одного и того же набора переменных, в который каждая переменная входит только один раз (возможно, с отрицанием).

В табл. 1.15 приведены формулы, которые соответствуют или не соответствуют приведенным выше определениям ЭК, ЭД, ДНФ, КНФ, СДНФ, СКНФ.

Таблица 1.15. Примеры формул [**39**, с.108-109]

Название формулы в определении	Формула, соответствующая определению	Формула, не соответствующая определению
ЭД	$x \vee \overline{x}$, $x \vee \overline{z}$, $\overline{x} \vee y \vee \overline{z}$	$x \vee y \,\&\, x$
ЭК	$\overline{x} \,\&\, x$, $x \,\&\, z$, $x \,\&\, \overline{y} \,\&\, \overline{x}$, $\overline{x} \,\&\, y \,\&\, \overline{z}$	$x \vee y \,\&\, x$
ДНФ	$x \,\&\, \overline{x} \vee x \,\&\, y \,\&\, \overline{z}$, $x \,\&\, y \vee \overline{y} \vee x \,\&\, z$	—
КНФ	$(x \vee y \vee \overline{x}) \,\&\, (\overline{x} \vee z)$, $x \,\&\, (\overline{x} \vee y) \,\&\, (x \vee \overline{z})$	—
СДНФ	$x \,\&\, y \,\&\, \overline{z} \vee x \,\&\, y \,\&\, z$, $x \vee \overline{x}$	$x \,\&\, y \vee \overline{y} \vee x \,\&\, \overline{z}$
СКНФ	$(\overline{x} \vee y \vee z) \,\&\, (x \vee \overline{y} \vee z)$, $\overline{x} \,\&\, x$	$(x \vee y \vee \overline{x}) \,\&\, (\overline{x} \vee z)$

Логические константы 0 и 1 могут быть представлены в виде СКНФ (для 0) и СДНФ (для 1) следующим образом:

$$0 = \overline{x} \,\&\, x,$$

$$1 = x \vee \overline{x}.$$

Найдены достаточно не сложные алгоритмы получения СДНФ и СКНФ по таблице истинности.

Рассмотрим алгоритм получения СДНФ по таблице истинности на следующем примере (табл. 1.16) [**39**, с.109]:

Таблица 1.16

x	y	$f(x, y)$
0	0	0
0	1	1
1	0	1
1	1	0

Шаг 1. В таблице истинности (табл. 1.16) отметить символом звездочка ***** те строки, где стоят логические единицы **1** в последнем столбце следующим образом (табл. 1.17):

Таблица 1.17

x	y	$f(x, y)$	
0	0	0	
0	1	1*	⇐
1	0	1*	⇐
1	1	0	

Шаг 2. Для каждой отмеченной строки в табл. 1.17 надо выписать *конъюнкцию* всех логических переменных, учитывая следующее правило:

если значение переменной в данной строке есть **1**, то в *конъюнкцию* следует включить саму эту переменную;

если значение переменной в данной строке есть **0**, то в *конъюнкцию* следует включить отрицание этой переменной.

Тогда для 2-х отмеченных строк табл. 1.17 (строки отмечены стрелками) будет получено следующее:

для 2-й строки — $\overline{x} \,\&\, y$;

для 3-й строки — $x \,\&\, \overline{y}$.

Шаг 3. Получившиеся все на предыдущем шаге *конъюнкции* следует связать в *дизъюнкцию* следующим образом:

$$(\overline{x}\ \&\ y) \vee (x\ \&\ \overline{y}),$$

что и будет искомой СДНФ для $f(x, y)$

$$f(x, y) = (\overline{x}\ \&\ y) \vee (x\ \&\ \overline{y}).$$

Рассмотрим алгоритм получения СКНФ по таблице истинности на примере той же самой таблицы (табл. 1.16) [**39**, с.109-110].

Шаг 1. В таблице истинности (табл. 1.16) отметить символом звездочка ***** те строки, где стоят логические нули **0** в последнем столбце следующим образом (табл. 1.18):

Таблица 1.18

x	y	$f(x, y)$	
0	0	0*	⇐
0	1	1	
1	0	1	
1	1	0*	⇐

Шаг 2. Для каждой отмеченной строки в табл. 1.18 надо выписать *дизъюнкцию* всех логических переменных, учитывая следующее правило:

если значение переменной в данной строке есть **0**, то в *дизъюнкцию* следует включить саму эту переменную;

если значение переменной в данной строке есть **1**, то в *дизъюнкцию* следует включить отрицание этой переменной.

Тогда для 2-х отмеченных строк табл. 1.18 (строки отмечены стрелками) будет получено следующее:

для 1-й строки — $x \vee y$;

для 4-й строки — $\overline{x} \vee \overline{y}$.

Шаг 3. Получившиеся все на предыдущем шаге *дизъюнкции* следует связать в *конъюнкцию* следующим образом:

$$(x \vee y)\ \&\ (\overline{x} \vee \overline{y}),$$

что и будет следующей искомой СДНФ для $f(x, y)$:

$$f(x, y) = (x \vee y) \,\&\, (\overline{x} \vee \overline{y}).$$

Таким образом, для одной и той же таблицы истинности получены следующее две разные формулы для логической функции:

$$f(x, y) = (\overline{x} \,\&\, y) \vee (x \,\&\, \overline{y}) \text{ — СДНФ,}$$
$$f(x, y) = (x \vee y) \,\&\, (\overline{x} \vee \overline{y}) \text{ — СКНФ.}$$

***Пример* 1.14** эквивалентности СДНФ и СКНФ [**39**, с.110].

Показать эквивалентность следующих выражений одной и той же логической функции, записанной в двух разных формах (СДНФ и СКНФ):

$$f(x, y)_{\text{СДНФ}} = (\overline{x} \,\&\, y) \vee (x \,\&\, \overline{y}),$$
$$f(x, y)_{\text{СКНФ}} = (x \vee y) \,\&\, (\overline{x} \vee \overline{y}).$$

Решение

Преобразуем СКНФ, используя правила алгебры логики, следующим образом:

$$f(x, y)_{\text{СКНФ}} = (x \vee y) \,\&\, (\overline{x} \vee \overline{y}) =$$
$$= x \,\&\, \overline{x} \vee x \,\&\, \overline{y} \vee \overline{x} \,\&\, y \vee y \,\&\, \overline{y} = (\overline{x} \,\&\, y) \vee (x \,\&\, \overline{y}) = f(x, y)_{\text{СДНФ}}$$

И тем самым задача решена■

Логическая функция в табличной форме является достаточно наглядным представлением при небольшом числе переменных.

В случае большого числа переменных такое представление уже перестает быть наглядным. Для этого случая используют иное представление — аналитическую запись ЛФ в виде формул.

Примеры аналитических записей ЛФ в виде формул приведены в табл. 1.12-1.13 (столбец *Примечание*). Из этих примеров видно, что аналитическая запись намного компактнее, чем табличное представление.

Построение таблицы истинности по аналитической записи ЛФ сводится к вычислению значений ЛФ при всех возможных значениях ее аргументов.

Определение 1.49

Базис [**30**, с.50] — система логических функций называется *функционально полной* или *базисом*, если любую логическую функцию можно представить в аналитической форме через эти функции, взятые в любом конечном числе экземпляров каждая.

На практике одну и ту же логическую функцию можно представить разным способом. Специалистами было доказано, что *конъюнкция*, *дизъюнкция* и *отрицание* образуют базис. Базис И, ИЛИ, НЕ — это избыточной базис, так как применяя формулу *де Моргана*, можно исключить, например И, заменяя И на ИЛИ и НЕ, так как $x_1 \& x_2 = \overline{\overline{x}_1 \vee \overline{x}_2}$ [**30**, с.50]. Другим базисом является функция Пирса (ИЛИ-НЕ). Применяя только функцию Пирса, можно представить любую логическую функцию на практике. Еще одним базисом является функция Шеффера (И-НЕ). Помимо базиса как *системы логических функций* очень большое значение играет не менее важный *вычислительный базис*.

Для выполнения логических вычислений над логическими переменными необходимо определиться, что считается *логическим нулем* и *логической единицей* в данной физической реализации логического элемента. Аналогично для выполнения арифметических вычислений (операций), например, в двоичной системе счисления, надо определить, что считать *двоичной единицей* и *двоичным нулем*. Таким образом, специалисты должны договориться о том, что на практике (при физической реализации) им считать 1 или 0. Для решения этой проблемы был введен *вычислительный базис*.

Определение 1.50

Вычислительный базис (ВБ) — это те (обычно два) устойчивых состояния некоторой физической системы, принятые для физической реализации на практике **0** или **1** (например, *логического нуля, логической единицы* или *двоичного нуля*, *двоичной единицы*).

Если за **1** принят высокий уровень сигнала, то говорят [**41**, с.53], что имеет место *положительная логика* работы логического элемента (устройства), а если за **1** принят низкий уровень сигнала, то — *отрицательная логика*. Обычно паспортные обозначения таких элементов приводятся для режима *положительной логики*.

ОТМЕТИМ [**41**, с.53]. Цифровые логические элементы потенциально могут работать в двух режимах как в режиме *положительной логики*, так и в режиме *отрицательной логики*.

Определение 1.51
Логический элемент (ЛЭ) — это устройство, реализующее логическую функцию.

Определение 1.52
Цифровой сигнал [**39**, с.105] — это сигнал, который может принимать только одно из двух установленных значений.

Работа логического элемента (устройства) может быть описана состоянием его выходов соответствующих состояниям его входов. Для ЛЭ существенно то, что они должны иметь два устойчивых физических состояния. В качестве примера таких состояний можно привести следующие:

- напряжение +5 В и +0.4 В;
- лампа (светодиод) горит или не горит;
- кнопка нажата или нет;
- переключатель включен или выключен.

На практике иногда в электрических схемах принято, что напряжение (см. [**39**, с.98]) от +2.4 В до +5 В соответствует сигналу *логической единицы* (высокий уровень цифрового сигнала), а напряжение, не превышающее +0.5 В — *логическому нулю* (низкий уровень цифрового сигнала). Если напряжение между +0.5 В и +2.4 В, то цифровой сигнал не определен.

Разработчики вычислительных устройств ввели следующие важные определения для напряжений уровней цифровых сигналов.

Определение 1.53
Напряжение логической единицы [**38**, с.38] — значение высокого уровня напряжения для *положительной логики* и значение низкого уровня напряжения для *отрицательной логики*.

Определение 1.54
Напряжение логического нуля [**38**, с.38] — значение низкого уровня напряжения для *положительной логики* и значение высокого уровня напряжения для *отрицательной логики*.

Определение 1.55

Пороговое напряжение логической единицы [**38**, с.38] — наименьшее значение высокого уровня напряжения для *положительной логики* и наибольшее значение низкого уровня напряжения для *отрицательной логики* на выходе микросхемы, при котором она переходит из одного состояния в другое.

Определение 1.56

Пороговое напряжение логического нуля [**38**, с.38] — наибольшее значение низкого уровня напряжения для *положительной логики* и наименьшее значение высокого уровня напряжения для *отрицательной логики*, при котором она переходит из одного состояния в другое.

Из логических элементов строят различные логические схемы, реализующие достаточно сложные логические функции на практике.

Определение 1.57

Логическая схема [**37**] — это схема, построенная из логических элементов.

Определение 1.58

Логическое устройство [**39**, с.102] — это цепочка из логических элементов, в которой выходы одних элементов являются входами других элементов.

Различное преобразование данных вычислительными устройствами выполняется следующими двумя типами логических устройств [**30**, с.57; **31**, с.205]:

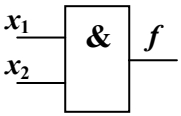
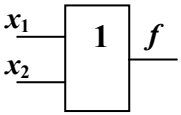
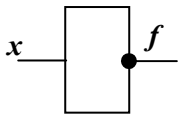
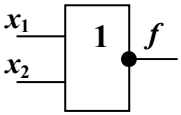
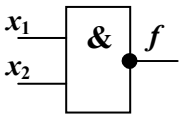
1) комбинационными схемами (схемы первого рода);
2) цифровыми автоматами с памятью (схемы второго рода).

Определение 1.59

Комбинационная схема [**31**, с.205] — это схема, выходной сигнал в которой завит только от состояния входов (наличия входных сигналов) в каждый момент времени.

В табл. 1.19 приведены условные обозначения типовых логических элементов с указанием их таблиц истинности.

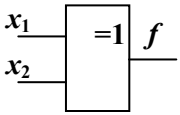
Таблица 1.19. Типовые логические элементы (ср. с [**30**, с.62])

Наименование элемента	Условное обозначение	Название и логическая функция	Таблица истинности
И		Конъюнкция $f(x_1,x_2)=x_1 \& x_2$	x_1 x_2 f 0 0 0 0 1 0 1 0 0 1 1 1
ИЛИ		Дизъюнкция $f(x_1,x_2)=x_1+x_2$	x_1 x_2 f 0 0 0 0 1 1 1 0 1 1 1 1
НЕ		Инверсия $f(x)=\overline{x}$	x f 0 1 1 0
ИЛИ-НЕ		Стрелка Пирса $f(x_1,x_2)=x_1 \downarrow x_2$	x_1 x_2 f 0 0 1 0 1 0 1 0 0 1 1 0
И-НЕ		Штрих Шеффера $f(x_1,x_2)=x_1 \mid x_2$	x_1 x_2 f 0 0 1 0 1 1 1 0 1 1 1 0

Рассмотрим еще некоторые важные, хотя и специфические логические элементы.

Логический элемент XOR — это хорошо известный элемент (рис. 1.16) для сложения по модулю 2, реализующий логическую функцию от двух переменных $f_7(x_1,x_2)=x_1\oplus x_2$ (см. табл. 1.13). На рис. 1.17**а** представлено новое обозначение для обобщенного элемента XOR, у которого в отличие от обычного элемента XOR (рис. 1.16**а**) появился еще один дополнительный выход $\boldsymbol{x'_1}$. Анализ таблицы истинности (рис. 1.17**б**) показывает, что этот дополнительный выход полностью дублирует вход $\boldsymbol{x_1}$, т.е. $\boldsymbol{x_1}=\boldsymbol{x'_1}$. Новое квантово-механическое обозначение (рис. 1.17**в**) такого обобщенного элемента XOR несколько необычно и отличается от способа обозначения традиционным способом в кибернетике (цифровой схемотехнике). Отметим, что пунктирная рамка (рис. 1.17**в**) — это дань цифровой схемотехнике (обычно ее не изображают).

а)

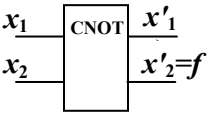


б)

x_1	x_2	f
0	0	0
0	1	1
1	0	1
1	1	0

Рис. **1.16.** Логический элемент XOR
а) принятое обозначение; б) таблица истинности

а)



б)

x_1	x_2	x'_1	$x'_2=f$
0	0	0	0
0	1	0	1
1	**0**	1	**1**
1	**1**	1	**0**

в)

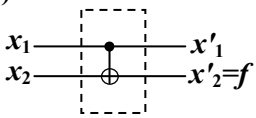


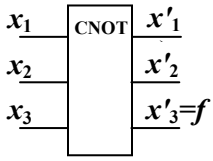
Рис. **1.17.** Логический обобщенный элемент XOR:
а) новое обозначение; б) таблица истинности;
в) квантово-механическое обозначение

При таком необычном обозначении (рис. 1.17**в**) принято следующее. Анализируя таблицу истинности (рис. 1.17**б**), можно заметить, что состояние входа x_1 как бы управляет состоянием входа x_2. Действительно, когда x_1=0, то состояние входа x_2 как бы не меняется (x'_2=x_2) и соответствует состоянию выхода элемента f, т.е. x'_2=f. В том случае, когда x_1=1, то состояние входа x_2 как бы меняется на противоположное (x'_2=$\overline{x}_2$) и также соответствует состоянию выхода элемента f, т.е. x'_2=f. Состояние входа x_1 не меняется.

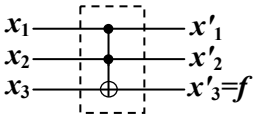
В квантово-механическом случае принято говорить [**26**, с.517], что такая операция есть **контролируемое НЕ** (CNOT — *controlled not*), а бит x_2 (т.е. бит цели) изменяет свое состояние тогда и только тогда, когда состояние бита источника x_1 есть 1, при этом состояние бита источника не меняется.

Аналогично можно ввести понятие и 3-входового элемента **контролируемое НЕ** (рис. 1.18**а,в**) и таблицу истинности для него (рис. 1.18**б**). Элемент на рис. 1.18**в** получил название [**26**, с.517] *универсальный трехбитовый вентиль Тоффоли*.

а)



в)



б)

Входы			**Выходы**		
x_1	x_2	x_3	x'_1	x'_2	x'_3=f
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	**0**	1	1	**1**
1	1	**1**	1	1	**0**

Рис. **1.18.** Логический элемент CNOT на три входа:
а) новое обозначение; б) таблица истинности;
в) квантово-механическое обозначение

Возможная схема реализации обратимого логического элемента CNOT на два входа с применением логического элемента XOR на два входа представлена на рис. 1.19.

Известная схема реализации (в базисе И-НЕ) логического элемента XOR на два входа с применением известных логических элементов И-НЕ на два входа представлена на рис. 1.20.

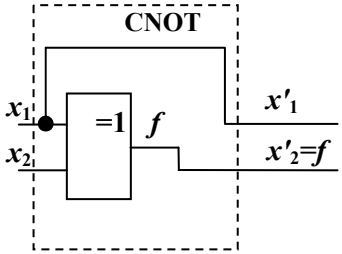


Рис. **1.19.** Реализация логического элемента **CNOT** на логическом элементе XOR

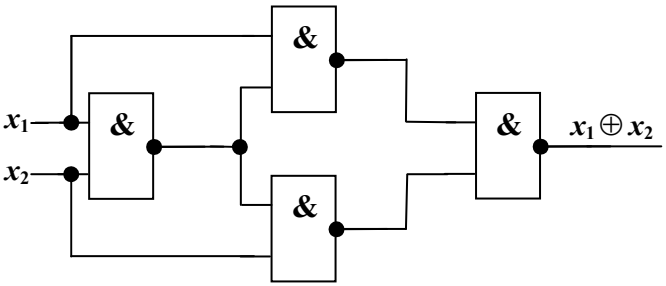


Рис. **1.20.** Реализация логического элемента XOR на логических элементах И-НЕ [**40**]

Известная схема реализации (в базисе ИЛИ, НЕ) логического элемента И на два входа с применением известных логических элементов ИЛИ, НЕ представлена на рис. 1.21.

Другая известная схема реализации (в базисе И, НЕ) логического элемента ИЛИ на два входа с применением известных логических элементов И, НЕ представлена на рис. 1.22.

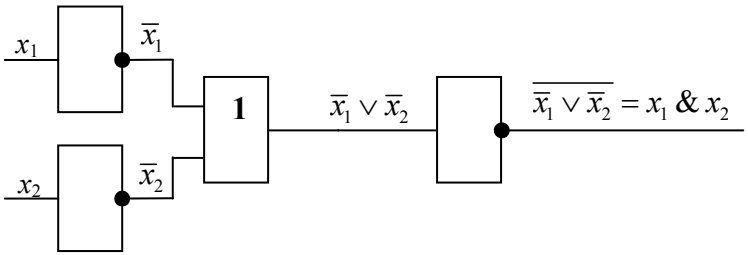


Рис. **1.21.** Реализация логического элемента И на логических элементах ИЛИ, НЕ [**30**, с.63]

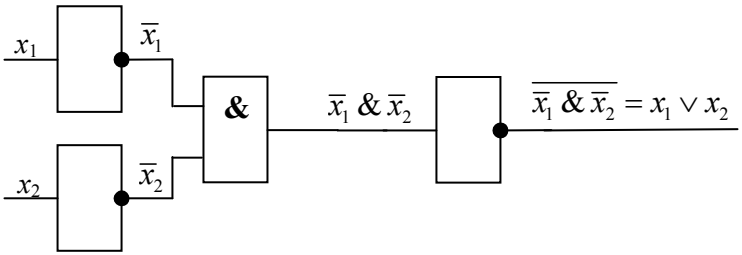


Рис. **1.22.** Реализация логического элемента ИЛИ на логических элементах И, НЕ [**30**, с.63]

Логические элементы на практике могут быть реализованы различным образом. Например, элемент ИЛИ (рис. 1.23), элемент И (рис. 1.24) могут быть реализованы по известной схеме с помощью переключателей. Пример реализации с помощью диодов приведен на рис. 1.25.

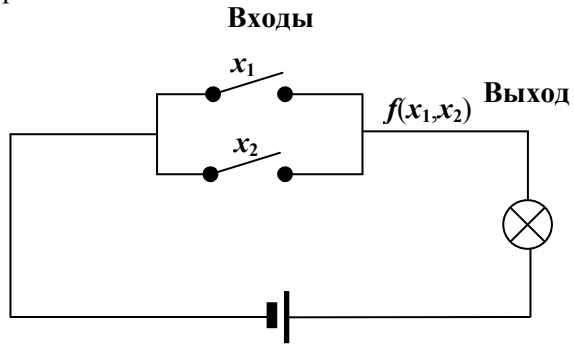


Рис. **1.23.** Схема элемента ИЛИ на переключателях

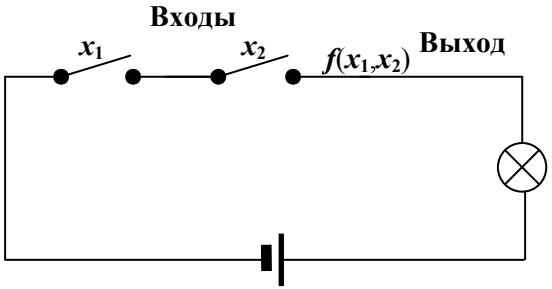


Рис. **1.24.** Схема элемента И на переключателях

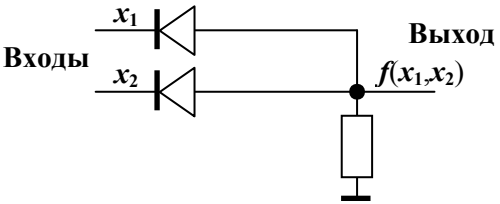


Рис. **1.25.** Известная схема элемента И на диодах [**31**, с.205]

Смена вычислительного базиса

На практике смена вычислительного базиса (смена режима работы ЛЭ) может в корне поменять логику работы этого ЛЭ. Действительно, пусть имеется ЛЭ ИЛИ и его таблица истинности (рис. 1.26**а**). Пусть для элемента ИЛИ принят следующий ВБ 1:

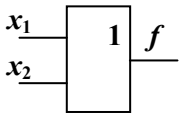
логическая единица – 5 В; *логический нуль* – 1 В.

В этом ВБ 1 этот ЛЭ реализует логику работы ЛЭ ИЛИ (рис. 1.26**а**). Если теперь сменить ВБ 1 на ВБ 2, т.е. теперь за *логическую единицу* и *логический нуль* принят другой уровень напряжения, например, следующий ВБ 2:

логическая единица – 1 В; *логический нуль* – 5 В;

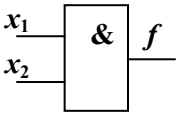
то это будет означать, что новый нуль 0’ — это есть старая единица 1, и новая 1’ есть старый 0 (рис. 1.26**б**).

а)



ИЛИ		
x_1	x_2	$f_{\text{ИЛИ}}$
0	0	0
0	1	1
1	0	1
1	1	1

б)



И		
x_1	x_2	$f_{\text{И}}$
1’	1’	1’
1’	0’	0’
0’	1’	0’
0’	0’	0’

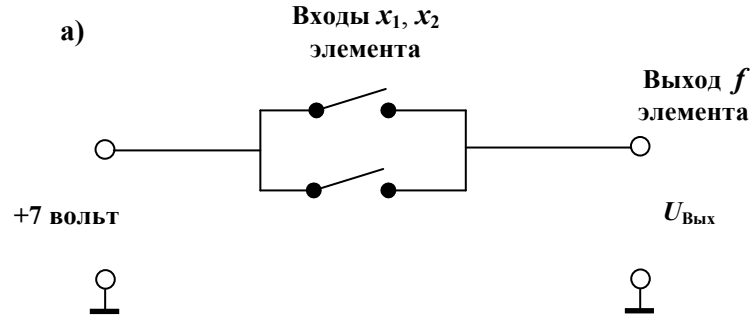
Рис. **1.26.** Смена ВБ для логического элемента ИЛИ

Перейдем к рассмотрению более конкретного примера, связанного с физической реализацией логического элемента и со сменой его вычислительного базиса.

***Пример* 1.15** смены вычислительного базиса для ЛЭ элемента ИЛИ, реализованного на переключателях.

Допустим, имеется логический элемент ИЛИ, реализованный на переключателях, как показано на рис. 1.27**а**. Для этого ЛЭ принят следующий ВБ 3:

логическая единица – (**+7**) В; *логический нуль* – **0** В.



б)

ИЛИ			
x_1	x_2	$U_{Вых}$	$f_{ИЛИ}$
0	0	**0**	0
0	1	**+7**	1
1	0	**+7**	1
1	1	**+7**	1

в)

И			
x_1	x_2	$U_{Вых}$	$f_{И}$
1’	1’	**0**	1’
1’	0’	**+7**	0’
0’	1’	**+7**	0’
0’	0’	**+7**	0’

Рис. **1.27.** Смена ВБ для ЛЭ ИЛИ на переключателях

В вычислительном базисе ВБ 3 данный ЛЭ реализует логику работы ЛЭ ИЛИ (рис. 1.27**а**) в соответствии с таблицей истинности, представленной на рис. 1.26**а**.

Если оба переключателя разомкнуты (рис. 1.27**а**, т.е. x_1=0, x_2=0), то напряжение $U_{Вых}$ на выходе ЛЭ будет отсутствовать ($U_{Вых}$=**0** В), что соответствует *логическому нулю*.

Если включены оба (т.е. x_1=1, x_2=1) или разомкнут только один переключатель (т.е. x_1=0, x_2=1 или x_1=1, x_2=0), то напряжение $U_{Вых}$ на выходе ЛЭ будет присутствовать ($U_{Вых}$=**+7** В), что соответствует *логической единице*. Этот факт отражен в таблице на рис. 1.27**б**. Отметим, что в этом случае включение переключателя означает, что установлена логическая единица, а отключение переключателя означает, что установлен логический нуль.

Если теперь сменить вычислительный базис ВБ 3 на ВБ 4, т.е. теперь за *логическую единицу* и *логический нуль* принят другой уровень напряжения, т.е. следующий ВБ 4:

логическая единица – **0** В; *логический нуль* – (+**7**) В;

то это будет означать, что новый нуль 0’ — это есть старая единица 1, и новая 1’ есть старый 0 (рис. 1.27**в**). Отметим, что в этом случае включение переключателя означает другое, а именно, что установлен логический нуль, а отключение переключателя означает, что установлена логическая единица.

Для данного логического элемента (независимо от того, какую он реализует логическую функцию для элемента (И, ИЛИ)) важно отметить следующее. Конечный результат работы ЛЭ (в более общем случае — комбинационной схемы) на практике получается путем **измерения** с помощью некоторого прибора (в данном случае, например, вольтметром). Измерив выходное напряжение $\boldsymbol{U_{\text{Вых}}}$ на выходе элемента и сопоставив его с принятым вычислительным базисом, можно определить, что имеется на выходе ЛЭ — логическая единица или логический нуль. В случае вычислительного базиса ВБ 4, если $\boldsymbol{U_{\text{Вых}}}$=**+7** В, то это означает, что на выходе ЛЭ наблюдается логический нуль. При этом, если аппаратура работает исправно, то всякий раз будет получено $\boldsymbol{U_{\text{Вых}}}$=**+7** В . Повторные измерения не изменяют состояние ЛЭ и не разрушают физические процессы, протекающие в физической реализации ЛЭ■

ВАЖНО. В случае *квантового вычислителя* процесс **измерения** разрушает текущее состояние квантового объекта (системы), используемого для физической реализации ЛЭ (гейта).

На практике реализация логических элементов не ограничивается рассмотренными примерами. Логические элементы могут быть реализованы с помощью транзисторов. В некоторых случаях эти элементы могут быть реализованы с помощью специальных механических клапанов, причем вместо электрического тока может использоваться сжатый воздух или жидкость, а вместо электрических проводов — трубопровод. Далее будет показано, что логические элементы могут быть реализованы с помощью квантовых объектов (так называемых квантовых гейтов).

ВАЖНО. В случае *квантового вычислителя* некоторым аналогом таблицы истинности для гейта является *унитарная матрица*.

Определение 1.60

Цифровая вычислительная машина (ЦВМ) [**31**, с.15] — машина, оперирующая информацией, представленной в дискретном виде.

Некоторые ошибки, возникающие в ЦВМ, можно выявить, а иногда и исправить с помощью специальных помехоустойчивых кодов. Далее кратко рассмотрим сумматоры и триггеры как составные части вычислительных устройств (ЦВМ).

Сумматоры

Таблица истинности полусумматора ***HS*** (half-sum) на 1 разряд представлена в табл. 1.20, а условное обозначение этого сумматора показано на рис. 1.28. Возможная схема комбинационного полусумматора ***HS*** представлена на рис. 1.29.

Таблица 1.20. Таблица истинности полусумматора ***HS*** [**30**, с.79]

Входы (слагаемые)		Выходы	
x_i	y_i	S_i (сумма)	P_{i+1} (бит переноса)
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

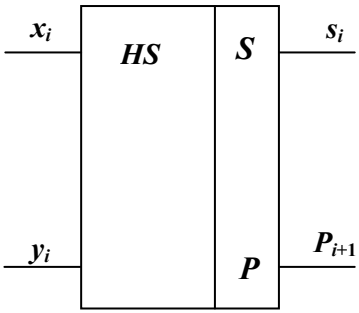


Рис. **1.28.** Одноразрядный комбинационный полусумматор ***HS*** (условное обозначение) [**30**, с.80]

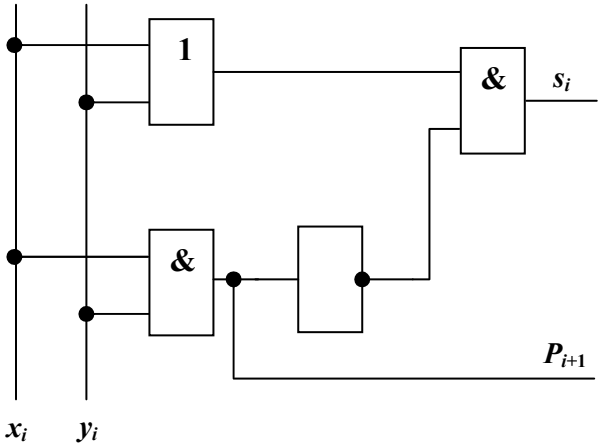


Рис. **1.29.** Одноразрядный комбинационный полусумматор ***HS*** (функциональная схема) [**30**, с.80; **39**, с.117]

Таблица истинности полного сумматора ***FS*** (full-sum) на 1 разряд, обозначенный как ***SM***, представлена в табл. 1.21, а условное обозначение этого сумматора показано на рис. 1.30.

Возможная схема комбинационного сумматора ***FS*** представлена на рис. 1.31.

Таблица 1.21. Таблица истинности полного одноразрядного сумматора ***FS*** (***SM***), учитывающего бит переноса [**30**, с.80]

Входы			Выходы	
x_i	y_i	P_i (бит переноса)	S_i (сумма)	P_{i+1} (бит переноса)
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

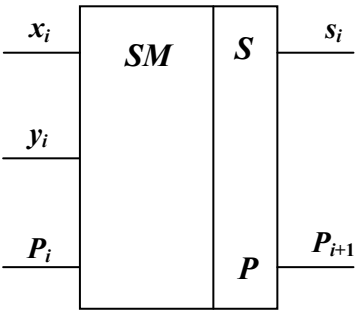


Рис. **1.30.** Одноразрядный комбинационный полный сумматор ***SM*** (условное обозначение) [**30**, с.81]

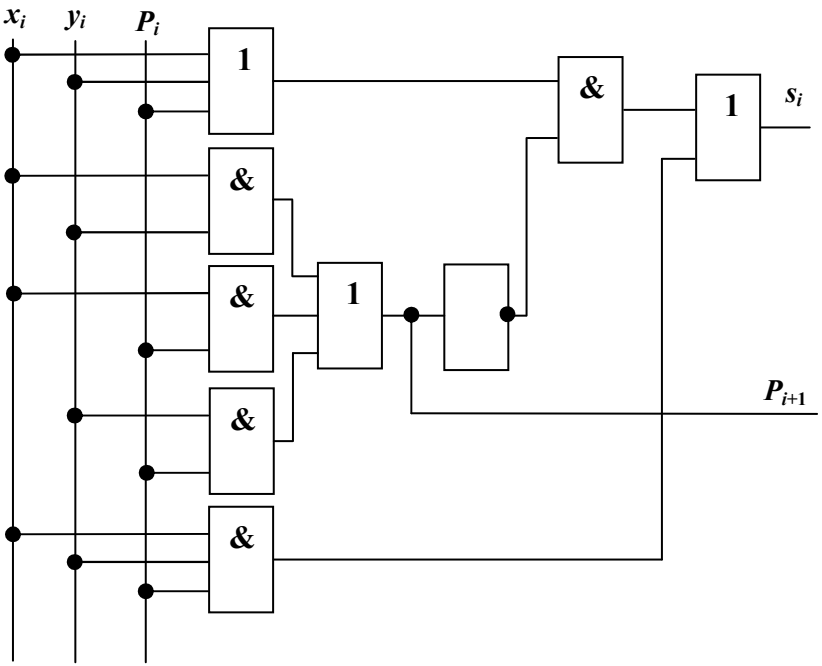


Рис. **1.31.** Одноразрядный комбинационный полный сумматор ***SM*** (функциональная схема) [**30**, с.81]

Полный сумматор ***SM*** в отличие от полусумматора ***HS*** должен воспринимать не два входных сигнала, а три и соответственно иметь для них три входа: два — для слагаемых x_i, y_i и один — для сигнала переноса с предыдущего i–го разряда P_i.

На практике при синтезе схем поступают следующим образом.

Если известна только таблица истинности для данной ЛФ, то по ней строят СДНФ или СКНФ. Далее уже выполняют сам синтез комбинационной схемы, реализующей данную ЛФ по этим формулам.

Если известна только формула для данной ЛФ, то по ней строят СДНФ или СКНФ путем преобразования этой формулы.

Имея СДНФ или СКНФ, выполняют синтез комбинационной схемы. Иногда выполняют синтез и по исходной формуле, не выполняя ее преобразований к СДНФ или СКНФ. Можно по формуле построить таблицу истинности, а по ней уже построить СДНФ или СКНФ, а затем уже выполнить сам синтез комбинационной схемы.

Если известна комбинационная схема, то строят ее таблицу истинности путем полного перебора возможных входных значений ее входов с фиксацией значений выходов схемы с последующей записью результатов перебора в таблицу истинности.

Имея таблицу истинности, строят СДНФ или СКНФ. В некоторых случаях можно сразу построить формулу, которая не обязательно будет СДНФ или СКНФ.

Триггеры

Триггеры в цифровой схемотехнике являются основными элементами, которые используют как запоминающие элементы в ЦВМ. Термин *триггер* происходит от английского слова *trigger* — защелка, спусковой крючок (спусковой механизм). Триггер — это, по сути, элемент с памятью.

Определение 1.61

Накапливающая схема (элемент с памятью) [**31**, с.205] — это схема, выходной сигнал в которой зависит как от входных сигналов, так и от состояния схемы в предыдущие моменты времени.

Определение 1.62

Триггер [**39**, с.120] — устройство, которое может запоминать сигналы 0 или 1, демонстрировать их, а в случае необходимости и забывать.

Триггер в *электронных* ЦВМ (ЭЦВМ) представляет собой электронную схему с двумя устойчивыми состояниями. Одно из этих состояний соответствует *логической единице*, а другое — *логическому нулю* (или, соответственно, *двоичной единице* и *двоичному нулю*). Отметим, что в случае реализации триггера с помощью электромеханического реле одно состояние такого триггера будет соответствовать одному набору каких-то замкнутых (разомкнутых) контактов реле, а другое состояние — другому набору каких-то замкнутых (разомкнутых) контактов в зависимости от конкретной реализации такого триггера на заданных типах реле и переключателей (кнопок).

Механическим аналогом триггера является [**39**, с.120] простейший (рис. 1.32) выключатель (тумблер).

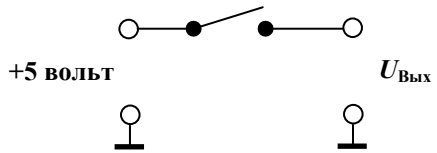


Рис. **1.32.** Механический триггер на тумблере

Тумблер (если он исправен) может находиться только в следующих двух устойчивых состояниях (положениях): включен или выключен.

Если тумблер включен, то на выходе (рис. 1.32) будет напряжение $\boldsymbol{U_{Вых}}$**=+5** В, что в данном случае соответствует логической единице. При включенном тумблере такой триггер хранит (помнит) логическую единицу.

Если тумблер выключен, то на выходе (рис. 1.32) не будет напряжения, т.е. $\boldsymbol{U_{Вых}}$**=0** В, что в данном случае соответствует логическому нулю. При выключенном тумблере такой триггер хранит (помнит) логический нуль.

Отметим, что при данной реализации триггера в виде тумблера у него нет запрещенных состояний, так как тумблер не может одновременно находиться как во включенном, так и в выключенном состоянии. Такой триггер, работа которого подчиняется законам *классической физики*, не может одновременно находиться в двух разных состояниях. Однако если триггер реализован с помощью квантовых объектов, то он уже может находиться в двух совершенно разных состояниях одновременно, т.е. в *суперпозиции*.

ВАЖНО. В *квантовом вычислителе* элемент *триггер* в виде так называемого **кубита** (*qubit* – quantum bit) может находиться в двух совершенно разных состояниях одновременно, т.е. быть в так называемой *суперпозиции* других состояний, где каждому состоянию соответствует своя *амплитуда вероятности* (т.е. комплексное число). *Система кубитов* может быть в *перепутанном* состоянии — необычное для цифровой схемотехники состояние таких триггеров в виде кубитов. Все это позволяет *квантовому вычислителю* выполнять параллельные вычисления с огромной скоростью.

Таблица истинности простейшего асинхронного ***RS*** триггера для ЦВМ представлена в табл. 1.22, а условное обозначение этого триггера показано на рис. 1.33. У ***RS*** триггера имеются два входа. Один вход установочный (***S*** – set), а другой вход сброса (***R*** – reset), и два выхода Q и $\overline{Q}$. Важно отметить, что два выхода связаны не со свойством обратимости данного элемента. Выход Q является прямым выходом, а выход $\overline{Q}$ – его инверсным выходом. Состояние ***RS*** триггера идентифицируется его прямым выходом Q.

Таблица 1.22. Таблица истинности ***RS*** триггера [**30**, с.65]

Вход		Выходы		Режим работы
R_t	S_t	Q_t	Q_{t+1}	
0	0	0	0	Хранение 0
0	0	1	1	Хранение 1
0	1	0	1	Установка в 1
0	1	1	1	Подтверждение 1
1	0	0	0	Подтверждение 0
1	0	1	0	Установка в 0
1	1	0	**?**	Недопустимое состояние
1	1	1	**?**	

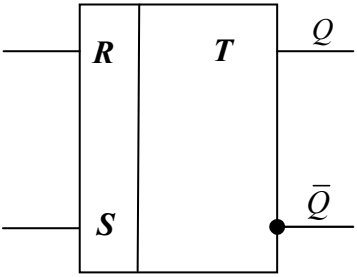


Рис. **1.33.** Простейший ***RS*** триггер (условное обозначение)

Работа триггера как некоторого автомата с памятью отражается с помощью таблицы переходов (таблицы истинности (табл. 1.22)), где отражена зависимость состояния Q_{t+1} ***RS*** триггера в такте t+1 от предшествующего состояния Q_t и от состояния входов ***R*** и ***S***.

Используя таблицу истинности ***RS*** триггера (табл. 1.22), нетрудно получить формулу для зависимости Q_{t+1} от Q_t, R_t, S_t в следующих двух базисах [**30**, с.65]:

$$Q_{t+1} = \overline{S_t \vee \overline{R_t \vee Q_t}}$$ (в базисе ИЛИ-НЕ см. рис. 1.34);

$$Q_{t+1} = \overline{\overline{S}_t \,\&\, \overline{\overline{R}_t \,\& Q_t}}$$ (в базисе И-НЕ).

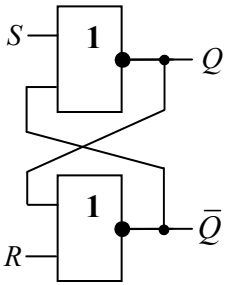


Рис. **1.34.** Реализация ***RS*** триггера на логических элементах ИЛИ-НЕ [**30**, с.66]

Триггеры в ЭЦВМ являются основными компонентами, из которых строят более сложные цифровые элементы — *регистры*.

В отличие от триггеров, которые могут хранить только один бит данных, в регистре, состоящем из 8 триггеров, можно уже хранить один байт данных (т.е. 8 бит данных). Аналогично в *квантовом вычислителе* используется *квантовый регистр,* содержащий *квантовые триггеры* (т.е. кубиты).

ВАЖНО. На практике при реализации цифровых схем следует учитывать так называемое время задержки элементов. Так для комбинационных схем при подаче на их входы цифровых сигналов конечный результат их работы следует считывать после того, как произойдут все переходные процессы во всех элементах схемы.

ВАЖНО. В цифровой схемотехнике при изображении электронных схем принято, что линии — это провода, по которым течет ток. С помощью этих линий изображают соединения входа одного элемента с выходом некоторого другого элемента. Порядок соединения элементов и связей между ними представляется схемой, на которой изображены сами элементы с их маркировкой (обозначением), с указанием входов и выходов этих элементов и связей между ними (т.е. соединений входов и выходов). Результатом работы устройства, представленного такой схемой, является содержимое элементов памяти (триггеров) или состояния выходов, например комбинационной схемы.

ВАЖНО. В случае *квантового вычислителя* применяют также схемы, похожие на те, что применяются в цифровой схемотехнике при изображении электронных схем. Однако есть различие в представлениях *квантовых схем*. Результат работы устройства, представленного *квантовой схемой*, всегда содержится только в *квантовом регистре*. Такую схему (см. [**17**, с.45]) читают слева направо. Линии показывают течение времени или физическую частицу (например, фотон), которая перемещается в пространстве из одного места в другое. Изображенные на схеме квантовые элементы (гейты) при конкретной их физической реализации показывают, какое физическое воздействие, в какой последовательности и на какие кубиты (т.е. *квантовые триггеры*) необходимо произвести, чтобы выполнить *квантовые* вычисления, предусмотренные данной *квантовой схемой*.

Рассмотрим некоторые типичные примеры решения задач, связанных с комбинационными схемами.

***Пример* 1.16** (задача прямого анализа комбинационной схемы)

Известен входной вектор $\vec{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$ и логические элементы НЕ, И-НЕ, ИЛИ с известными таблицами истинности, представленными на рис. 1.35.

НЕ

x_1	f_1
0	1
1	0

И-НЕ

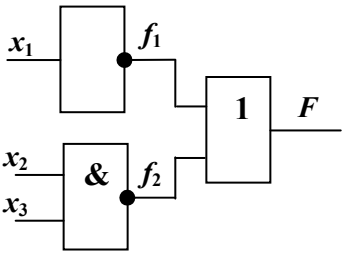
x_2	x_3	f_2
0	0	1
0	1	1
1	0	1
1	1	0

ИЛИ

f_1	f_2	F
0	0	0
0	1	1
1	0	1
1	1	1

Рис. **1.35.** Таблицы истинности элементов НЕ, И-НЕ, ИЛИ

Требуется определить выходной вектор $\vec{y} = [F]$ на выходе следующей комбинационной схемы, состоящей из этих логических элементов:



Решение

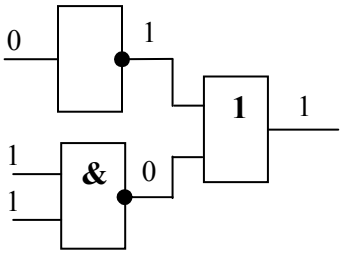
1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $\vec{x}$, выходной вектор $\vec{y}$ и таблицы истинности соответствуют одному и тому же вычислительному базису, который для решения этой задачи знать не обязательно.

2). Рассматриваем схему с начала (т.е. слева направо). Узнаем, что будет на выходе элемента НЕ, если на его вход подан логический нуль (так как x_1=0). Согласно таблице истинности элемента НЕ на его выходе при x_1=0 будет логическая единица, т.е. f_1=1 (на рис. 1.35 стрелкой показана соответствующая строка x_1=0 таблицы истинности для элемента НЕ).

3). Узнаем, что будет на выходе двухвходового элемента И-НЕ, если на оба его входа подана логическая единица (так как x_2=1 и x_3=1). Согласно таблице истинности элемента И-НЕ на его выходе при x_2=1 и x_3=1 будет логический нуль, т.е. f_2=0 (на рис. 1.35 стрелкой показана соответствующая строка x_2=1 и x_3=1 таблицы истинности для элемента И-НЕ).

4). Узнаем, что будет на выходе двухвходового элемента ИЛИ, если на один его вход подана логическая единица (так как f_1=1), а на другой его вход подан логический нуль (так как f_2=0). Согласно таблице истинности элемента ИЛИ на его выходе при f_1=1 и f_2=0 будет логическая единица, т.е. F =1 (на рис. 1.35 стрелкой показана соответствующая строка f_1=1 и f_2=0 таблицы истинности для элемента ИЛИ).

5). Полученный результат удобно представить следующим образом:



Таким образом, выходной вектор есть $\vec{y}$=[1], т.е. на выходе комбинационной схемы будет логическая единица, если на ее вход подан вектор $\vec{x} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$.

6). И тем самым задача решена■

***Пример* 1.17** (задача обратного анализа комбинационной схемы)

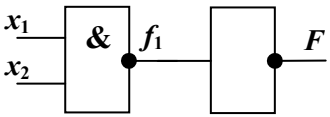
Известен выходной вектор $\vec{y}$ =[***F***] = [1] и логические элементы И-НЕ, НЕ с известными таблицами истинности, представленными на рис. 1.36.

И-НЕ			
x_1	x_2	f_1	
0	0	1	
0	1	1	
1	0	1	
1	1	0	⇐

НЕ		
f_1	F	
0	1	⇐
1	0	

Рис. **1.36.** Таблицы истинности элементов И-НЕ, НЕ

Требуется определить входной вектор $\vec{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ на входе следующей комбинационной схемы, состоящей из этих логических элементов:



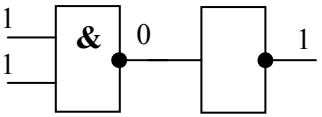
Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $\vec{x}$, выходной вектор $\vec{y}$ и таблицы истинности соответствуют одному и тому же вычислительному базису, который для решения этой задачи знать не обязательно.

2). Рассматриваем схему с конца (т.е. справа налево). Узнаем, что было на входе элемента НЕ, если на его выходе была логическая единица (так как ***F***=1). Согласно таблице истинности элемента НЕ на его входе при ***F***=1 был логический нуль, т.е. f_1=0 (на рис. 1.36 стрелкой показана соответствующая строка f_1=0 таблицы истинности для элемента НЕ).

3). Узнаем, что было на входе элемента И-НЕ, если на его выходе был логический нуль (так как f_1=0). Согласно таблице истинности элемента И-НЕ на его входе при f_1=0 были две логические единицы, т.е. x_1=1 и x_2=1 (на рис. 1.36 стрелкой показана соответствующая строка x_1=1 и x_2=1 таблицы истинности для элемента И-НЕ).

4). Полученный результат удобно представить следующим образом:



Таким образом, входной вектор есть $\vec{x}=\begin{bmatrix}1\\1\end{bmatrix}$, т.е. на входе комбинационной схемы было две логических единицы, если на ее выходе был вектор $\vec{y}$ = [1], т.е. логическая единица (так как F=1) .

5). И тем самым задача решена■

ОТМЕТИМ. В данном примере удалось решить задачу обратного анализа комбинационной схемы, т.е. восстановить однозначно входной вектор. В общем случае это сделать не всегда удается, так как используемые логические элементы **необратимы** (например, элементы И, ИЛИ, И-НЕ (на два входа) и др. являются необратимыми элементами), и получить однозначно один единственный входной вектор (зная выходной вектор) не представляется возможным. В квантовых вычислениях используются обратимые элементы наподобие рассмотренного выше элемента **CNOT**. Применение обратимых элементов позволяет однозначно восстанавливать входные данные по выходным данным.

***Пример* 1.18** (задача синтеза комбинационной схемы)

Известна аналитическая запись логической функции в виде следующей формулы (структурной формулы [**39**,с.102]):

$$f(x_1,x_2)=\left(\overline{\overline{x}_1+x_2}\right)+x_1.$$

Требуется синтезировать (построить) комбинационную схему, реализующую логику работы согласно этой логической функции. Так как данной логической функции (в общем случае) может соответствовать не одна комбинационная схема, то достаточно найти хотя бы одно решение (т.е. построить одну комбинационную схему).

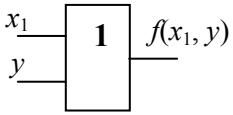
Решение

1). В условиях задачи не указан явно вычислительный базис. Будем далее предполагать, что входной вектор $\vec{x}$, выходной вектор $\vec{y}$ и таблицы истинности соответствуют одному и тому же вычислительному базису, который для решения этой задачи знать не обязательно.

2). Введем дополнительные логические переменные и представим исходную структурную формулу следующим образом:

$$f(x_1,x_2)=\left(\overline{\overline{x}_1+x_2}\right)+x_1=y+x_1,\ \text{где}\ y=\left(\overline{\overline{x}_1+x_2}\right).$$

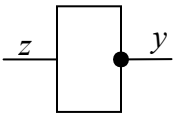
Тогда ЛФ $f(x_1,x_2)=y+x_1$ соответствует следующая комбинационная схема 1:



3). Аналогично ЛФ $y=\left(\overline{\overline{x}_1+x_2}\right)$ представим следующим образом:

$$y=\left(\overline{\overline{x}_1+x_2}\right)=\overline{z},\ \text{где}\ z=\left(\overline{x}_1+x_2\right).$$

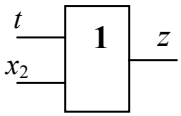
Тогда ЛФ $y = \overline{z}$ соответствует следующая комбинационная схема 2:



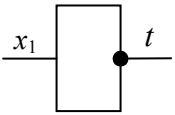
4). Аналогично ЛФ $z = \left(\overline{x}_1 + x_2\right)$ представим следующим образом:

$$z = \left(t + x_2\right), \text{ где } t = \overline{x}_1 .$$

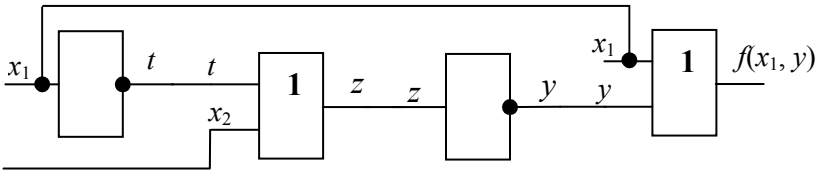
Тогда ЛФ $z = \left(t + x_2\right)$ соответствует следующая комбинационная схема 3:



5). Логической функции $t = \overline{x}_1$ соответствует следующая комбинационная схема 4:



6). Объединяя все 4 комбинационные схемы в одну, получаем следующую итоговую комбинационную схему:



Таким образом, найдено одно из возможных решений в базисе элементов ИЛИ, НЕ.

7). И тем самым задача решена■

Выводы (резюме) по разделу 1.2

1. **Цифровая вычислительная машина** (ЦВМ) — машина, оперирующая информацией, представленной в дискретном виде.
2. При разработке ЦВМ применяют *анализ* и *синтез* цифровых схем, в основе которых лежат *логические элементы*, реализующие заданные *логические функции* (ЛФ). Подходящим математическим аппаратом для анализа и синтеза цифровых схем является *алгебра Буля.*
3. ЛФ можно представить таблицей истинности или формулой. ЛФ можно представить в двух различных формах: *совершенная дизъюнктивная нормальная форма* (СДНФ) и *совершенная конъюнктивная нормальная форма* (СКНФ).
4. Одну и ту же ЛФ можно представить разными способами. Доказано, что *конъюнкция*, *дизъюнкция* и *отрицание* образуют базис. Другим базисом является функция Пирса (ИЛИ-НЕ) или функция Шеффера (И-НЕ). Помимо базиса как *системы логических функций* очень большое значение играет не менее важный *вычислительный базис*.
5. **Вычислительный базис** — это обычно два устойчивых состояния некоторой физической системы, принятые для физической реализации на практике **0** или **1** (например, *логического нуля, логической единицы* или *двоичного нуля*, *двоичной единицы*). Смена вычислительного базиса (т.е. смена режима работы ЛЭ) может в корне поменять логику работы ЛЭ, так ЛЭ ИЛИ может начать функционировать как элемент И.
6. Логика работы ЛЭ описывается таблицей истинности, и они могут быть реализованы различным образом. Например элемент ИЛИ, элемент И могут быть реализованы с помощью переключателей или диодов. Логические элементы могут быть реализованы с помощью квантовых объектов (так называемых квантовых гейтов). В случае *квантового вычислителя* некоторым аналогом таблицы истинности для гейта является *унитарная матрица*.
7. Квантово-механическое обозначение обобщенного элемента XOR несколько необычно и отличается от способа обозначения традиционным способом в кибернетике. В кван-

тово-механическом случае принято говорить, что такая операция есть **контролируемое НЕ** (CNOT — *controlled not*), а бит цели изменяет свое состояние тогда и только тогда, когда состояние бита источника есть 1, при этом состояние бита источника не меняется. Аналогично вводится понятие и 3-входового элемента **контролируемое НЕ**, которое получило название *вентиля Тоффоли*.

8. Конечный результат работы ЛЭ (в более общем случае — комбинационной схемы) на практике получается путем **измерения** с помощью некоторого прибора (в данном случае, например, вольтметром). Повторные измерения не изменяют состояние ЛЭ и не разрушают физические процессы, протекающие в физической реализации ЛЭ. В случае *квантового вычислителя* процесс **измерения** разрушает текущее состояние квантового объекта (системы), используемого для физической реализации ЛЭ (гейта).
9. Триггеры в цифровой схемотехнике являются основными элементами, которые используют как запоминающие элементы. Триггер в ЭЦВМ представляет собой электронную схему с двумя устойчивыми состояниями. Одно из этих состояний соответствует *логической единице*, а другое — *логическому нулю* (или, соответственно, *двоичной единице* и *двоичному нулю*).
10. При реализации триггера в виде тумблера у него нет запрещенных состояний, так как тумблер не может одновременно находиться как во включенном, так и в выключенном состоянии. Такой триггер, работа которого подчиняется законам *классической физики*, не может одновременно находиться в двух разных состояниях. Однако если триггер реализован с помощью квантовых объектов, то он уже может находиться в двух совершенно разных состояниях одновременно, т.е. в состоянии так называемой *суперпозиции*.
11. В случае *квантового вычислителя* элемент *триггер* в виде так называемого **кубита** может находиться в двух совершенно разных состояниях одновременно, т.е. быть в состоянии, являющемся *суперпозицией* других состояний. *Система кубитов* может быть в *перепутанном* состоянии — необычное для цифровой схемотехники состоя-

ние таких триггеров в виде кубитов. Все это позволяет *квантовому вычислителю* выполнять параллельные вычисления с огромной скоростью.

12. В отличие от триггеров, которые могут хранить только один бит данных, в регистре, состоящем из 8 триггеров, можно хранить один байт данных (8 бит). Аналогично в *квантовом вычислителе* используется *квантовый регистр,* содержащий *квантовые триггеры* (кубиты).
13. На практике при реализации цифровых схем следует учитывать так называемое время задержки элементов. Так для комбинационных схем при подаче на их входы цифровых сигналов конечный результат их работы следует считывать после того, как произойдут все переходные процессы во всех элементах схемы.
14. В цифровой схемотехнике при изображении электронных схем принято, что линии — это провода, по которым течет ток. С помощью этих линий изображают соединения входа одного элемента с выходом некоторого другого элемента. Порядок соединения элементов и связей между ними представляется схемой, на которой изображены сами элементы с их маркировкой (обозначением) с указанием входов и выходов этих элементов и связей между ними (т.е. соединений входов и выходов). Результатом работы устройства, представленного такой схемой, является содержимое элементов памяти (триггеров) или состояния выходов, например, комбинационной схемы.
15. В случае *квантового вычислителя* применяют схемы, похожие на те, что применяются в цифровой схемотехнике для ЭЦВМ. Однако есть различие. Результат работы устройства, представленного *квантовой схемой*, всегда содержится только в *квантовом регистре*. Такую схему читают слева направо. Линии показывают течение времени или физическую частицу. Изображенные на схеме квантовые элементы (гейты) показывают, какое физическое воздействие, в какой последовательности и на какие кубиты (*квантовые триггеры*) необходимо произвести, чтобы выполнить *квантовые* вычисления, предусмотренные данной *квантовой схемой*.

1.3. Аналоговые вычисления

«Не говори, чему учили, а скажи, что узнал.»
(Пословица) [**28**]

«Можно было бы подумать, что квантовые компьютеры являются разновидностью аналоговых компьютеров, поскольку при описании состояний кубитов используются непрерывные параметры; однако оказывается, что влияние шума на квантовый компьютер может быть *оцифровано*. В результате преимущества квантовых компьютеров сохраняются даже при наличии конечного шума.»
М. Нильсен, И. Чанг [**17**, с.215]

Содержание
Аналоговая вычислительная машина (АВМ). Гибридная вычислительная машина (ГВМ). Аналоговый умножитель, решатель кубического уравнения, двоичный сумматор. Квантовый вычислитель как современная ГВМ.

Вид перерабатываемой информации оказывает [**31**, с.14] влияние на структуру вычислительного устройства (*вычислительной машины* (ВМ)). Обычно быстродействие ЦВМ ограничено тактовой частотой работы процессора и объемом оперативной памяти и ее быстродействием. Точность решения задачи зависит от многих параметров и, в частности, от разрядности процессора, а иногда и от времени решения задачи. В некоторых случаях на практике не всегда удается обеспечить с помощью ЦВМ требуемое быстродействие при решении заданной задачи. Для обеспечения большого быстродействия вместо ЦВМ применяют аналоговые вычислительные устройства (машины). Принято полагать, что точность решения задачи на ЦВМ обычно выше, чем на аналоговых ВМ.

Определение 1.63
Аналоговая вычислительная машина (АВМ) [**31**, с.14] — машина, оперирующая информацией, представленной в виде непрерывных изменений некоторых физических величин.

ОТМЕТИМ. В качестве переменных физических величин могут быть взяты [**31**, с.14-15] сила тока, напряжение, изменение скорости, ускорения движения тела и т.п. Важным элементом АВМ является *операционный усилитель* (ОУ). Используя ОУ, можно реализовать, например [**66**, с.231-258], арифметические операции.

Определение 1.64

Гибридная вычислительная машина (ГВМ) [**31**, с.14] — машина, оперирующая информацией, представленной в виде непрерывных изменений некоторых физических величин.

ОТМЕТИМ [**64**, с.6]. ГВМ не присущи свойства универсальности и поэтому ГВМ — *специализированные* вычислительные машины.

На практике специалисты (в зависимости от принципа действия основных узлов АВМ, ЦВМ, ГВМ) вычислительные устройства разделяют на ([**31**, с.18]) механические, смешанные (гидромеханические, электромеханические, пневмомеханические и т.п.) и электронные. В настоящее время широкое распространение получили именно электронные ЦВМ в виде персональных компьютеров (электронных ВМ (ЭВМ)). В отличие от персональных ЭВМ (на данном этапе развития техники) АВМ и ГВМ [**64**, **65**, **67**, **68**] широко пока не применяются. Несмотря на наличие мощных современных ЭВМ все-таки стали развиваться и другие типы вычислительных устройств — это нейрокомпьютеры [**79** – **85**], ДНК компьютеры [**70**] и квантовые компьютеры [**17**, **19**, **26**, **71** – **78**].

В основе квантового компьютера (*квантового вычислителя*) лежит квантовый процессор. *Квантовый вычислитель* (КВ) обладает похожими свойствами не только, как и ЦВМ — одна информация представлена дискретно в виде отдельных (дискретных) **кубитов**, но и как в АВМ — другая информация представлена непрерывно в виде **непрерывных амплитуд вероятностей**. В некотором смысле можно (с осторожностью) полагать, что *квантовый вычислитель* это и есть современная ГВМ.

ОТМЕТИМ. На практике в электронных компонентах АВМ возникают различные шумы, приводящие к потере точности проводимых вычислений. Специалисты [**17**, с.24,215] полагают, что в отличие от аналоговых вычислений квантовые вычисления в принципе допускают наличие конечного уровня шума, сохраняя свои вычислительные достоинства.

Именно то, что *квантовый вычислитель* есть ГВМ, позволило КВ вобрать в себя лучшие свойства как ЦВМ (это возможность применить помехоустойчивое кодирование с целью исправления

возникающих ошибок, что не доступно АВМ), так и АВМ (это огромное быстродействие, что пока не могут обеспечить современные ЦВМ).

Аналоговый умножитель

На рис. 1.37 представлен аналоговый умножитель, реализованный с помощью линейного потенциометра.

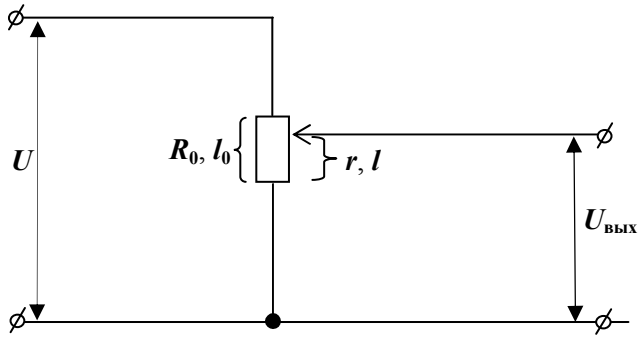


Рис. **1.37.** Линейный потенциометр [**32**, с.48]

Потенциометр имеет щетку и сопротивление. Щетку можно перемещать вдоль той части, где размещено его сопротивление. Щетку можно установить в начало сопротивления (потенциометра), в конец потенциометра, а можно и в промежуточное положение. Сопротивление характеризуется длиной. На рис. 1.37 щетка обозначена стрелкой, а сопротивление — прямоугольником.

Для линейного потенциометра характерно то, что на каждую единицу его длины (т.е. той части, где размещено его сопротивление) приходится одно и то же сопротивление. На рис. 1.37 показано:

U – напряжение питания;

$U_{вых}$ – выходное напряжение потенциометра;

R_0 – полное сопротивление потенциометра;

l_0 – максимальная величина длины перемещения щетки;

r – промежуточное значение сопротивления потенциометра;

l – величина длины перемещения щетки от начального положения.

Выходное напряжение потенциометра в режиме холостого хода можно выразить следующим образом [**32**, с.48]:

$$U_{\text{вых}} = \frac{r}{R_0} U \ . \qquad (1.25)$$

Так как рассматриваемый потенциометр линейный, то для него справедливо следующее [**32**, с.48]:

$$\frac{r}{R_0} = \frac{l}{l_0}, \qquad (1.26)$$

а следовательно для выходного напряжения потенциометра справедливо следующее [**32**, с.48]:

$$U_{\text{вых}} = \frac{l}{l_0} U = m \cdot U \ , \qquad (1.27)$$

где $m = \frac{l}{l_0}$ — это относительное перемещение щетки потенциометра, причем $0 \le m \le 1$.

Умножение двух чисел можно выполнять следующим образом. Допустим, надо перемножить два числа ***x*** и ***y***. Первый сомножитель ***x*** устанавливается с помощью напряжения ***U***, так что ***U*** = ***x***. Второй сомножитель ***y*** устанавливается с помощью щетки на расстоянии ***l***, так что ***m*** = ***y***.

После того как потенциометр выставлен (т.е. щетка установлена) и подано входное напряжение ***U***, на выходе потенциометра его выходное напряжение $\boldsymbol{U_{\text{вых}}}$ будет соответствовать результату умножения числа ***x*** на число ***y***. Точность выполнения вычисления зависит от точности выставления напряжения ***U***, точности измерения конечного результата, т.е. напряжения $\boldsymbol{U_{\text{вых}}}$, а также от того, насколько действительно линеен сам потенциометр, т.е. от качества механизма перемещения щетки.

Так работает аналоговое электронное устройство умножения двух чисел.

На рис. 1.38 представлен более усложненный вариант аналогового умножителя на три числа ***x***, ***y***, ***z***.

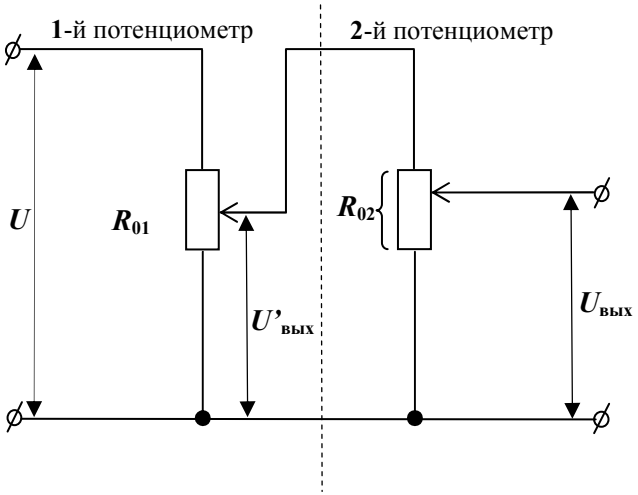


Рис. **1.38.** Аналоговый умножитель на потенциометрах [**32**, с.48]

Умножение трех чисел можно выполнять следующим образом. Первый сомножитель $\boldsymbol{x}$ устанавливается с помощью напряжения $\boldsymbol{U}$, так что $\boldsymbol{U}=\boldsymbol{x}$. Второй сомножитель $\boldsymbol{y}$ устанавливается с помощью щетки первого потенциометра на расстоянии $\boldsymbol{l_1}$, так что $\boldsymbol{m_1}=\boldsymbol{y}$.
Третий сомножитель $\boldsymbol{z}$ устанавливается с помощью щетки второго потенциометра на расстоянии $\boldsymbol{l_2}$, так что $\boldsymbol{m_2}=\boldsymbol{z}$. После того как оба потенциометра выставлены (т.е. обе щетки установлены) и подано входное напряжение $\boldsymbol{U}$, на выходе второго потенциометра его выходное напряжение $\boldsymbol{U_{вых}}$ будет соответствовать результату умножения числа $\boldsymbol{x}$ на число $\boldsymbol{y}$. Для этого умножителя справедливо следующее [**32**, с.49]:

$$U'_{\text{вых}} = m_1 \cdot U \,, \tag{1.28}$$

$$U_{\text{вых}} = m_2 \cdot U'_{\text{вых}} = m_1 \cdot m_2 \cdot U \,. \tag{1.29}$$

Последовательное применение этих потенциометров позволяет увеличить число сомножителей до заданного их числа.

Аналоговый решатель кубического уравнения

Следующий рассматриваемый аналоговый процессор предназначен для решений кубических уравнений следующего вида [**27**]:

$$ax^3 + bx^2 + cx + d = 0. \tag{1.30}$$

Напомним, что решить такое уравнение (1.30) означает определить его корень, т.е. найти такое значение переменной $\boldsymbol{x}$, что многочлен

слева от знака равенства будет равен 0.

В устройстве механического процессора используются (рис. 1.39):

- емкость с водой в виде большого аквариума;
- весы в виде коромысла с двумя чашами;
- набор 4-х твердых тел вращения различной геометрической формы, являющихся аналогами для следующих членов уравнения:
  - цилиндр соответствует $\sim \boldsymbol{x}^1$, $V_{\text{Ц}} = \pi R_{\text{Ц}}^2 h$;
  - конус соответствует $\sim \boldsymbol{x}^2$, $V_{\text{К}} = \frac{1}{3}\pi R_{\text{К}}^2 h$;
  - параболоид соответствует $\sim \boldsymbol{x}^3$, $V_{\text{П}} = \frac{1}{2}\pi R_{\text{П}}^2 h$;
  - шар соответствует $\sim \boldsymbol{x}^0$, $V_{\text{Ш}} = \frac{4}{3}\pi R_{\text{Ш}}^3$.

В устройстве (рис. 1.39) *шар* всегда остается полностью погруженным в воду. *Параболоид* (при глубине погружения, равной $\boldsymbol{x}$ см), опущенный в воду скругленной вершиной вниз, вытеснит $\sim \boldsymbol{x}^3$ куб. см воды. Аналогично *конус* (при глубине погружения, равной $\boldsymbol{x}$ см), опущенный в воду острой вершиной вниз, вытеснит $\sim \boldsymbol{x}^2$ куб. см воды.

К коромыслу весов подвешены 4 тела, как показано на рис. 1.39. Дополнительно к этому коромыслу по краям подвешены еще по одной чашке для гирек, причем центр коромысла совпадает с осью весов.

Это устройство на практике решает заданное кубическое уравнение вида (1.30) следующим образом.

Параболоид располагают справа от оси весов на расстоянии a см, если $a>0$, или слева, если $a<0$. Аналогично располагаются и другие 3 тела. В соответствии с законом Архимеда, тело, погруженное в воду, уменьшает свой вес пропорционально погруженному объему в воду этого тела. Величина отклонения весов (т.е. коромысла весов) от положения равновесия зависит от глубины погружения тел и от расстояния, на котором эти тела находятся от оси весов.

Равновесие системы добиваются путем добавления гирек на соответствующую чашу весов.

Установление нулевого уровня

Для того чтобы установить нулевой уровень, необходимо, удерживая весы в равновесии, заливать небольшими порциями воду в аквариум. Как только 3 подвешенных тела коснутся воды, то подачу воды в аквариум следует немедленно прекратить (отметим, что при отпускании весов они выйдут из равновесия). Установившийся уровень воды в аквариуме следует отметить как нулевой.

Решение кубического уравнения

Перед началом поиска решения весы находятся в равновесии и нам известно, где находится нулевой уровень. Далее необходимо заливать небольшими порциями воду в аквариум. В процессе добавления воды весы выйдут из равновесия, однако при дальнейшем добавлении воды весы вернутся в равновесие. Как только наступит равновесие весов, подачу воды в аквариум срочно прекращают. Уровень воды в аквариуме отмечают как достигнутый. Разница между достигнутым уровнем и нулевым и есть значение $\boldsymbol{x}$. Отметим, что если уравнение не имеет решения, то весы не удастся установить в равновесие при заполнении водой аквариума.

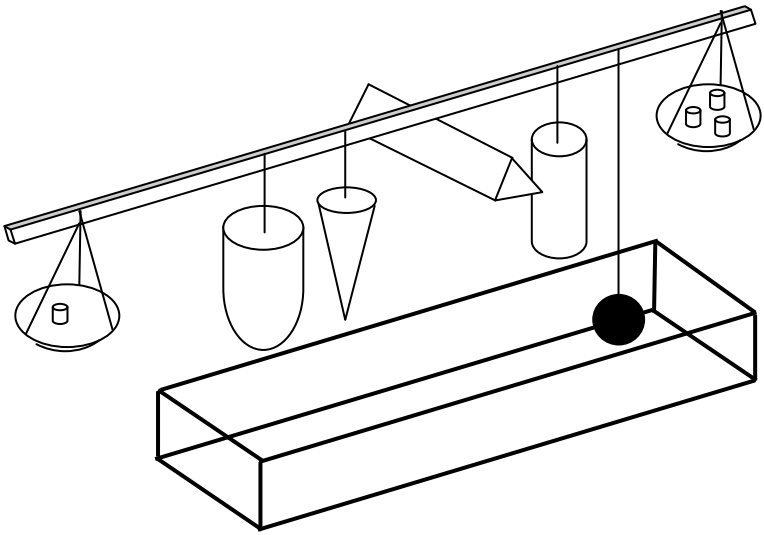


Рис. **1.39.** Аналоговый механический процессор на воде для решения кубических уравнений (см. и ср. с [**27**])

Аналоговый двоичный сумматор

Рассмотрим простейшую аналоговую схему механического сумматора для двух ***m*** разрядных двоичных чисел. Аналогия здесь понимается в том смысле, что в этом сумматоре используются механические логические элементы вместо аналогичных цифровых элементов. На рис. 1.40, 1.41 представлена механическая схема такого суммирующего процессора на *шариках*, *каналах* и *заслонках* для ***m***=4. Это вычислительное устройство имеет в своем составе следующие основные компоненты (элементы):

- два 4-разрядных регистра для хранения (записи, установки) слагаемых чисел: первый регистр для первого слагаемого (он представлен заслонками типа **B**), второй регистр для второго слагаемого (он представлен заслонками типа **A** и набором шариков); каждый механический *регистр* состоит из 4-х механических *триггеров*;
- шарики по числу единиц в двоичной записи второго слагаемого;
- заслонки типа **A** по числу двоичных разрядов слагаемых;
- заслонки типа **C** по числу возможных переносов в следующий разряд;
- заслонки типа **B** (*регистр* из механических *триггеров*) по числу двоичных разрядов слагаемых;
- каналы, по которым могут двигаться шарики под действием силы тяжести; для каждой заслонки типа **B** имеется один *подводящий канал* (слева) и два *отводящих канала* (справа), причем нижний отводящий канал необходим для реализации бита переноса в следующий разряд, а верхний используется для выброса (вывода) шариков из устройства;
- механизм для поворота всего устройства относительно горизонтальной оси данного устройства.

Таким образом, рассматриваемый аналоговый сумматор состоит из заслонок и каналов, соединяющих их. По каналам могут двигаться шарики под действием силы тяжести. Эти шарики могут переводить заслонки из одного состояния в другое.

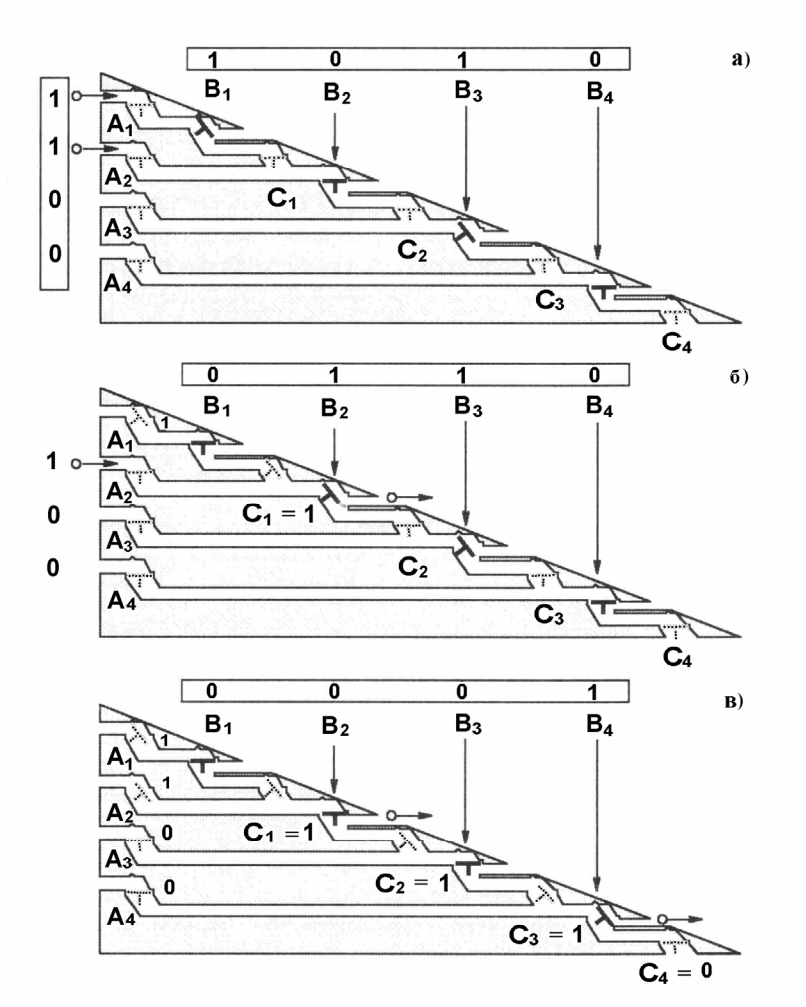


Рис. **1.40.** Механический сумматор на шариках [**26**, **89**]

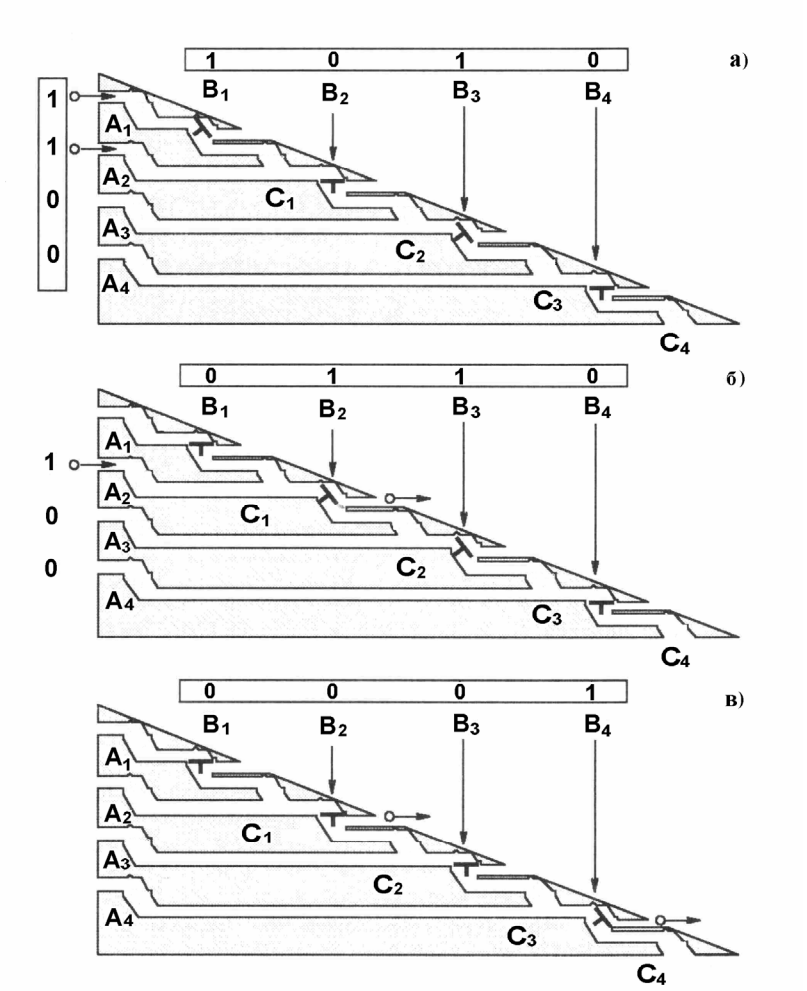


Рис. **1.41.** Необратимый механический сумматор на шариках

Каждая заслонка может быть только в одном из двух следующих состояний:

- **T**– состояние (соответствует двоичному значению 0);
- **λ** – состояние (соответствует двоичному значению 1).

Положение заслонки, соответствующее **λ**–состоянию, означает, что она повернута, положение заслонки, соответствующее **T**–состоянию означает, что она не повернута (рис. 1.40).

Наличие шарика в канале на входе для заслонки **B** соответствует двоичному значению 1, а его отсутствие — 0.

Будем также полагать, что значение 0 соответствует для логической переменной — **ложь**, а значение 1 — **истина**.

Для дальнейшего удобства будем иногда *первый регистр* устройства называть *регистром сумматора* и будем также различать саму заслонку **B** и сам механический блок, реализующий логику работы логического вентиля, обозначенный в данном случае как **V**.

Логический вентиль **V** состоит из заслонки **B**, трех каналов (один подводящий и два отводящих канала) с реализацией возможности наличия в них шарика. Таким образом, в устройстве имеются 4 вентиля **V** — $\mathbf{V_1, V_2, V_3, V_4}$.

Легко заметить, что логический блок данного аналогового сумматора, состоящий из вентиля **V**, реализует свою работу согласно таблице истинности, представленной в табл. 1.23.

Таблица 1.23. Таблица истинности вентиля **V** [**26**]

Начальное состояние входа вентиля **V** (наличие шарика – 1, а его отсутствие – 0)	Состояние заслонки **B**		Конечное состояние нижнего канала выхода (бита переноса)
	Начальное	Конечное	
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Нетрудно убедиться, что табл. 1.23 соответствует операции сложения двух битов данных (под 1-м битом понимается состояние

входа в вентиль **V**; под 2-м битом понимается начальное состояние заслонки **B**). Конечное состояние заслонки **B** и конечное состояние нижнего канала выхода (бита переноса) являются конечным результатом сложения двух двоичных чисел.

Рассмотрим сначала упрощенный вариант сумматора, т.е. без заслонок типа **A** и **C** (рис. 1.41).

Исходное состояние сумматора следующее. Во втором регистре (с помощью двух шариков) установлено (приготовлено) двоичное число 0011 или десятичное число **3** (на рис. 1.41 самому младшему разряду соответствует самый верхний шарик). В первом регистре приготовлено (установлено) двоичное число 0101 или десятичное число **5** (на рис. 1.41 самому младшему разряду соответствует самая левая заслонка типа **B**, т.е. $\mathbf{B_1}$).

Число 0101 (первое слагаемое) в первом регистре установлено следующим образом:

- заслонка $\mathbf{B_1}$ переведена в **λ**–состояние;
- заслонка $\mathbf{B_2}$ переведена в **T**–состояние;
- заслонка $\mathbf{B_3}$ переведена в **λ**–состояние;
- заслонка $\mathbf{B_4}$ переведена в **T**–состояние.

Число 0011 (второе слагаемое) во втором регистре установлено иным образом:

- наличие шарика в канале на входе вентиля $\mathbf{V_1}$ (заслонка $\mathbf{B_1}$);
- наличие шарика в канале на входе вентиля $\mathbf{V_2}$ (заслонка $\mathbf{B_2}$);
- отсутствие шарика в канале на входе вентиля $\mathbf{V_3}$ (заслонка $\mathbf{B_3}$);
- отсутствие шарика в канале на входе вентиля $\mathbf{V_4}$ (заслонка $\mathbf{B_4}$).

Требуется к двоичному числу 0101, содержащемуся в регистре сумматора (т.е. в первом регистре устройства), прибавить другое двоичное число 0011, содержащееся во втором регистре устройства, при этом, если возникнет бит переноса в следующий разряд (что эквивалентно признаку переполнения разрядной сетки при фиксированной разрядности данного сумматора), то необходимо выработать признак этого переноса (в данном случае шарик должен попасть в нижний канал последней (т.е. самой нижней) заслонки типа **B**, т.е. $\mathbf{B_4}$).

Теперь, если заставить двигаться самый верхний шарик (действие начинается с самого младшего разряда) по каналу, то он

(рис. 1.41**б**) сначала повернет первую заслонку $\mathbf{B_1}$, т.е. переведет ее из **λ**–состояния в **Т**–состояние (и тем самым вместо 1 установит 0) и попадет в канал, соответствующий биту переноса в следующий 2-й двоичный разряд. Затем этот шарик повернет вторую заслонку $\mathbf{B_2}$, т.е. переведет ее из **Т**–состояния в **λ**–состояние (и тем самым вместо 0 установит 1) и только после этого покинет данное устройство. Заслонки $\mathbf{B_3}$ и $\mathbf{B_4}$ не использовались (этот первый шарик на них не действовал), т.е. их состояние не изменилось.

Таким образом, число 0101 после действия первого шарика будет преобразовано в промежуточное число 0110 и тем самым будет получен промежуточный результат суммирования.

Число 0110 в первом регистре после действия первого шарика получено следующим образом:

- заслонка $\mathbf{B_1}$ переведена в **Т**–состояние;
- заслонка $\mathbf{B_2}$ переведена в **λ**–состояние;
- заслонка $\mathbf{B_3}$ осталась в **λ**–состоянии;
- заслонка $\mathbf{B_4}$ осталась в **Т**–состоянии.

Далее, если заставить двигаться второй (считая сверху вниз) верхний шарик (вычислительное действие продолжается со второго младшего разряда) по каналу, то он (рис. 1.41**в**) сначала повернет вторую заслонку $\mathbf{B_2}$, т.е. переведет ее из **λ**–состояния в **Т**–состояние (и тем самым вместо 1 установит 0) и попадет в канал, соответствующий биту переноса в следующий 3-й двоичный разряд. Затем этот шарик повернет третью заслонку $\mathbf{B_3}$, т.е. переведет ее из **λ**–состояния в **Т**–состояние (и тем самым вместо 1 установит 0) и попадет в канал, соответствующий биту переноса в следующий 4-й двоичный разряд. Затем этот шарик повернет четвертую заслонку $\mathbf{B_4}$, т.е. переведет ее из **Т**–состояния в **λ**–состояние (и тем самым вместо 0 установит 1) и только после этого покинет данное устройство.

Все заслонки $\mathbf{B_1}$, $\mathbf{B_2}$ и $\mathbf{B_3}$, $\mathbf{B_4}$ использовались обоими шариками.

Таким образом, число 0110 после действия второго шарика будет преобразовано в промежуточное число 1000 и тем самым будет получен окончательный результат суммирования, так как больше шариков нет (было только 2 шарика).

Число 1000 в первом регистре после действия второго шарика получено следующим образом:

- заслонка $\mathbf{B_1}$ осталась в **Т**–состоянии;
- заслонка $\mathbf{B_2}$ переведена в **Т**–состояние;
- заслонка $\mathbf{B_3}$ переведена в **Т**–состояние;
- заслонка $\mathbf{B_4}$ переведена в **λ**–состояние.

На этом работа данного сумматора в виде аналогового механического устройства завершена. Результат суммирования необходимо прочитать (определить, измерить) на механическом регистре, содержащем заслонки типа **В**, что и будет соответствовать конечному результату суммирования, т.е. двоичному числу 1000 или десятичному числу 8 (так как в десятичной системе счисления 5+3=8, а число 8 в двоичной системе счисления есть 1000).

Можно отметить следующее. Запуская в устройство каждый шарик в отдельности, мы как бы расслаиваем исходное двоичное число на слагаемые в записях, в которых присутствует только одна двоичная единица, например исходное число 0011 было представлено следующими двумя двоичными числами 0010 и 0001:

$$\begin{array}{r} 00\mathbf{1}0 \\ + \\ 000\mathbf{1} \\ \hline 00\mathbf{11} \end{array}$$

В данном устройстве выполняется сложение подобных расслоенных чисел с числом, записанным в регистре сумматора. Таких чисел будет столько, сколько единиц в двоичной записи исходного числа, представленного содержимым второго регистра.

Представленный сумматор является необратимым. Действительно, если заставить двигаться шарики в обратном направлении по каналу из тех мест, откуда они вылетели (т.е. были сброшены), то они (см. рис. 1.41**в**) не вернутся достоверно обратно туда, откуда первоначально были запущены в данном устройстве, а конечное состояние такого сумматора после прохождения шариков не будет совпадать с начальным его состоянием. Для того чтобы сделать данный сумматор обратимым, необходимо наличие заслонок типа **А** и **С**. Назначение заслонок типа **А** и **С** — фиксировать состояние входов $\mathbf{A}_i$ и битов $\mathbf{C}_i$ переноса в каждом разряде.

Рассмотрим теперь более усложненный вариант сумматора, т.е. имеющего заслонки типа **A** и **C** (рис. 1.40).

Манипуляции с шариками в данном случае такие же, но есть дополнительные заслонки типа **A** и **C**, которые переходят из одного состояния в другое под воздействием на них этих шариков.

Так, если заставить двигаться самый верхний шарик (действие начинается с самого младшего разряда) по каналу, то он (рис. 1.40**б**) сначала повернет первую заслонку $\mathbf{A_1}$, т.е. переведет ее из **T**–состояния в **λ**–состояние (и тем самым вместо 0 установит 1 на входе вентиля $\mathbf{V_1}$), а затем уже повернет первую заслонку $\mathbf{B_1}$, т.е. переведет ее из **λ**–состояния в **T**–состояние (и тем самым вместо 1 установит 0) и попадет в канал, соответствующий биту переноса в следующий 2-й двоичный разряд, т.е. повернет первую заслонку $\mathbf{C_1}$, и переведет ее из **T**–состояния в **λ**–состояние (и тем самым вместо 0 установит 1 на входе вентиля $\mathbf{V_2}$). Затем этот шарик повернет вторую заслонку $\mathbf{B_2}$, т.е. переведет ее из **T**–состояния в **λ**–состояние (и тем самым вместо 0 установит 1) и только после этого покинет данное устройство.

Заслонки $\mathbf{A_2}$, $\mathbf{A_3}$, $\mathbf{A_4}$ и $\mathbf{C_2}$, $\mathbf{C_3}$, $\mathbf{C_4}$, а также $\mathbf{B_3}$, $\mathbf{B_4}$ не использовались (этот первый шарик на них не действовал), т.е. их состояние не изменилось.

Таким образом (как и в случае с необратимым сумматором), число 0101 после действия первого шарика будет также преобразовано в промежуточное число 0110 и тем самым будет получен промежуточный результат суммирования.

Далее, если заставить двигаться второй (считая сверху вниз) верхний шарик (действие продолжается со второго младшего разряда) по каналу, то он (рис. 1.40**в**) сначала повернет вторую заслонку $\mathbf{A_2}$, т.е. переведет ее из **T**–состояния в **λ**–состояние (и тем самым вместо 0 установит 1 на входе вентиля $\mathbf{V_2}$), а затем уже повернет вторую заслонку $\mathbf{B_2}$, т.е. переведет ее из **λ**–состояния в **T**–состояние (и тем самым вместо 1 установит 0) и попадет в канал, соответствующий биту переноса в следующий 3-й двоичный разряд, т.е. повернет вторую заслонку $\mathbf{C_2}$, и переведет ее из **T**–состояния в **λ**–состояние (и тем самым вместо 0 установит 1 на входе вентиля $\mathbf{V_3}$). Затем этот шарик повернет третью заслонку $\mathbf{B_3}$, т.е. переведет ее из **λ**–состояния в **T**–состояние (и тем самым

вместо 1 установит 0) и попадет в канал, соответствующий биту переноса в следующий 4-й двоичный разряд, т.е. повернет третью заслонку $\mathbf{C_3}$, и переведет ее из **Т**–состояния в **λ**–состояние (и тем самым вместо 0 установит 1 на входе вентиля $\mathbf{V_4}$). Затем этот шарик повернет четвертую заслонку $\mathbf{B_4}$, т.е. переведет ее из **Т**–состояния в **λ**–состояние (и тем самым вместо 0 установит 1) и только после этого покинет данное устройство.

Заслонки $\mathbf{A_1}$, $\mathbf{A_3}$, $\mathbf{A_4}$ и $\mathbf{C_1}$, $\mathbf{C_4}$ не использовались (этот второй шарик на них не действовал), т.е. их состояние не изменилось.

Заслонки $\mathbf{A_3}$, $\mathbf{A_4}$ и $\mathbf{C_4}$ не использовались обоими шариками.

Таким образом (как и в случае с необратимым сумматором), число 0110 после действия второго шарика также будет преобразовано в промежуточное число 1000 и тем самым будет также получен окончательный результат суммирования, так как больше шариков нет (изначально было только 2 шарика).

На этом работа данного сумматора в виде аналогового механического устройства завершена. Результат суммирования необходимо также прочитать (определить, измерить) на механическом регистре, содержащем заслонки типа **В**, что и будет соответствовать конечному результату суммирования, т.е. двоичному числу 1000 или десятичному числу 8.

Представленный сумматор на рис. 1.40 является уже обратимым, в отличие от сумматора на рис. 1.41, который необратимый. Состояния заслонок типа **А** и **С** как бы запоминают состояние канала, по которому двигался шарик. После прохождения шарика они помнят, что здесь двигался шарик, так как их состояние изменилось (а изменить их состояние мог только именно шарик). Заслонки $\mathbf{A_1}$, $\mathbf{A_2}$, $\mathbf{A_3}$, $\mathbf{A_4}$, изменяя свои состояния, фиксируют наличие шарика во входном канале (прохождение шарика по входному каналу). После того как шарик прошел по каналу и покинул устройство по состоянию заслонок типа **А**, и по наличию еще оставшихся шариков на входе устройства можно однозначно восстановить двоичное число, которое необходимо прибавить к числу из регистра сумматора. Даже после того как все шарики покинут устройство, по состоянию только заслонок типа **А** можно однозначно восстановить второе слагаемое. Заслонки $\mathbf{C_1}$, $\mathbf{C_2}$, $\mathbf{C_3}$, $\mathbf{C_4}$, изменяя свои состояния, фиксируют наличие шарика в нижнем канале выхода для бита переноса (прохождение шарика по этому каналу). После

того как шарик прошел по каналу и покинул устройство, состояние соответствующей заслонки типа **C** фиксирует наличие или отсутствие бита переноса.

Поэтому этот сумматор обратим. Действительно, если заставить двигаться шарики в обратном направлении по каналу из тех мест, откуда они вылетели (т.е. были сброшены), то конечное состояние такого сумматора после прохождения шариков будет совпадать с его начальным состоянием. Так, если перевернуть относительно горизонтальной оси усложненный вариант сумматора (см. рис. 1.40**в**) и последовательно "запустить" эти два шарика после попадания их в канал для сброса, то в этом случае конечное состояние этого механического сумматора уже будет совпадать с его начальным состоянием.

ОТМЕТИМ [**26**]. Представленная схема (см. рис. 1.40) механического сумматора может легко быть обобщена на заданное число ***m*** двоичных разрядов. Для этого необходимо объединить подходящее число логических вентилей **V** до заданной размерности ***m*** разрядных двоичных чисел с учетом подходящей длины канала, числа и места расположений заслонок типа **A** и **C**, а также с учетом подходящего числа шариков (можно использовать только один шарик, вылавливая его в месте сброса и запуская повторно в соответствующий канал столько раз, сколько единиц в записи числа).

Функционирование обратимого механического сумматора (см. рис. 1.40) можно описать *логической схемой* (рис. 1.42) в виде *сети* логических элементов и связей между ними. Такая сеть показывает развитие во времени состояний классических **битов** механического процессора, реализующего функцию классического, механического двоичного сумматора на шариках. Заметим, это пока еще не квантовое вычислительное устройство. Каждая горизонтальная линия соответствует состоянию классического бита (двоичного разряда механического сумматора). Складываются двоичные разряды (двух двоичных чисел), представленные заслонками $\mathbf{A_1}$, $\mathbf{A_2}$, $\mathbf{A_3}$, $\mathbf{A_4}$ и $\mathbf{B_1}$, $\mathbf{B_2}$, $\mathbf{B_3}$, $\mathbf{B_4}$ с учетом возможных битов переноса $\mathbf{C_1}$, $\mathbf{C_2}$, $\mathbf{C_3}$, $\mathbf{C_4}$ в следующие разряды (см. рис. 1.42).

Поразрядно суммирующие блоки (т.е. одноразрядные сумматоры) реализуют операцию (на рис. 1.42 элементы этих блоков для

полусумматоров **HS** (half-sum) обведены сплошной прямоугольной рамкой, а для полных сумматоров **FS** (full-sum), обозначенных как **SM**, обведены пунктирной прямоугольной рамкой), которую может выполнять шарик (см. рис. 1.40), попадающий на заслонки типа **B**.

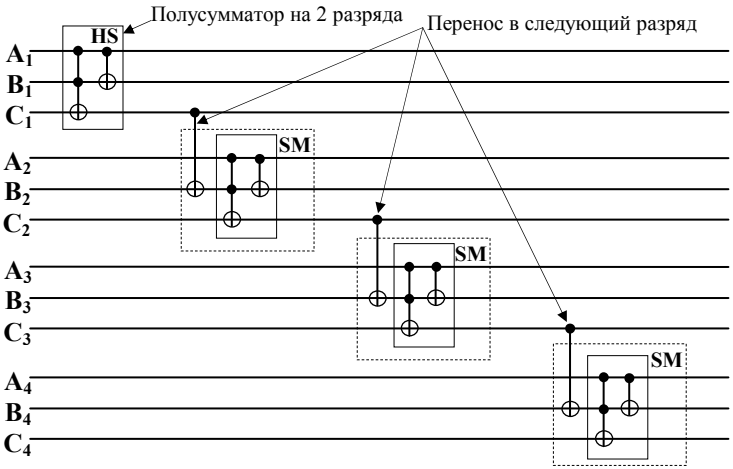


Рис. **1.42.** Логическая схема обратимого 4-разрядного, классического, механического сумматора на шариках [**26**]

Заслонка типа **B** (см. рис. 1.40) изменяет свое состояние (положение), если в *подводящем канале* находится шарик. Причем, если заслонка типа **B** до взаимодействия с шариком была в **λ**–состоянии (т.е. была установлена в 1), то шарик переходит в нижний *отводящий канал*, необходимый для реализации бита переноса в следующий разряд, при этом шарик изменяет состояние заслонки типа **C** (т.е. меняет ее положение).

Блоки переноса (см. рис. 1.42), реализующие при необходимости бит переноса в следующий разряд, выполняют операцию ***контролируемого НЕ*** путем изменения состояния заслонки $\mathbf{B}_{i+1}$ шариком, попавшим на вход суммирующего вентиля $\mathbf{V}_{i+1}$ из канала бита переноса $\mathbf{C}_i$.

Заметим [**26**, с.519], что заслонки типа **A** и **C** являются аналогами операции *отрицания* **НЕ**, заслонки типа **B** — аналогами операции ***условное НЕ***.

Теперь осталось совсем немного, чтобы перейти от механических вычислителей к квантовым вычислителям. Для этого необходимо сделать следующее:

- заменить механические системы представления *битов* квантовыми системами, представляющими *кубиты*, и использовать тем самым *квантовые состояния* систем вместо *классических состояний* для реализации обратимых вычислений, т.е. в случае с механическим сумматором надо заменить механический *регистр*, состоящий из механических *триггеров*, на *квантовый регистр*, состоящий уже из квантовых *триггеров* (т.е. так называемых **кубитов**);
- заменить классические (механические, электрические или др.) логические элементы на квантовые логические вентили (гейты);
- заменить классическое представление связей (электрические провода, механические желоба, каналы и т.п. представление) между логическими элементами на квантовое представление таких связей в виде линий, соответствующих состоянию кубитов и направлению движения времени слева направо (или частице [**17**, с.45]), т.е. последовательности состояния кубитов в разные моменты времени.

Выполнив описанную выше замену, классический вычислитель будет представлен квантовым вычислителем (для этого надо вместо механических заслонок иметь в устройстве двухуровневые квантовые системы, взаимодействия между которыми соответствуют необходимым унитарным преобразованиям).

ВАЖНО. В случае *квантового вычислителя* схема, представленная на рис. 1.42 (без пунктирных рамок и обозначений **HS** и **SM**), соответствует схеме квантовых вычислений при условии, что элемент CNOT является квантовым объектом (элементом).

ВАЖНО. Рассматриваемый аналоговый механический вычислитель (сумматор) требуется изначально приготовить (т.е. подготовить шарики и заслонки). Первый регистр приготовляется путем записи в него первого слагаемого. После действия шариков состояние этого первого регистра может измениться, и, главное, будет содержать (с учетом возможного последнего бита переноса)

конечный результат вычислений. Шарики как-то действуют (в соответствии с законами классической физики) на механический *регистр*, состоящий из механических *триггеров* (заслонки **В**), и переводят эти механические *триггеры* из одного физического состояния в другое. Этот вычислитель является обратимым. Далее мы увидим, что *квантовый вычислитель* обладает похожими свойствами — он обратим, *квантовый регистр* также надо изначально приготовить, а конечный результат будет также содержаться в этом квантовом регистре. Чтобы выполнить квантовые вычисления, надо также как-то подействовать (например, с помощью **гейтов**) на содержимое квантовых *триггеров* (так называемых **кубитов**), составляющих основу квантового *регистра*.

> «От подобной обратимой логической сети состояний битов до понятия квантового процессора — один шаг. И сделан он был в восьмидесятые годы Р. Фейнманом, который осознал, что вместо классических состояний битов для построения обратимых сетей для вычислений можно использовать состояния квантовых систем как объектов, подчиняющихся обратимой гамильтоновой динамике. Это время можно считать началом истории развития квантовых компьютеров.» [**26**, с.517]

Выводы (резюме) по разделу 1.3

1. **Аналоговая вычислительная машина** (АВМ) — машина, оперирующая информацией, представленной в виде непрерывных изменений некоторых физических величин.
2. **Гибридная вычислительная машина** (ГВМ) — машина, оперирующая информацией, представленной в виде непрерывных изменений некоторых физических величин.
3. На практике в электронных компонентах АВМ возникают различные шумы, приводящие к потере точности проводимых вычислений. Специалисты полагают, что в отличие от аналоговых вычислений квантовые вычисления в принципе

допускают наличие конечного уровня шума, сохраняя свои вычислительные достоинства.

4. Именно то, что *квантовый вычислитель* (КВ) есть ГВМ, позволило КВ вобрать в себя лучшие свойства как ЦВМ (это возможность применить помехоустойчивое кодирование с целью исправления возникающих ошибок, что не доступно АВМ), так и АВМ (это огромное быстродействие, что пока не могут обеспечить современные ЦВМ).
5. В основе *квантового вычислителя* лежит квантовый процессор. *Квантовый вычислитель* обладает похожими свойствами не только, как и ЦВМ — одна информация представлена дискретно в виде отдельных (дискретных) **кубитов**, но и как в АВМ — другая информация представлена непрерывно в виде **непрерывных амплитуд вероятностей**. В некотором смысле можно (с осторожностью) полагать, что *квантовый вычислитель* — это и есть современная ГВМ.
6. Функционирование обратимого механического сумматора можно описать *логической схемой* в виде *сети* логических элементов и связей между ними. Такая сеть показывает развитие во времени состояний классических **битов** механического процессора, реализующего функцию классического, механического двоичного сумматора на шариках. Заметим, это пока еще не квантовое вычислительное устройство.
7. В случае *квантового вычислителя* схема, представленная на рис. 1.22 (без пунктирных рамок и обозначений **HS** и **SM**), соответствует схеме квантовых вычислений при условии, что элемент CNOT является квантовым объектом (элементом).
8. Рассматриваемый аналоговый механический вычислитель (сумматор) требуется изначально приготовить (т.е. подготовить шарики и заслонки). После действия шариков состояние первого регистра может измениться, и, главное, будет содержать (с учетом возможного последнего бита переноса) конечный результат вычислений. Шарики как-то действуют (в соответствии с законами классической физики) на механический *регистр*, состоящий из механических *триггеров*, и переводят эти механические *триггеры* из од-

ного физического состояния в другое. Этот вычислитель является обратимым.

9. *Квантовый вычислитель* обладает похожими свойствами — он обратим, *квантовый регистр* также надо изначально приготовить, а конечный результат будет также содержаться в этом квантовом регистре. Чтобы выполнить квантовые вычисления, надо также как-то подействовать (например, с помощью **гейтов**) на содержимое квантовых *триггеров* (так называемых **кубитов**), составляющих основу квантового *регистра*.
10. Теперь осталось совсем немного, чтобы перейти от механических вычислителей к квантовым вычислителям. Для этого, например, с механическим сумматором необходимо сделать следующее:

    - заменить механические системы представления *битов* квантовыми системами, представляющими *кубиты*, и использовать тем самым *квантовые состояния* систем вместо *классических состояний* для реализации обратимых вычислений, т.е. в случае с механическим сумматором надо заменить механический *регистр*, состоящий из механических *триггеров*, на *квантовый регистр*, состоящий уже из квантовых *триггеров* (т.е. так называемых **кубитов**);
    - заменить классические (механические, электрические или др.) логические элементы на квантовые логические вентили (гейты);
    - заменить классическое представление связей (электрические провода, механические желоба, каналы и т.п. представление) между логическими элементами на квантовое представление таких связей в виде линий, соответствующих состоянию кубитов, и направлению движения времени слева направо (или частице), т.е. последовательности состояния кубитов в разные моменты времени.

1.4. Вероятность события и диаграммная техника

«… истинной логикой для этого мира является исчисление вероятностей, занимающееся нахождением величин вероятностей, которые учитывает или должен учитывать любой здравомыслящий человек.»

Дж. Максвелл [**35**, с. 23]

Содержание

Основы теории вероятностей (ТВ). Принцип практической уверенности. Принцип статистической устойчивости относительных частот. Теорема сложения и умножения вероятностей. Формула полной вероятности. Формула Бейеса. Вычисление вероятности. Диаграммная техника. Два правила. Дерево событий и *диаграмма переходов. Система. Состояние системы. Изменение состояния системы. Процесс. Траектория. Вероятностные логические элементы. Квантовый элемент Адамара. Амплитуда вероятности.*

1.4.1. Основные понятия теории вероятностей

В теории вероятностей исторически сложилось так (см. [**55**, с.18, с.90]), что в ней применяется своя терминология, которая стала уже общепринятой. В принципе, термины из этой теории можно заменить на их аналогичные понятия (общематематические термины), используемые из других разделов математики (табл. 1.24). Полагают, что если это сделать, то язык теории вероятностей стал бы менее понятен в приложениях. Аналогичное справедливо и для *математической статистики* (табл. 1.25). Согласно работе [**48**, с. 7-8] *А.Н. Колмогорова* можно сделать следующие сопоставления терминов (терминологические замечания), представленные в табл. 1.26.

Таблица 1.24. Первая группа терминов [**55**, с. 19]

Общематематический термин	Термин теории вероятностей
Множество событий	Пространство событий
Элемент	Элементарное событие
Подмножество	Событие
Длина, площадь, объем подмножества	Вероятность события
Числовая функция	Случайная величина

Таблица 1.25. Вторая группа терминов [**55**, с. 90]

Общематематический термин	Термин теории вероятностей	Термин математической статистики
Множество	Пространство элементарных событий $\boldsymbol{\Omega}$	Генеральная совокупность (**ГС**)
Подмножество	Событие	Выборка
Значение числовой функции	Значение случайной величины	Наблюдение

Таблица 1.26. Третья группа терминов [**48**, с. 7-8]

Термин теории множеств	Термин теории вероятностей
$\boldsymbol{A}$ и $\boldsymbol{B}$ не пересекаются, т.е. $\boldsymbol{A} \cap \boldsymbol{B}=\varnothing$	События $\boldsymbol{A}$ и $\boldsymbol{B}$ несовместны
$\boldsymbol{A} \cap \boldsymbol{B} \cap \ldots \cap \boldsymbol{N}=\varnothing$	События $\boldsymbol{A}$, $\boldsymbol{B}$,…, $\boldsymbol{N}$ несовместны
$\boldsymbol{A} \cap \boldsymbol{B} \cap \ldots \cap \boldsymbol{N}=\boldsymbol{X}$	Событие $\boldsymbol{X}$ заключается в одновременной реализации всех событий $\boldsymbol{A}$, $\boldsymbol{B}$,…, $\boldsymbol{N}$
$\boldsymbol{A} \cup \boldsymbol{B} \cup \ldots \cup \boldsymbol{N}=\boldsymbol{X}$	Событие $\boldsymbol{X}$ заключается в наступлении, по крайней мере, одного из событий реализации всех событий $\boldsymbol{A}$, $\boldsymbol{B}$,…, $\boldsymbol{N}$
Дополнительное множество $\bar{\boldsymbol{A}}$	Противоположное событие $\bar{\boldsymbol{A}}$, состоящее в ненаступлении события $\boldsymbol{A}$
$\boldsymbol{A}=\varnothing$	$\boldsymbol{A}$ невозможно
$\boldsymbol{A}=\boldsymbol{\Omega}$	$\boldsymbol{A}$ должно необходимо наступить
Система $\Re$ множеств $\boldsymbol{A_1}$, …, $\boldsymbol{A_n}$ образует разложение множества $\boldsymbol{\Omega}$, если $\boldsymbol{A_1} \cup \ldots \cup \boldsymbol{A_n}=\boldsymbol{\Omega}$ (где $\boldsymbol{A_i}$ попарно не пересекаются)	*Испытание* $\Re$ заключается в том, что устанавливают, какое из событий $\boldsymbol{A_1}$, $\boldsymbol{A_2}$,…, $\boldsymbol{A_n}$ происходит; $\boldsymbol{A_1}$, $\boldsymbol{A_2}$,…, $\boldsymbol{A_n}$ называются при этом возможными исходами испытания $\Re$
$\boldsymbol{B}$ является подмножеством $\boldsymbol{A}$: $\boldsymbol{B} \subseteq \boldsymbol{A}$	Из осуществления события $\boldsymbol{B}$ с необходимостью следует осуществление $\boldsymbol{A}$

ОТМЕТИМ [**42**, с. 38, 40, 41; **56**, с. 11; **57**, с. 17-18]. Из теории множеств следует, что

$A=A \cup A \cup A = A + A + A$ (объединение, сложение);

$A=A \cap A \cap A= A \cdot A \cdot A = AAA$ (пересечение, умножение);

$A=A \cup \varnothing$; $\varnothing=A \cap \varnothing$; $B - A = B \cdot \bar{A}$;

$\varnothing$ – это пустое множество, не содержащее ни одного элемента;

$\varnothing$ есть подмножество всякого множества D, т.е. $\varnothing \subset D$;

хотя $\varnothing \subset D$, тем не менее, возможно, что $\varnothing \notin D$;

$A + B=B + A$ (переместительное свойство для сложения);

$A \cdot B=B \cdot A$ (переместительное свойство для умножения);

$(A + B)+C=A+(B +C)$ (сочетательное свойство для сложения);

$(A \cdot B) \cdot C=A \cdot (B \cdot C)$ (сочетательное свойство для умножения);

$A \cdot (B +C) =A \cdot B + A \cdot C$ (распределительное свойство);

если $B \subseteq A$, *то* $A \cdot B=B$;

если $A \subset B$ *и* $B \subset A$, *то* $A=B$.

Определение 1.65

Разностью событий A и B называют [**58**, с. 8] событие C, состоящее в том, что событие A происходит, а B не происходит: $C=A - B$.

Определение 1.66

Под опытом (*экспериментом*, *испытанием*) понимается [**42**, с. 15; **58**, с. 6] некоторая воспроизводимая совокупность (комплекс) условий, в которых наблюдается то или другое явление, фиксируется тот или иной результат. Если при повторении опыта (комплекса условий) варьируется его результат (событие может произойти или не произойти), то говорят об *опыте со случайным исходом*.

ОТМЕТИМ [**42**, с. 15; **58**, с. 3]:

1). Опыт может протекать независимо от человека. Человек выступает в роли наблюдателя или фиксатора происходящего, и от него зависит только решение, что наблюдать и какие параметры фиксировать (измерять).

2). Каждое осуществление ***комплекса условий*** называют реализацией. Этот комплекс условий не определяет всех необходимых требований, при которых осуществляется событие. Включены в него лишь основные требования, а второстепенные НЕ учитываются или НЕ могут быть учтены в силу различных причин и меняются от опыта к опыту.

Определение 1.67

Случайным событием (**СС**) [**42**, с. 15] (или просто событием) называют всякий факт, который в опыте со *случайным исходом* может произойти или не произойти, и обозначают прописными (большими) буквами латинского алфавита, например $\boldsymbol{A}$.

ОТМЕТИМ [**45**, с. 16-17]. **Фундаментальные условия,** при которых определяются ***случайные события,*** **это:**

- ♦ опыт можно повторять много раз;
- ♦ исход опыта НЕпредсказуем;
- ♦ относительная частота **случайного** события у с т о й ч и в а (при увеличении числа опытов она устойчиво колеблется около определенного значения – это определение не очень точно).

Определение 1.68

Чтобы (см. и ср. [**42**, с. 16-18]) сравнить между собой СС (в результате опыта) по степени возможности, **надо** связать с каждым из них какое-то ***число***, которое тем больше, чем **более возможно** событие. Это число $\boldsymbol{P}$ и будем называть **вероятностью** события $\boldsymbol{A}$ и обозначать как $P(\boldsymbol{A})$.

ОТМЕТИМ: Согласно аксиомам ТВ и следствиям из них:

$$P(\boldsymbol{\Omega})\equiv 1,\ P(\varnothing)\equiv 0, \text{ а также } P(\varnothing)\le P(\boldsymbol{A})\le P(\boldsymbol{\Omega}).$$

ВАЖНО ПОМНИТЬ. Есть ДВА подхода [**58**, с. 6] к вычислению вероятности СС, основанные на априорной (классической на базе симметрии опыта и равновозможности) и эмпирической (статистической на базе многократного повторения опыта) вероятности.

Определение 1.69

Достоверное событие (**Ω**) [**42**, с. 17, 42; **45**, с. 17] — это событие (например, $\boldsymbol{B}$ и часто обозначаемое как **Ω**), которое обязательно произойдет, причем вероятность его наступления равна ЕДИНИЦЕ, т.е. $P(\boldsymbol{B})\equiv 1$ или $P(\boldsymbol{\Omega})\equiv 1$.

ОТМЕТИМ. Если $P(\boldsymbol{A})=\mathbf{1}$, то это еще не означает, что событие $\boldsymbol{A}$ является *достоверным* событием:

например, если $\boldsymbol{A}$ – событие, состоящее в попадании в точку из интервала (0;4), то $P(\boldsymbol{A})=0$, но $P(\bar{\boldsymbol{A}})=1$, так как $P(\boldsymbol{A})+P(\bar{\boldsymbol{A}})\equiv 1$ и $\bar{\boldsymbol{A}}$ есть **НЕдостоверное** событие, хотя $P(\bar{\boldsymbol{A}})=1$ [**42**, с. 91].

Определение 1.70

НЕвозможное событие ($\varnothing$) [**42**, с. 17, 42; **45**, с. 17] — это событие (например $\boldsymbol{A}$), которое никогда НЕ произойдет, причем вероятность его наступления равна НУЛЮ, т.е. $P(\boldsymbol{A})\equiv 0$ или $P(\varnothing)\equiv 0$.

ОТМЕТИМ. Если $P(\boldsymbol{A})=0$, то это еще не означает, что событие $\boldsymbol{A}$ является **НЕвозможным** событием [**42**, с. 91]; если $P(\boldsymbol{A})=0$, то событие может произойти, но вероятность этого есть НУЛЬ [**45**, с. 17] (так, если $\boldsymbol{A}$ – это событие есть попадание в точку из интервала (0,1)); из $P(\boldsymbol{A})=0$ следует только то, что при неограниченном повторении опытов (т.е. увеличении объема выборки) событие $\boldsymbol{A}$ будет появляться сколь угодно редко [**42**, с. 91-92].

Определение 1.71

Практически достоверное (возможное) событие [**42**, с. 18-19] — это событие $\boldsymbol{A}$, для которого его вероятность наступления близка к единице: $P(\boldsymbol{A})\approx 1$.

Определение 1.72

Практически НЕвозможное событие [**42**, с. 18-19] — это событие $\boldsymbol{A}$, для которого его вероятность наступления близка к нулю: $P(\boldsymbol{A})\approx 0$.

ОТМЕТИМ [**42**, с. 19-20]. Самый тонкий и трудный вопрос: насколько должна быть мала вероятность события, чтобы его можно было считать **практически** НЕвозможным? Ответ на этот вопрос выходит за рамки математической теории. На практике следует подходить к решению этого вопроса отдельно в каждом конкретном случае.

***Пример* 1.19** (см. [**20**, с. 35]). Если взрыватель отказывает при выстреле с вероятностью 0.01, то при некоторых обстоятельствах еще можно мириться с этим и считать отказ взрывателя *практически невозможным событием.* А если парашют отказывает при прыжке человека с той же вероятностью 0.01, то очевидно, что нельзя считать этот отказ *практически невозможным событием*■

Определение 1.73

Противоположными событиями называют два несовместных события, образующих полную группу [**20**, с. 42].

ОТМЕТИМ. Если событие ***A*** *практически НЕвозможное*, то противоположное ему событие $\bar{A}$ есть *практически достоверное*, и наоборот [**42**, с.18]. Справедливо $P(A)+P(\bar{A}) \equiv 1$ и $A+\bar{A}$ есть *полная группа событий* (ПГС). Определение ПГС будет дано далее.

Определение 1.74

Противоположным событию ***A*** называют событие $\bar{A}$, состоящее в НЕпоявлении события ***A*** [**42**, с. 18, 43].

Определение 1.75

Равновозможные события [**42**, с. 23] — несколько событий в данном опыте называются *равновозможными*, если по условиям симметрии есть основания полагать, что ни одно из них не является объективно более возможным, чем другое.

ОТМЕТИМ. Два события ***A*** и ***B*** равновозможные, если $P(A)=P(B)$.

Определение 1.76

Случаями (или шансами) называют события, обладающие тремя свойствами: они образуют *полную группу*, *равновозможны* и *несовместны* [**20**, с. 26].

Определение 1.77

Случай (или шанс) называется *благоприятным* (или *благоприятствующим*) некоторому событию, если появление этого случая влечет за собой появление данного события [**20**, с. 26].

Определение 1.78

Схема случаев (или схема урн) [**20**, с. 26] – если какой-либо опыт по своей структуре обладает *симметрией* возможных исходов, то случаи представляют собой *исчерпывающую* систему *равновозможных* и *исключающих* друг друга исходов опыта. О таком опыте говорят, что он сводится к ***схеме случаев***.

ОТМЕТИМ [**20**, с. 27]. Если опыт сводится к схеме случаев, то вероятность события ***A*** в данном опыте можно оценить по относительной доле *благоприятных* случаев. Вероятность события ***A*** вычисляется как отношение числа *благоприятных* случаев (***m***) к общему числу случаев (***N***), т.е. имеет место классическая формула для вычисления вероятности:

$$P(A)=\frac{m}{N}.$$

Определение 1.79

Случайная величина (**СВ**) [**48**, с. 26-28] — однозначную действительную функцию $\xi=\xi(\omega)$, определенную на основном множестве Ω, называют *случайной величиной*, если при каждом выборе действительного числа x множество $\{\xi<x\}$ всех тех ω, для которых справедливо неравенство $\xi(\omega)<x$, принадлежит к системе множеств $\breve{R}$ ($\breve{R}$ – это *алгебра множеств*).

Определение 1.80

Сходимость по вероятности [**20**, с. 31] — говорят, что случайная величина X_n *сходится по вероятности* к величине a, если при сколь угодно малом ε вероятность неравенства $|X_n - a|<\varepsilon$ с увеличением n неограниченно приближается к единице:

$$\lim_{n\to\infty} P\left[\left|X_n - a\right| < \varepsilon\right] = 1.$$

ОТМЕТИМ [**20**, с. 31]. Применяя этот термин, можно сказать, что при увеличении числа опытов частота события не *стремится* к вероятности события, а *сходится к ней по вероятности.*

Определение 1.81

Полная группа событий (**ПГС**) [**42**, с. 43,45] — события $A_1, A_2,\ldots, A_n$ образуют *полную группу событий*, если событие, образованное путем всех их объединения, образует *достоверное событие* Ω: $\Omega=\bigcup_{i=1}^{n}\{A_i\}$, а $P(\Omega)\equiv 1$, т.е. (см. [**42**, с. 22-23]) в результате опыта неизбежно должно появиться ***хотя бы одно из них,*** т.е. *одно* или *больше* событий (ср. с определением из [**56**, с. 13; **50**, с. 400]).

ОТМЕТИМ. В разных источниках дается разное определение ПГС (например, требуется НЕ ***хотя бы одно из них*** [**20**, с. 25; **42**, с. 22-23], а ***одно и только одно событие*** [**45**, с. 11]). Если (см. [**42**, с. 23]) события образуют *полную группу событий*, то опыт НЕ может кончиться помимо них! Если (см. [**42**, с. 23]) к *полной группе событий* добавить еще какие-то события, любые исходы опыта, то от этого свойство *полноты группы событий* не утрачивается!

ВАЖНО ПОМНИТЬ (см. [**42**, с. 22-23]). Специалисты обращают внимание на то, что в ПГС могут быть *совместные* события, не исключающие друг друга.

Определение 1.82

Полная группа попарно несовместных событий (**ПГПНС**) [**58**, с. 9; **61**, с. 66] — если события $\boldsymbol{H_1}$, $\boldsymbol{H_2}$,…, $\boldsymbol{H_n}$, образующие ПГС, попарно несовместны, т.е. $\boldsymbol{H_i \cap H_j = \varnothing}$ при любых $\boldsymbol{i \neq j}$, то говорят, что они образуют *полную группу попарно несовместных событий*.

***Пример* 1.20** [**34**, с. 75]. В АСОИУ, содержащей только 4 блока памяти (2 блока ОЗУ и 2 блока жестких дисков), случайно отказали 2 каких-то блока памяти из 4. Здесь ПГС (два события):

$$\text{ПГС} = \{\boldsymbol{A}, \boldsymbol{B}\};$$

где

$\boldsymbol{A}$={*блоки однотипные*};

$\boldsymbol{B}$={*блоки разнотипные*}.

Добавим к ПГС еще одно событие: $\boldsymbol{C}$={*два блока ОЗУ*}. Группа из трех событий: {$\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$} является ПГС, так как обязательно наступит одно из них, либо $\boldsymbol{A}$, либо $\boldsymbol{B}$, а в случае, когда наступит событие $\boldsymbol{C}$, одновременно с ним наступит и событие $\boldsymbol{A}$ ■

***Пример* 1.21** (см. и ср. [**56**, с. 19]). Показать, что события $A, B-A$ и $\overline{A+B}$ образуют полную группу событий и попарно несовместны.

Решение

1). Проверим попарную несовместимость, т.е. надо показать, что:

$A \cdot (B - A) = \varnothing$; $A \cdot \left(\overline{A + B}\right) = \varnothing$; $(B - A) \cdot \left(\overline{A + B}\right) = \varnothing$ ·

Действительно очевидно, что $A \cdot (B - A) = \varnothing.$ Далее, с одной стороны, если $\omega \in A$, то $\omega \in (A + B)$ и $\omega \notin \left(\overline{A + B}\right)$, а значит $A \cdot \left(\overline{A + B}\right) = \varnothing$. С другой стороны, если $\omega \in (B - A)$, то $\omega \in (A + B)$ и $\omega \notin \left(\overline{A + B}\right)$, а значит $(B - A) \cdot \left(\overline{A + B}\right) = \varnothing$.

2). Проверим, что эти три события образуют ПГС:

Действительно, так как $\boldsymbol{\Omega} = (A + B) + \overline{A + B}$ и $A + B = A + (B - A)$, то

$\boldsymbol{\Omega} = A + (B - A) + \left(\overline{A + B}\right)$, а значит, эти события образуют ПГС ■

ОТМЕТИМ. Событие ω — это элементарное событие [**56**, с. 9].

Пространство Ω элементарных событий (см. [**42**; **43**; **48**; **50**])

В теории вероятностей используют понятие пространства **Ω** *элементарных событий*.

Для этого все возможное множество исходов некоторого **опыта** представляют в виде *элементарных событий* так, чтобы все они были ***НЕсовместными*** событиями и при этом составляли *полную группу событий* (т.е. $P(\mathbf{\Omega})\equiv 1$).

Определение 1.83

Элементарное событие (**ЭС**) [**50**, с. 816] — исходное понятие. В определении вероятностного пространства непустое множество **Ω** называется *пространством элементарных событий*, а его любая точка $\omega \in \mathbf{\Omega}$ называется *элементарным событием*.

ВАЖНО ПОМНИТЬ (см. [**35**, с.16]). Каждый неразложимый исход эксперимента (опыта) представляется одним и только одним элементарным событием. Набор (т.е. множество или совокупность) всех **ЭС** в теории вероятностей принято называть пространством *элементарных событий*

ОТМЕТИМ (см. [**50**, с. 816]). При неформальном подходе множество **Ω** описывает множество всех исходов некоторого случайного эксперимента и ω соответствует элементарному исходу (эксперимент заканчивается **одним** и **только одним** элементарным исходом; эти исходы **неразложимы** и **взаимно исключают** друг друга).

ОТМЕТИМ (см. [**56**, с. 8-9]). При неформальном подходе исход испытания называется событием. Все те события, что могут произойти в результате выполнения комплекса условий, составляют *достоверное событие* **Ω**. Те из событий, что **нельзя разложить** на составляющие их события, называются *элементарными событиями*.

ОТМЕТИМ (см. [**56**, с. 8-9]). Любое событие ***B*** из *пространства элементарных событий* **Ω** **можно составить** из *элементарных событий*.

ОТМЕТИМ (см. [**11**, с. 19]). Каждый **неразложимый** исход (идеализированного) опыта представляется одним и только одним ЭС.

Совокупность всех ЭС называют *пространством* ЭС, а сами ЭС называют **точками** этого пространства. Все события, связанные с данным опытом, могут быть описаны с помощью ЭС.

ОТМЕТИМ. Использование показателя $P(\mathbf{\Omega})$ для оценки эффективности технической системы (например, АФИПС) бессмысленно, так как **всегда** $P(\mathbf{\Omega})\equiv 1$**.** Поэтому (на практике) множество $\mathbf{\Omega}$ разбивают иногда на два (или несколько) НЕпересекающихся множества элементарных событий E_1 и E_2, т.е. $E_1 \cap E_2 \equiv \varnothing$ и $E_1 \cup E_2 \equiv \mathbf{\Omega}$. Тогда можно принять, что:

$P(E_1)$ — это вероятность правильного ответа АФИПС;

$P(E_2)$ — это вероятность НЕправильного ответа АФИПС.

Например, подпространству (множеству событий) E_1 соответствуют события правильного ответа АФИПС на запрос, подпространству (множеству событий) E_2 соответствуют события НЕправильного ответа АФИПС на запрос.

ОТМЕТИМ. $P(E_1)+P(E_2)\equiv 1$. Способ объединения событий в E_1 и E_2 зависит от конкретной практической задачи и цели, для достижения которой строится АФИПС. Так, в одном случае одно событие может быть отнесено в E_1 а, в другом случае — в E_2.

***Пример* 1.22** [**34**, с. 77]. Если в АФИПС нет требуемой информации, то в одном случае НЕвыдача ее в ответ на запрос может быть правильным ответом (ее там нет и, естественно, ее нет и в ответе АФИПС), а в другом случае это может быть НЕправильный ответ (то, что в системе нет нужной информации — плохо, так как она должна быть там, раз ее запрашивают) ■

ОТМЕТИМ. Иногда вводят E_3 — третье множество событий: E_1, E_2 и E_3, т.е. $E_1 \cap E_2 \equiv \varnothing$, $E_1 \cap E_3 \equiv \varnothing$, $E_2 \cap E_3 \equiv \varnothing$ и $E_1 \cup E_2 \cup E_3 \equiv \mathbf{\Omega}$. События из E_3 соответствуют случаям *отказа от принятия решения* АФИПС (в теории распознавания образов это аналог зоны **НПВ –** *Не Представляется Возможным* принять решение), когда АФИПС НЕ может по какой-то причине выдать пользователю ответ на его запрос. Например, АФИПС иногда выгоднее не отвечать, чем давать сомнительный ответ.

***Пример* 1.23** (см. и ср. [**57**, с. 106-107])

Рассмотрим эксперимент $\boldsymbol{X}$ с бросанием монеты, при котором происходит только выпадение *герба* или *решетки*. Пусть

$\boldsymbol{H}$ **–** выпадение *герба*;

$\boldsymbol{T}$ **–** выпадение *решетки*;

тогда

$$\Omega_X = \{\boldsymbol{H}, \boldsymbol{T}\}.$$

Рассмотрим эксперимент $\boldsymbol{Y}$ с бросанием монеты, при котором происходит только выпадение *герба*, *решетки*, или монета может встать на *ребро*. Пусть

$\boldsymbol{H}$ **–** выпадение *герба*;

$\boldsymbol{T}$ **–** выпадение *решетки*;

$\boldsymbol{R}$ **–** монета встала на *ребро*;

тогда

$$\Omega_Y = \{\boldsymbol{H}, \boldsymbol{T}, \boldsymbol{R}\}.$$

Рассмотрим эксперимент $\boldsymbol{Z}$ с бросанием монеты, при котором происходит только выпадение *герба*, *решетки*, монета может встать на *ребро* или зависнуть в *воздухе*. Пусть

$\boldsymbol{H}$ **–** выпадение *герба*;

$\boldsymbol{T}$ **–** выпадение *решетки*;

$\boldsymbol{R}$ **–** монета встала на *ребро*;

$\boldsymbol{V}$ **–** монета зависла в *воздухе*;

тогда

$$\Omega_Z = \{\boldsymbol{H}, \boldsymbol{T}, \boldsymbol{R}, \boldsymbol{V}\}\blacksquare$$

ВАЖНО ПОМНИТЬ. Специалисты обращают внимание на то (см. [**57**, с. 106-107]), что пространство исходов (т.е. ЭС) эксперимента не всегда *очевидно* и *однозначно*. Может существовать целый набор таких пространств. На практике окончательный выбор пространства исходов (т.е. ЭС) эксперимента зависит от человека (т.е. экспериментатора).

ОТМЕТИМ (см. [**57**, с. 107]). Необходимо следить за тем, чтобы все практически осуществимые исходы (т.е. ЭС) эксперимента были включены в пространство исходов (ЭС) исследуемой **модели**.

ВАЖНО ПОМНИТЬ (см. [**57**, с. 107]). Выводы и прогнозы, полученные по модели, для которой ошибочно сформулировано пространство исходов, могут оказаться на практике ложными.

Пусть (см. работу [**46**, с. 17]) в результате осуществления однородных условий произведены $\boldsymbol{m}$ серий опытов (в каждой серии опытов было $\boldsymbol{N_i}$ однородных испытаний, в которых наблюдалось случайное событие $\boldsymbol{A}$ (т.е. фиксировалось, произошло или нет это событие $\boldsymbol{A}$). Среди $\boldsymbol{N_i}$ испытаний событие $\boldsymbol{A}$ происходило $\boldsymbol{N_i(A)}$ раз, а $\boldsymbol{N_i(\bar{A})}=\{\boldsymbol{N_i}-\boldsymbol{N_i(A)}\}$ раз это событие не происходило. При больших значениях $\boldsymbol{N_i}$ *относительные частоты* $\boldsymbol{N_i(A)/N_i}$ обладают *статистической устойчивостью* в том смысле, что имеют место следующие приближенные равенства:

$$\frac{N_1(A)}{N_1} \approx \frac{N_2(A)}{N_2} \approx \frac{N_3(A)}{N_3} \approx \cdots \approx \frac{N_m(A)}{N_m} \approx P(A),$$

где $\boldsymbol{P(A)}$ мы называем *вероятностью события* $\boldsymbol{A}$, причем на ПРАКТИКЕ эта вероятность события $\boldsymbol{A}$ может быть очень МАЛА (близка к **0**), и поэтому его можно считать *практически невозможным*. Тогда могут быть сформулированы ДВА основных принципа (см. работу *А.Н. Колмогорова* [**46**, с.4] и работы [**42**, с.19; **46**, с.18]), лежащих в основе практических вычислений.

Принцип практической уверенности (см. работы [**42**, с. 19; **46**, с.18; **51**, с. 224; **48**, с. 5-7])

В основе применяемых на ПРАКТИКЕ **всех** *выводов* и *рекомендаций* (получаемых с помощью теории вероятностей) лежит так называемый следующий *принцип практической уверенности* [**42**, с. 19]:

> *Если вероятность события* $\boldsymbol{A}$ *в данном опыте весьма мала, то (при однократном выполнении опыта) можно вести себя так, как будто событие* $\boldsymbol{A}$ *вообще невозможно, т.е. не рассчитывать на его появление.*

Принцип статистической устойчивости относительных частот

Многовековая практика убедительно показала, что для *массовых случайных событий* может быть сформулирован следующий *принцип статистической устойчивости относительных частот* [**46**, с. 18]:

> *В длинных сериях однородных испытаний относительные частоты случайного события* $\boldsymbol{A}$ *колеблются около некоторого числа* $P(\boldsymbol{A})$, *которое мы называем вероятностью события* $\boldsymbol{A}$.

Несовместность и независимость событий

Пусть события ***A*** и ***H*** принадлежат пространству *элементарных событий* **Ω**, причем $P(\boldsymbol{H})>0$.

Определение 1.84

Уловная вероятность события [**20**, с. 46] — вероятность события ***A***, вычисленная при условии, что имело место другое событие ***H***, называется *условной вероятностью события* ***A*** и обозначается $P(\boldsymbol{A}|\boldsymbol{H})$.

ОТМЕТИМ (см. [**53**, с. 443]). Иногда используют другой символ в обозначении *условной вероятности события* ***A*** — $P(\boldsymbol{A/H})$. Далее мы будем использовать только обозначение — $P(\boldsymbol{A}|\boldsymbol{H})$.

ОТМЕТИМ (см. [**55**, с. 53-54]). $P(\boldsymbol{A}|\boldsymbol{H})$ называется *условной вероятностью события* ***A*** при условии ***H*** (при гипотезе ***H***) и вычисляется по следующей формуле:

$$P(A\,|\,H)=\frac{P(A\cap H)}{P(H)}.$$

ОТМЕТИМ [**57**, с. 124]. Если $P(\boldsymbol{H})=0$, то *условная вероятность события* ***A*** при условии ***H*** не определена.

Определение 1.85

Несовместные **события** [**20**, с. 26] — несколько событий называются *несовместными* в данном опыте, если никакие два из них не могут появиться вместе.

Определение 1.86

Зависимые события [**20**, с. 46] — событие ***A*** называется *зависимым от события* ***B***, если вероятность события ***A*** меняется в зависимости от того, произошло событие ***B*** или нет, т.е. (см. [**42**, с. 53]) $P(\boldsymbol{A}|\boldsymbol{B})\neq P(\boldsymbol{A})$.

Определение 1.87

Независимые события (см. и ср. [**20**, с. 45; **57**, с. 124]) — событие ***A*** называется *стохастически* НЕ*зависимым от события* ***B*** (или просто *независимым*), если вероятность события ***A*** НЕ зависит от того, произошло событие ***B*** или нет, т.е. (см. [**42**, с.53]) $P(\boldsymbol{A}|\boldsymbol{B})=P(\boldsymbol{A})$.

ОТМЕТИМ [**57**, с. 124]. Можно показать, если ***A*** независимо от ***B,*** то и ***B*** независимо от ***A***.

Определение 1.88

Независимые события [**20**, с. 48] — два события называются НЕ*зависимыми*, если появление одного из них НЕ изменяет вероятности появления другого; несколько событий называются НЕ*зависимыми*, если любое из них НЕ зависит от любой совокупности остальных.

ОТМЕТИМ (см. [**42**, с. 55-56]). Если имеется несколько событий $\boldsymbol{H_1}$, $\boldsymbol{H_2}$,..., $\boldsymbol{H_n}$, то их попарная независимость (т.е. независимость любых двух событий $\boldsymbol{H_i}$ и $\boldsymbol{H_j}$ с разными индексами) еще не означает их *независимости в совокупности.*

ВАЖНО ПОМНИТЬ (см. [**42**, с. 56]). На практике в основе *независимости* событий лежит их *физическая независимость*, сводящаяся к тому, что множества случайных факторов, приводящих к тому или другому исходу опыта, не пересекаются (или почти не пересекаются).

Рассмотрим некоторые важные случаи (см. [**55**, с. 54-57]):

1) если (рис. 1.43) $\boldsymbol{A}\cap\boldsymbol{H}=\varnothing$, то $P(\boldsymbol{A}|\boldsymbol{H})=0$ (т.е. *несовместные* события $\boldsymbol{A}$ и $\boldsymbol{H}$); если произошло событие $\boldsymbol{A}$, то событие $\boldsymbol{H}$ произойти не может;
2) если (рис. 1.44) $\boldsymbol{H}\subset\boldsymbol{A}$, то $\boldsymbol{A}\cap\boldsymbol{H}=\boldsymbol{H}$ и $P(\boldsymbol{A}|\boldsymbol{H})=1$ (т.е. событие $\boldsymbol{A}$ является *следствием* события $\boldsymbol{H}$); если произошло событие $\boldsymbol{H}$, то заведомо произошло и событие $\boldsymbol{A}$;
3) если (рис. 1.45) $\boldsymbol{A}\cap\boldsymbol{H}\neq\varnothing$ и $\boldsymbol{A}\cap\boldsymbol{H}\neq\boldsymbol{H}$ ($\boldsymbol{A}\cap\boldsymbol{H}\neq\boldsymbol{A}$), то $0<P(\boldsymbol{A}|\boldsymbol{H})<1$;
4) если события $\boldsymbol{A}$ и $\boldsymbol{H}$ *независимы*, то $P(\boldsymbol{A}\cap\boldsymbol{H})=P(\boldsymbol{A})P(\boldsymbol{H})$ и $P(\boldsymbol{A}|\boldsymbol{H})=P(\boldsymbol{A})$.

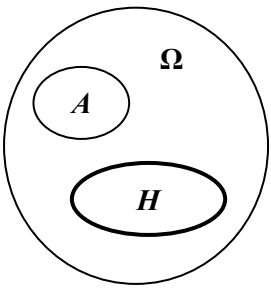


Рис. 1.43. Случай 1

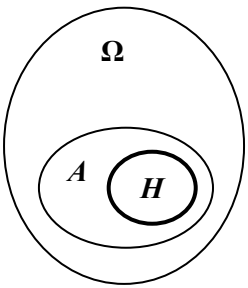


Рис. 1.44. Случай 2

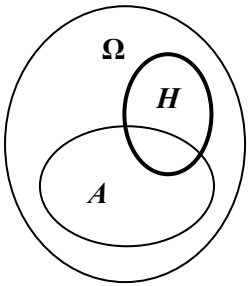


Рис. 1.45. Случай 3

***Пример* 1.24** (см. и ср. [**57**, с. 124-126])

Рассмотрим множество студентов в некоторой аудитории, причем известно следующее (рис. 1.46 и [**57**, с. 124-126]):

- общее число студентов в аудитории s=20 (множество S);
- число курящих студентов w=8 (подмножество E);
- число студентов в очках f=12 (подмножество F);
- число курящих студентов в очках u=6 (подмножество U).

На рис. 1.46 студенты условно изображены точками. Множество S показано сплошной рамкой. Подмножества E и F обведены каждый в свою пунктирную рамку. Подмножество U в рамку не обведено и состоит из 6 элементов (студентов), одновременно входящих как в E, так и в F, т.е. $U=E\cap F$.

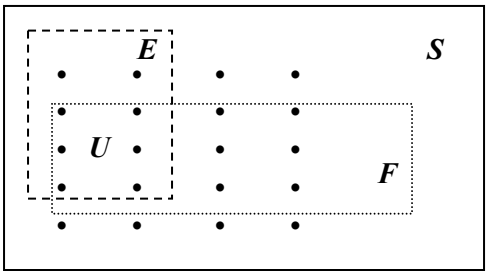


Рис. 1.46. Множество студентов

Условная вероятность. Эксперимент №1

Случайно выбираем одного из студентов, и этот студент выходит из аудитории. Предположим, что мы не знаем, курит ли этот студент и носит ли он очки. Пусть: $\tilde{E}$ — событие, что этот студент курит; $\check{Z}$ — событие, что этот студент носит очки; $\ddot{U}$ — событие, что этот студент курит и носит очки. Вопрос: *какова вероятность того, что этот студент курящий и носит очки*?

Решение

Будем полагать, что Ω_S — это множество всех *элементарных событий* эксперимента №1 и $P(\Omega_S)$=1. Тогда (см. рис. 1.46)

$$P(\tilde{E})=w/s=8/20; \quad P(\check{Z})=f/s=12/20; \quad P(\ddot{U})=u/s=6/20.$$

Эти вероятности приписываются соответствующим событиям еще до эксперимента (или опыта). Искомая вероятность есть

$$P(\ddot{U})=6/20.$$

Условная вероятность. Эксперимент №2

Случайно выбираем одного из студентов, и этот студент выходит из аудитории. Теперь предположим, что когда студент выходил, мы заметили на нем очки. ***Ü**** — событие, что этот студент курит при условии, что мы заметили на нем очки. Вопрос тот же: *какова вероятность того, что этот студент курящий и носит очки*?

Решение

Будем полагать, что $\boldsymbol{\Omega_F}$ — это множество всех *элементарных событий* эксперимента №2 и $P(\boldsymbol{\Omega_F})=1$. Таким образом, для нового уже измененного эксперимента №2 по сравнению с экспериментом №1 множество $\boldsymbol{\Omega_F}$ принято в качестве нового множества всех *элементарных событий*.

Поскольку мы заметили (т.е. получили информацию), когда студент выходил, что он был в очках, то наверняка можно утверждать, что этот студент из множества ***F*** (пока мы не знаем, курящий он или нет). Очевидно (см. [**57**, с. 125]), что такая дополнительная информация изменит условия опыта, и приписываемые событиям вероятности должны быть пересмотрены.

Поскольку известно, что выходящий студент был в очках, а во множестве ***F*** есть только 6 таких курящих студентов, то понятно, что вероятность того, что студент курит, есть

$$P(\ddot{\boldsymbol{U}}^*)=\boldsymbol{u}/\boldsymbol{f}=6/12,$$

причем это и будет условной вероятностью события $\tilde{\boldsymbol{E}}|\check{\boldsymbol{Z}}$ (сравните $P(\ddot{\boldsymbol{U}})$ и $P(\ddot{\boldsymbol{U}}^*)$ — у них разный знаменатель, т.е. разные множества всех *элементарных событий*). В итоге $P(\tilde{\boldsymbol{E}}|\check{\boldsymbol{Z}})=6/12$.

ВАЖНО ПОМНИТЬ. Новая информация заставляет исследователя (см. [**57**, с. 125-126]) изменить пространство исходов модели (т.е. множество всех *элементарных событий*), при этом надо также (см. [**57**, с. 126]) пересмотреть и вероятности, приписываемые событиям.

ВАЖНО ПОМНИТЬ. Специалисты полагают [**57**, с. 125], что вероятность, приписываемая событию, изменяется тем больше, чем больше информации получено из *случайного* эксперимента.

ОТМЕТИМ. Специалисты полагают [**59**, с. 26] (см. рис. 1.47), что условие, состоящее в том, что событие ***H*** произошло, равносильно изменению условий опыта, когда из всех *элементарных событий* **Ω** остаются только те, которые благоприятны событию ***A***, при этом

все остальные отбрасываются. Поэтому вместо пространства *элементарных событий* $\boldsymbol{\Omega}$ уже рассматривается новое пространство *элементарных событий* $\boldsymbol{\Omega_H}$, соответствующее событию $\boldsymbol{H}$. Область (на рис. 1.47 она заштрихована), соответствующая $\boldsymbol{A \cap H}$, есть благоприятная событию $\boldsymbol{A}$ при наличии события $\boldsymbol{H}$.

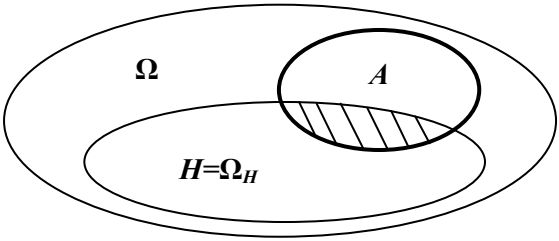


Рис. 1.47. События $\boldsymbol{A}$, $\boldsymbol{H}$ и $\boldsymbol{\Omega}$

Стохастическая независимость. Эксперимент №3

Случайно выбираем одного из студентов. Рассматриваем следующие два события:

$\tilde{\boldsymbol{E}}$={*студент курит*}, $\check{\boldsymbol{Z}}$={*студент носит очки*}.

Вопрос: *являются ли независимыми события* $\tilde{\boldsymbol{E}}$ *и* $\check{\boldsymbol{Z}}$?

Решение

С одной стороны, можно полагать, что ношение очков и курение никак не связаны друг с другом. С другой стороны, не исключено, что выкуривание большого числа сигарет может повлиять на остроту зрения у тех, кто курит. Специалисты полагают [**57**, с. 126], чтобы полностью ответить на поставленный вопрос, нужно провести полное статистическое обследование, которое включало бы проверку зрения у большого числа людей, и исследование некурящих, непостоянно и постоянно курящих людей.

Ранее мы нашли $P(\tilde{\boldsymbol{E}})=8/20$ и $P(\tilde{\boldsymbol{E}}|\check{\boldsymbol{Z}})=6/12$. Тогда из *определения 1.86* следует, что так как $P(\tilde{\boldsymbol{E}}|\check{\boldsymbol{Z}})\neq P(\tilde{\boldsymbol{E}})$, то события $\tilde{\boldsymbol{E}}$ и $\check{\boldsymbol{Z}}$ *зависимы*■

ВАЖНО ПОМНИТЬ (см. [**57**, с. 126]). Следует остерегаться обобщения вывода из последнего решения на предположение относительно уже всех студентов. Вывод о зависимости событий $\tilde{\boldsymbol{E}}$ и $\check{\boldsymbol{Z}}$ имеет место только в рамках эксперимента №3.

Теорема сложения и умножения вероятностей

Теорема сложения вероятностей несовместных событий [**44**]
Вероятность появления одного из двух несовместных событий, безразлично какого, равна сумме вероятностей этих событий:

$$P(\boldsymbol{A} + \boldsymbol{B}) = P(\boldsymbol{A}) + P(\boldsymbol{B}) \blacksquare$$

Следствие. Вероятность появления одного из нескольких попарно несовместных событий, безразлично какого, равна сумме вероятностей этих событий:

$$P(\boldsymbol{H}_1+\boldsymbol{H}_2+...+\boldsymbol{H}_n)=P(\boldsymbol{H}_1)+ P(\boldsymbol{H}_2)+\ldots+ P(\boldsymbol{H}_n) \blacksquare$$

Теорема умножения вероятностей событий [**20**, с.46-47; **44**, с.19]
Вероятность совместного появления двух событий равна произведению вероятности одного из них на условную вероятность другого, вычисленную в предположении, что первое событие уже наступило:

$$P(\boldsymbol{A} \cdot \boldsymbol{B}) = P(\boldsymbol{A}) \cdot P(\boldsymbol{B}|\boldsymbol{A})$$

или

$$P(\boldsymbol{A} \cdot \boldsymbol{B}) = P(\boldsymbol{B}) \cdot P(\boldsymbol{A}|\boldsymbol{B}) \blacksquare$$

Следствие 1. Вероятность совместного появления нескольких событий равна произведению вероятности одного из них на условные вероятности всех остальных, причем вероятность каждого последующего события вычисляется в предположении, что все предыдущие события уже наступили:

$$P(\boldsymbol{H}_1\cdot\boldsymbol{H}_2\cdot...\cdot\boldsymbol{H}_n)=P(\boldsymbol{H}_1) \cdot P(\boldsymbol{H}_2|\boldsymbol{H}_1) \cdot P(\boldsymbol{H}_3|\boldsymbol{H}_1\boldsymbol{H}_2) \cdot \ldots$$
$$\ldots\cdot\ P(\boldsymbol{H}_n) \cdot P(\boldsymbol{H}_3|\boldsymbol{H}_1\boldsymbol{H}_2\ldots\ \boldsymbol{H}_{n-1}) \blacksquare$$

Следствие 2. Для независимых в совокупности событий теорема упрощается и принимает вид:

$$P(\boldsymbol{H}_1\cdot\boldsymbol{H}_2\cdot...\cdot\boldsymbol{H}_n)=P(\boldsymbol{H}_1)\cdot P(\boldsymbol{H}_2) \cdot P(\boldsymbol{H}_3) \cdot\ldots\cdot P(\boldsymbol{H}_n) \blacksquare$$

ОТМЕТИМ. Условная вероятность $P(\boldsymbol{B}|\boldsymbol{A})$ есть (см. [**57**, с. 125]) вероятность некоторого события, которое далее (для удобства изложения) будем обозначать просто как событие $\boldsymbol{B}|\boldsymbol{A}$. Запись $\boldsymbol{A}|\boldsymbol{H}$, например, будет означать (см. и ср.[**44**, с. 36]) "*при гипотезе* $\boldsymbol{H}$ *событие* $\boldsymbol{A}$". Так, если $\boldsymbol{A}|\boldsymbol{H}$ достоверно (или иначе — *при гипотезе* $\boldsymbol{H}$ *событие* $\boldsymbol{A}$ достоверно), то соответствующая условная вероятность равна единице, т.е. $P(\boldsymbol{A}|\boldsymbol{H})=1$. Такие события, как $\boldsymbol{A}|\boldsymbol{H}$**,** будем также представлять как комбинацию других событий, например, $\boldsymbol{A}|\boldsymbol{H}=E_2\cap(E_3 \cup E_1)$ и т.п.

1.4.2. Рассматриваемый класс задач ТВ

Теория вероятностей позволяет сформулировать класс задач, связанный с применением формулы Бейеса и формулы *полной вероятности*. Этот класс задач обладает следующими характерными чертами (или особенностями):

- имеется конкретная проблема о некотором объекте, например технического характера, и требуется выяснить, в каком состоянии находится этот объект (исправна ли данная АСОИУ, правильно ли отвечает на вопросы АФИПС и т.п.);
- в этой проблеме можно выделить и сформулировать конечный набор из n гипотез (случайных событий) H_1, H_2,..., H_n об этом объекте;
- в этой проблеме можно выделить и сформулировать некоторое случайное событие A об этом объекте, причем вероятность его появления $P(A)>0$;
- известны или могут быть получены значения вероятностей $P(A)$, $P(A|H_i)$, $P(H_i)$, $P(H_i|A)$, $i=1, 2, 3,..., n$;
- процесс расчета может быть многошаговым.

Для таких задач есть смысл пытаться применять формулу Бейеса и формулу полной вероятности.

Вообще принимать решение о выборе вероятной гипотезы можно не только с использованием формул Бейеса и полной вероятности. Главное, надо как-то определить вероятности гипотез и сравнить их между собой, затем выбрать наиболее вероятную гипотезу, которая и будет искомой.

ОТМЕТИМ (см. задачу №3.35 из [**59**, с. 69]). Не обязательно всегда пытаться применять формулу Бейеса. Существуют задачи, которые можно успешно решить, и не применяя эту формулу.

ВАЖНО ПОМНИТЬ. На практике не следует слепо применять полученные навыки в решении учебных задач. Жизнь намного богаче и разнообразнее, чем учебные примеры. Опыт убедительно показывает, что одно и то же решение может быть получено разными путями с применением совершенно различных средств и подходов. И тем ценнее для науки и будущей практики решение, когда оно неожиданно, красиво, оригинально и не стандартно.

1.4.3. Формулы полной вероятности и формулы Бейеса

Теорема (о полной вероятности) [**20**, с. 54; **42**, с. 69; **48**, с. 9-10]

Пусть требуется найти вероятность некоторого события A, которое может произойти (появиться) только вместе с одним из событий $H_1, H_2,..., H_n$ (называемых далее *гипотезами*), образующих полную группу попарно несовместных событий.

Известны

- все априорные вероятности $P(H_i)$ наступления гипотез H_i, где $i=1, 2, 3,..., n$ и $\sum_{i=1}^{n} P(H_i) = 1$;
- все условные вероятности $P(A|H_i)$ наступления события A при условии, что наступило событие H_i (т.е. верна гипотеза H_i), где $i=1, 2, 3,..., n$.

Тогда вероятность события $P(A)$ находят по *формуле полной вероятности* (ФПВ):

$$P(A)=\sum_{i=1}^{n}\left\{P(H_i)\cdot P(A\,|\,H_i)\right\} \blacksquare$$

ОТМЕТИМ [**42**, с. 69]. В условиях теоремы принято, что предполагается провести опыт, об условиях которого можно выдвинуть исключающие друг друга гипотезы $H_1, H_2,..., H_n$ такие, что

$$\sum_{i=1}^{n} H_i = \Omega;\ H_i \cdot H_j = \varnothing,\ \text{где } i \neq j,$$

при этом каждая из гипотез осуществляется случайным образом.

ОТМЕТИМ [**20**, с.55]. Гипотезы, для которых член $P(H_i)\cdot P(A|H_i)$ есть нуль, иногда не вводят при решении задач.

ОТМЕТИМ [**42**, с. 69-70]. Формула полной вероятности применяется специалистами тогда, когда опыт со случайным исходом как бы распадается на следующие два этапа:

на 1-м *разыгрываются* условия опыта;

на 2-м *разыгрывается* его результат.

ОТМЕТИМ. В условиях теоремы некоторый *объект* и *опыт* присутствуют не явно. Согласно [**50**, с. 472] формула *полной вероятности* верна при $n=\infty$. Во избежание недоразумений далее будем полагать, что число гипотез n конечно.

Доказательство теоремы (о полной вероятности) [**58**, с.18-19]

Пусть событие A (рис. 1.48) может произойти с одной из полной группы попарно несовместных гипотез H_1, H_2,..., H_n, причем: $A=\bigcup_{i=1}^{n}(A\cap H_i)$. Тогда на рис. 1.48 ($n$=4) под событием A понимается попадание в круг точки, случайно брошенной в прямоугольник. События H_i, i=1, 2, 4 есть события, состоящие в попадании точки в секторы. События $A\cap H_i$, i=1, 2, 4 — события, состоящие в попадании точки в малые секторы (эти секторы заштрихованы на рис. 1.48).

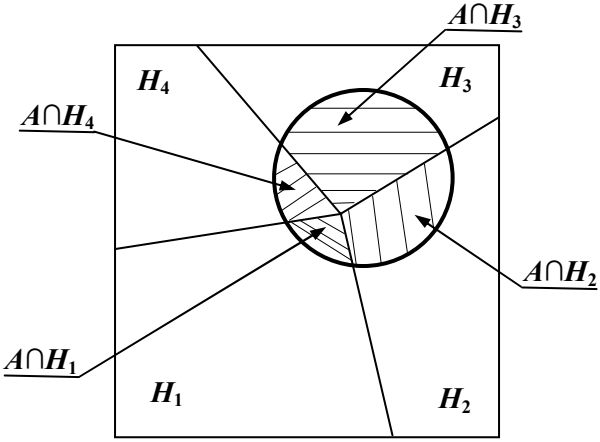


Рис. 1.48. События A, H_i и $A\cap H_i$

Поскольку события $A\cap H_i$ несовместны (это следует (см. также [**20**, с. 54]) из несовместности событий H_1, H_2,..., H_n), то можно воспользоваться теоремой сложения вероятностей и получить промежуточное выражение:

$$P(A)=\sum_{i=1}^{n}P(A\cap H_i).$$

Затем применим к событию AH_i теорему умножения вероятностей, получим другое окончательное выражение:

$$P(A)=\sum_{i=1}^{n}\{P(H_i)\cdot P(A\,|\,H_i)\}.$$

И тем самым теорема доказана ■

Теорема гипотез (формула Бейеса) [**20**, с. 56-58; **48**; **50**, с. 37]

Пусть некоторое событие A (для которого вероятность появления $P(A)>0$) наступает только при появлении одного из попарно несовместных событий H_1, H_2,..., H_n (гипотез), образующих полную группу событий ($\sum_{i=1}^{n} H_i = \Omega$; $H_i \cdot H_j = \varnothing$, где $i \neq j$).

Известны заранее до испытания (опыта или эксперимента):

- все априорные вероятности $P(H_i)$ наступления событий H_i, где $i=1, 2, 3,..., n$ и $\sum_{i=1}^{n} P(H_i) = 1$;
- все условные вероятности $P(A|H_i)$ наступления события A при условии, что наступило событие H_i (т.е. верна гипотеза H_i), где $i=1, 2, 3,..., n$.

Известно также, что в результате некоторого испытания A произошло, причем (см. [**20**, с.54; **49** с.12]): $A = \bigcup_{i=1}^{n} (A \cap H_i)$.

Тогда все вероятности гипотез (событий) могут быть пересмотрены (переоценены или переопределены) с помощью следующей *формулы Бейеса*:

$$P(H_i \mid A) = \frac{P(H_i) \cdot P(A \mid H_i)}{P(A)},$$

где вероятность события $P(A)$ находят по формуле *полной вероятности*: $P(A) = \sum_{i=1}^{n} \{P(H_i) \cdot P(A \mid H_i)\}$ ■

ОТМЕТИМ. Согласно [**50**, с. 37] эта теорема доказана *Т. Бейесом* (*T. Bayes*) и опубликована в 1763 г. Однако согласно [**60**, с. 37] *Т. Бейес* ее не доказывал, и лишь из уважения к его заслугам она носит его имя (подробнее см. [**54**, с. 39-41]).

ОТМЕТИМ. В условиях теоремы некоторый *объект* и *опыт* присутствуют не явно.

ОТМЕТИМ. Во избежание недоразумений далее будем полагать, что число гипотез n конечно.

ВАЖНО ПОМНИТЬ. На практике, прежде чем применять эти две теоремы, следует убедиться – события случайны, гипотезы несовместны и образуют полную группу событий.

Для этих двух формул нужны следующие исходные данные:

n — общее число гипотез (событий) H_1, H_2,..., H_n (рассматриваем конечное число гипотез);

H_i — сами гипотезы (их формулировки) относительно объекта, причем именно те, что *попарно несовместны* и образуют *полную группу* событий, i=1, 2, 3,..., n;

A — центральное (основное или главное) событие, которое по условию задачи наступило (его формулировка), причем вероятность его появления есть $P(A)>0$), и наступает это событие только при появлении одного из событий (гипотез) H_i, где i=1, 2, 3,..., n;

объект — тот объект, относительно которого высказываются n гипотез H_i;

опыт — опыт (эксперимент или испытание) со случайным исходом над объектом, в результате которого наступает главное событие A (т.е. среди всех событий эксперимента выделяют одно главное и обозначают символом A);

$P(H_i)$ — априорные вероятности наступления событий H_i, где i=1, 2, 3,..., n и $P(H_1)+P(H_2)\ldots+P(H_n)=1$;

$P(A|H_i)$ — условные вероятности наступления события A при условии, что верна гипотеза H_i, где i=1, 2, 3,..., n;

$P(H_i|A)$ — условные вероятности наступления события H_i, где i=1, 2, 3,..., n при условии, что наступило событие A.

Важно подчеркнуть следующее:

- обычно требуется найти именно вероятности $P(H_i|A)$ или $P(A)$;
- событие A отражает результат опыта, т.е. если событие A произошло, то достоверным стало одно из событий H_1A или H_2A или H_3A или ... H_nA, так как (см. [**49**, с. 12]): $A=\bigcup_{i=1}^{n}(A\cap H_i)$;
- под опытом понимается [**42**, с. 15; **58**, с. 6] некоторая воспроизводимая совокупность (комплекс) условий, в которых наблюдается то или другое явление, фиксируется тот или иной результат; если при повторении опыта варьируется его результат (т.е. событие может произойти или не произойти), то говорят об опыте со случайным исходом;
- объект – устройство, прибор, система “стрелок — мишень”, абстрактный объект и т.п.

Проблема получения исходных данных для решения задачи

Формула Бейеса позволяет вычислять $P(\boldsymbol{H_i}|\boldsymbol{A})$. Однако откуда берутся значения исходных данных, например,

$P(\boldsymbol{H_i})$ — априорные вероятности наступления событий $\boldsymbol{H_i}$;

$P(\boldsymbol{A})$ — вероятность центрального события;

или

$P(\boldsymbol{A}|\boldsymbol{H_i})$ — условные вероятности наступления события $\boldsymbol{A}$ при условии, что наступило событие $\boldsymbol{H_i}$

— это не предмет теории вероятностей. Эта теория только позволяет вычислять вероятности по другим исходным данным, например, по вероятностям элементарных событий, при этом (см. [**42**, с. 46]) откуда берутся сами эти вероятности элементарных событий, в этой теории не рассматривается.

На практике обычно поступают следующим образом:

- либо все исходные вероятности известны и их берут из условий задачи;
- либо неизвестные исходные вероятности вычисляют с помощью теории вероятностей по косвенным исходным данным из условий задачи;
- либо неизвестные исходные вероятности становятся известными в результате их определения по экспериментальным статистическим данным.

Формула Бейеса и ФПВ не дает ответ об $\boldsymbol{n}$ – числе гипотез $\boldsymbol{H_i}$. Это число должно быть известно исследователю, применяющему эту формулу. Практика решения задач с применением формулы Бейеса и ФПВ показала, что обычно число гипотез известно из условия задачи. Однако имеются случаи, когда число гипотез неизвестно (не задано) в условиях задачи, и исследователю надо принять решение об их числе.

На практике решение обычно принимается следующим образом:

- либо $\boldsymbol{n}$ известно и его берут из условий задачи;
- либо $\boldsymbol{n}$ неизвестно, но его можно определить по косвенным исходным данным из условий задачи;
- либо $\boldsymbol{n}$ неизвестно, но его можно задать (ввести самостоятельно) с учетом условий задачи.

1.4.4. Вычисление вероятности по формулам

Теория вероятностей позволяет решать задачи, связанные с нахождением вероятностей по известным формулам и доказанным теоремам. Рассмотрим несколько простых примеров.

***Пример* 1.25** (см. задачу №94 из [**44**, с. 32])

В первой урне содержится 10 шаров, из них 8 белых; во второй урне содержится 20 шаров, из них 4 белых. Из каждой урны наудачу извлекли по одному шару, а затем из этих двух шаров наудачу взят один шар. Найти вероятность того, что взят белый шар.

Решение [**34**, с. 118]

1). Введем ($\boldsymbol{n}$=4) гипотезы и сформулируем событие $\boldsymbol{A}$:

$\boldsymbol{H_1}$={*два белых шара*},

$\boldsymbol{H_2}$={*черный шар из 1-й урны и белый шар из 2-й урны*},

$\boldsymbol{H_3}$={*белый шар из 1-й урны и черный шар из 2-й урны*},

$\boldsymbol{H_4}$={*два черных шара*},

$\boldsymbol{A}$={*взят белый шар*}.

Априорные вероятности гипотез $P(\boldsymbol{H_i})$ практически могут быть вычислены из условия задачи:

$$P(\boldsymbol{H_1})=\frac{8}{10}\cdot\frac{4}{20}=\frac{32}{200}=\frac{4}{25};\quad P(\boldsymbol{H_2})=\frac{2}{10}\cdot\frac{4}{20}=\frac{8}{200}=\frac{1}{25};$$

$$P(\boldsymbol{H_3})=\frac{8}{10}\cdot\frac{16}{20}=\frac{128}{200}=\frac{16}{25};\quad P(\boldsymbol{H_4})=\frac{2}{10}\cdot\frac{16}{20}=\frac{32}{200}=\frac{4}{25};$$

причем $P(\boldsymbol{H_1})+P(\boldsymbol{H_2})+P(\boldsymbol{H_3})+P(\boldsymbol{H_4})=1$.

Требуется найти $P(\boldsymbol{A})$.

2). Гипотезы $\boldsymbol{H_1}$, $\boldsymbol{H_2}$, $\boldsymbol{H_3}$ и $\boldsymbol{H_4}$ попарно несовместны (всего только $\boldsymbol{n}$=4 гипотезы и иметь место может быть только одна из них) и образуют полную группу событий, так как $\boldsymbol{H_1}+\boldsymbol{H_2}+\boldsymbol{H_3}+\boldsymbol{H_4}=\boldsymbol{\Omega}$.

3). Найдем все условные вероятности $P(\boldsymbol{A}|\boldsymbol{H_i})$, а и затем $P(\boldsymbol{A})$:

$P(\boldsymbol{A}|\boldsymbol{H_1})=1$; $P(\boldsymbol{A}|\boldsymbol{H_2})=P(\boldsymbol{A}|\boldsymbol{H_3})=1/2$; $P(\boldsymbol{A}|\boldsymbol{H_4})=0$;

$$P(\boldsymbol{A})=\sum_{i=1}^{n}\left\{P\left(H_i\right)\cdot P\left(A\,|\,H_i\right)\right\}=\frac{4}{25}\cdot 1+\frac{1}{25}\cdot\frac{1}{2}+\frac{16}{25}\cdot\frac{1}{2}+\frac{4}{25}\cdot 0=\frac{25}{50}=\frac{1}{2}.$$

4). Условные вероятности $P(\boldsymbol{H_i}|\boldsymbol{A})$ вычислять не требуется.

5). И тем самым задача решена■

***Пример* 1.26** (см. [**56**, с. 20])

Инвестор вложил капитал в ценные бумаги двух финансовых фирм. При этом он надеется получить доход в течение обусловленного времени от 1-й фирмы с вероятностью 0.9; от 2-й – с вероятностью 1. Однако есть возможность банкротства фирм независимо друг от друга, которая оценивается для 1-й фирмы вероятностью $\boldsymbol{p}_1$=0.1; для 2-й — $\boldsymbol{p}_2$=0.02. В случае банкротства фирмы инвестор получает только вложенный капитал. Какова вероятность того, что инвестор получит прибыль?

Решение [**34**, с. 105]

1). Введем ($\boldsymbol{n}$=4) гипотезы, дополнительные обозначения и сформулируем событие $\boldsymbol{A}$:

$\boldsymbol{H}_1$= $E_1\cdot\bar{E}_2$={*1-я фирма банкрот, 2-я фирма не банкрот*},

$\boldsymbol{H}_2$= $\bar{E}_1\cdot E_2$={*1-я фирма не банкрот, 2-я фирма банкрот*},

$\boldsymbol{H}_3$= $E_1\cdot E_2$={*обе фирмы банкроты*},

$\boldsymbol{H}_4$= $\bar{E}_1\cdot\bar{E}_2$={*обе фирмы не банкроты*},

E_1={*банкротство 1-й фирмы*}, E_2={*банкротство 2-й фирмы*},

$\boldsymbol{A}$={*получение инвестором прибыли*}.

Вычислим все ($\boldsymbol{n}$=4) априорные вероятности гипотез:

$$P(\boldsymbol{H}_1) = \boldsymbol{p}_1(1-\boldsymbol{p}_2)=0.1\cdot 0.98=0.098;$$
$$P(\boldsymbol{H}_2) =(1-\boldsymbol{p}_1)\,\boldsymbol{p}_2=0.9\cdot 0.02=0.018;$$
$$P(\boldsymbol{H}_3) = \boldsymbol{p}_1\,\boldsymbol{p}_2 = 0.1\cdot 0.02=0.002;$$
$$P(\boldsymbol{H}_4) = (1-\boldsymbol{p}_1)(1-\boldsymbol{p}_2)= 0.9\cdot 0.98=0.882;$$

причем $P(\boldsymbol{H}_1)+P(\boldsymbol{H}_2)+P(\boldsymbol{H}_3)+P(\boldsymbol{H}_4)=0.098+0.018+0.002+0.882=1$.

Требуется найти $P(\boldsymbol{A})$.

2). Гипотезы $\boldsymbol{H}_1$, $\boldsymbol{H}_2$, $\boldsymbol{H}_3$ и $\boldsymbol{H}_4$ являются попарно несовместными, так как это следует из введенных нами гипотез (всего только $\boldsymbol{n}$=4 гипотезы и иметь место может быть только одна из них) и образуют полную группу событий, так как $\boldsymbol{H}_1+\boldsymbol{H}_2+\boldsymbol{H}_3+\boldsymbol{H}_4=\boldsymbol{\Omega}$.

3). Найдем все условные вероятности $P(\boldsymbol{A}|\boldsymbol{H}_i)$ и затем $P(\boldsymbol{A})$:

$P(\boldsymbol{A}|\boldsymbol{H}_1)$= 1; $P(\boldsymbol{A}|\boldsymbol{H}_2)$= 0.9; $P(\boldsymbol{A}|\boldsymbol{H}_3)$= 0; $P(\boldsymbol{A}|\boldsymbol{H}_4)$= 1;

$$P(\boldsymbol{A})= \sum_{i=1}^{n}\left\{P\left(H_i\right)\cdot P\left(A\,|\,H_i\right)\right\} \text{ или}$$

$P(\boldsymbol{A})$= 0.098·1+0.018·0.9+0.02·0+ 0.882·1=0.9962 .

4). Условные вероятности $P(\boldsymbol{H}_i|\boldsymbol{A})$ вычислять не требуется.

5). И тем самым задача решена■

***Пример* 1.27** (см. [**56**, с. 18])

Экономист считает, что вероятность роста стоимости акции компании в следующем году составит **0.75**, если экономика страны будет на подъеме, и **0.3**, если экономика не будет успешно развиваться. По мнению экспертов, вероятность экономического подъема равна **0.6** . Оценить вероятность того, что акции компании поднимутся в следующем году.

Решение [**34**, с. 106]

1). Введем (***n***=2) гипотезы и сформулируем событие ***A***:

$\boldsymbol{H_1}$={*экономика страны будет на подъеме*},

$\boldsymbol{H_2}$={*экономика не будет успешно развиваться*},

A={*акции компании поднимутся в следующем году*}.

Априорные вероятности гипотез $P(\boldsymbol{H_i})$ практически известны из условия задачи:

$P(\boldsymbol{H_1})=0.6$;

$P(\boldsymbol{H_2})=[1-P(\boldsymbol{H_1})]=0.4$;

причем естественно, что $P(\boldsymbol{H_1})+P(\boldsymbol{H_2})= 0.6+0.4=1$.

Требуется найти $P(\boldsymbol{A})$.

2). Гипотезы $\boldsymbol{H_1}$ и $\boldsymbol{H_2}$ являются несовместными, так как это следует из введенных нами гипотез (всего только ***n***=2 гипотезы и иметь место может быть только одна из них) и образуют полную группу событий, так как $\boldsymbol{H_1}+\boldsymbol{H_2} = \boldsymbol{\Omega}$.

3). Найдем только $P(\boldsymbol{A})$, так как все условные вероятности $P(\boldsymbol{A}|\boldsymbol{H_i})$, где ***i***=1, 2 уже известны из условия задачи:

$P(\boldsymbol{A}|\boldsymbol{H_1})= 0.75$ (будет рост стоимости акции компании в следующем году, если экономика страны будет на подъеме);

$P(\boldsymbol{A}|\boldsymbol{H_2})= 0.3$ (будет рост стоимости акции компании в следующем году, если экономика страны не будет на подъеме);

$$P(\boldsymbol{A})= \sum_{i=1}^{n}\left\{P\left(H_i\right)\cdot P\left(A\,|\,H_i\right)\right\} = 0.6\cdot 0.75+0.4\cdot 0.3=0.57 .$$

4). Условные вероятности $P(\boldsymbol{H_i}|\boldsymbol{A})$ вычислять не требуется.

5). И тем самым задача решена■

***Пример* 1.28** (см. [**20**, с. 57])

2 стрелка независимо один от другого стреляют по одной мишени, делая каждый по одному выстрелу. Вероятность попадания в мишень для 1-го стрелка $\boldsymbol{p_1}$=0.8; для 2-го стрелка $\boldsymbol{p_2}$=0.4 . После стрельбы в мишени обнаружена одна пробоина. Найти вероятность того, что эта пробоина принадлежит 1-му стрелку (т.е. 1-й стрелок автор этой пробоины).

Решение [**34**, с. 102]

1). Введем гипотезы ($\boldsymbol{n}$=4) и сформулируем событие $\boldsymbol{A}$:

$\boldsymbol{H_1}$={*оба стрелка не попали*},

$\boldsymbol{H_2}$={*оба стрелка попали*},

$\boldsymbol{H_3}$={*1-й стрелок попал, 2-й не попал*},

$\boldsymbol{H_4}$={*1-й стрелок не попал, 2-й попал*},

$\boldsymbol{A}$={*обнаружена одна пробоина*}.

Вычислим все ($\boldsymbol{n}$=4) априорные вероятности гипотез:

$P(\boldsymbol{H_1}) = (1-\boldsymbol{p_1})(1-\boldsymbol{p_2})=0.2\cdot0.6=0.12;$

$P(\boldsymbol{H_2}) = \boldsymbol{p_1}\,\boldsymbol{p_2}= 0.8\cdot0.4=0.32;$

$P(\boldsymbol{H_3}) = \boldsymbol{p_1}(1-\boldsymbol{p_2}) = 0.8\cdot0.6=0.48;$

$P(\boldsymbol{H_4}) = (1-\boldsymbol{p_1})\boldsymbol{p_2}= 0.2\cdot0.4=0.08;$

причем $P(\boldsymbol{H_1})+P(\boldsymbol{H_2})+P(\boldsymbol{H_3})+P(\boldsymbol{H_4})=0.12+0.32+0.48+0.08=1$.

Требуется найти $P(\boldsymbol{H_3}|\boldsymbol{A})$.

2). Проверим, что гипотезы $\boldsymbol{H_1}, \boldsymbol{H_2}, \boldsymbol{H_3}$ и $\boldsymbol{H_4}$ являются попарно несовместными и образуют полную группу событий: это не требуется, так как это прямо следует из условия задачи и из введенных нами гипотез (всего только $\boldsymbol{n}$=4 гипотезы и иметь место может быть только одна из них).

3). Найдем $P(\boldsymbol{A})$ и все условные вероятности $P(\boldsymbol{A}|\boldsymbol{H_i})$:

$P(\boldsymbol{A}|\boldsymbol{H_1})=P(\boldsymbol{A}|\boldsymbol{H_2})=0$, так как $\boldsymbol{H_i}\not\subset\boldsymbol{A}$, где $\boldsymbol{i}$=1, 2;

$P(\boldsymbol{A}|\boldsymbol{H_3})=P(\boldsymbol{A}|\boldsymbol{H_4})=1$, так как $\boldsymbol{H_i}\subset\boldsymbol{A}$, где $\boldsymbol{i}$=3, 4;

$P(\boldsymbol{A})= P(\boldsymbol{H_1})\cdot0+P(\boldsymbol{H_2})\cdot0 + P(\boldsymbol{H_3})\cdot1+P(\boldsymbol{H_4})\cdot1= 0.48\cdot1+0.08\cdot1=0.56$.

4). Так как $P(\boldsymbol{A})\neq0$, то $P(H_3\,|\,A)=\dfrac{P(H_3)\cdot P(A\,|\,H_3)}{P(A)}=\dfrac{0.48\cdot1}{0.56}=\dfrac{6}{7}\approx0.857.$

5). И тем самым задача решена■

***Пример* 1.29**

Ковбой Джон 3 раза стреляет из кольта по консервной банке. Вероятность его удачного выстрела (т.е. попадания в банку) есть p=0.5 . Требуется найти вероятность того, что в банке будет ровно одна пробоина (см. [**35**, с. 35]).

Решение

1). Введем гипотезы (n=4) и сформулируем событие A:

H_1={*1-й выстрел попал, 2-й и 3-й не попали*},
H_2={*1-й выстрел не попал, 2-й попал и 3-й не попал*},
H_3={*1-й и 2-й выстрел не попали, 3-й попал*},
H_4={*есть 2 или 3 или 0 попаданий*},

A={*обнаружена одна пробоина*}.

Вычислим все (n=3) априорные вероятности гипотез:

$P(H_1) = p(1-p)(1-p)$=0.5·0.5·0.5=0.125;
$P(H_2) = (1-p)p\ (1-p)$= 0.5·0.5·0.5=0.125;
$P(H_3) = (1-p)(1-p)\ p$ = 0.5·0.5·0.5=0.125;
$P(H_4)$ = (1– 0.375) =0.625;

причем естественно, что $P(H_1)+P(H_2)+P(H_3)+P(H_4)$ =1.

2). Гипотезы H_1, H_2, H_3 и H_4 являются несовместными, так как это следует из введенных нами гипотез (всего только n=4 гипотезы и иметь место может быть только одна из них).

3). Найдем $P(A)$ и все условные вероятности $P(A|H_i)$:

$P(A|H_1)=P(A|H_2)=P(A|H_3)$=1, так как $H_i \subset A$, где i=1, 2, 3;

$P(A|H_4)$=0, так как $H_i \not\subset A$, где i=4;

$P(A)= P(H_1)\cdot 1+P(H_2)\cdot 1 + P(H_3)\cdot 1+P(H_4)\cdot 0$= 0.375·1+0=0.375 .

4). Условные вероятности $P(H_i|A)$ вычислять не требуется.

5). И тем самым задача решена■

В теории вероятностей изначально задается пространство **Ω**. Каждому *элементарному событию* $\omega \in \mathbf{\Omega}$ присвоено число $P(\omega)$ в виде вероятности появления этого события. Обычно требуется определить вероятность $P(\boldsymbol{A})$ заданного *составного* события ***A***. Теория вероятностей позволяет определить (вычислить) вероятность $P(\boldsymbol{A})$ путем разложения заданного *составного* события ***A*** и с помощью аксиом, правил и теорем этой теории. Специалисты предупреждают (см. [**35**, с. 22]), что с теорией вероятностей не так уж все просто и ясно, как это может показаться на первый взгляд.

Во-первых [**35**, с. 22], увеличение некоторого параметра (например, числа бросков монеты) может приводить к резкому увеличению числа точек в пространстве **Ω**. Графическое представление **Ω** становится невозможным или крайне затруднительно.

Во-вторых [**35**, с. 22], бывает очень сложно определить сами вероятности $P(\omega)$ элементарных событий. Приведем известную задачу [**35**]. Попробуйте самостоятельно ввести пространство **Ω** для случая, когда из мешка случайно (одна за одной) извлекаются 4 карточки с изображением букв **М**, **м**, **а**, **а**, причем, как видно, одна из букв прописная, а остальные — строчные. После того как **Ω** будет введено, попробуйте найти вероятность того, что, последовательно выкладывая эти карточки, будет образовано слово **Мама**.

В-третьих [**35**, с. 22], на практике реальные задачи становятся еще более сложными, чем учебные примеры. Для реальной задачи требуются необходимые знания той предметной области, в которой решается задача. Приведем известный пример [**35**, с. 22]. Составное событие "*Произошла аварийная остановка атомной электростанции (АЭС)* " может быть разделено на следующие 2 события:

- аварийная остановка АЭС произошла в результате автоматического срабатывания аварийной защиты;
- человек-оператор нажал кнопку аварийной защиты.

Важно понять, что каждое из этих событий может являться также составным. Действия человека-оператора могут быть как правильными, так и ошибочными, а сами ошибки тоже могут быть различимыми и т.д. На практике бывает очень трудно понять, где же следует все-таки остановиться и как зафиксировать саму совокупность *элементарных событий*.

Во всем этом и может помочь *диаграммная техника*.

1.4.5. Вычисление вероятности и диаграммная техника

Существует еще один способ вычисления вероятности заданного события и связан он с *диаграммной техникой* (ДТ).

Диаграммная техника, применяемая в теории вероятностей и которую будем сейчас рассматривать, опирается на идеи, связанные с подходом, который предложил *Р. Фейнман* для решения задач квантовой механики.

Суть этого метода ДТ состоит в следующем.

Вводится понятие *системы* (или *модели*). Эта система (модель) может находиться в каких-то *состояниях*. Выделяют два состояния системы (модели): *начальное* и *конечное*. Происходит изменение состояния системы (модели) в результате какого-то *процесса*. В конкретное состояние система (модель) может придти различными путями (или *траекториями*). Применяются два правила. Одно правило позволяет вычислить вероятность перехода системы (модели) по траектории, а другое позволяет вычислить вероятность перехода системы (модели) из начального положения в конечное положение.

Система (модель)

В конкретных рассматриваемых примерах речь обычно идет о монете, шарах, кубике или переключателе и т.п. физических *объектах*. Далее будем использовать более общее понятие *система* (или *модель*). Строгое формальное определение этому понятию давать не будем, однако отметим следующее (см. и ср. [**35**, с. 23]).

В **физике** наиболее распространено понятие *система*, несмотря на то, что используется и понятие *модель*. Так в квантовой механике рассматривают *систему квантовых объектов,* например систему, состоящую из двух кубитов.

В **кибернетике** большее распространение получило понятие *модель*, хотя понятие *системы* также используется, например, в вычислительной технике.

Далее будем полагать, как и в работе [**35**, с. 23-24], что *система* и *модель* — это синонимы.

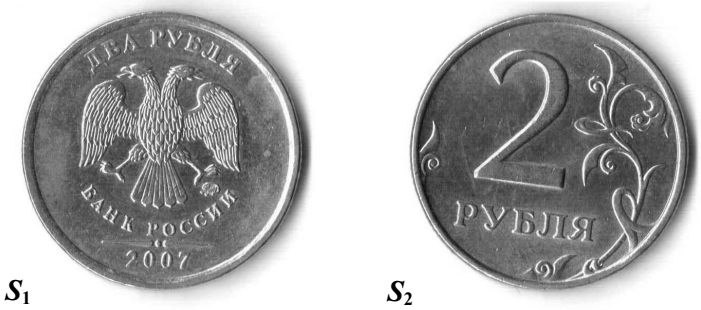
Состояние системы (модели)

Далее будем полагать, как и в работе [**35**, с. 24], что в фиксированный момент времени $\boldsymbol{T}$ системы могут находиться только в одном из $\boldsymbol{n}$ различных состояний $\boldsymbol{S}=\{\boldsymbol{S}_1, \boldsymbol{S}_2, \boldsymbol{S}_3,\ldots, \boldsymbol{S}_i,\ldots, \boldsymbol{S}_n\}$, при этом имеются моменты времени, в которых состояние рассматри-

ваемых систем является неопределенным (это связано с тем, что в эти моменты времени происходит смена (т.е. изменение) состояния системы). На практике иногда удобно начинать нумеровать состояния не с 1, а с 0, т.е. удобно вводить состояние $\boldsymbol{S_0}$. Рассмотрим некоторые простые примеры.

***Пример* 1.30** (см. [**35**, с. 24])

Монета, лежащая на поверхности стола, может находиться в одном из двух состояний: $\boldsymbol{S_1}$ или $\boldsymbol{S_2}$ (рис. 1.49).



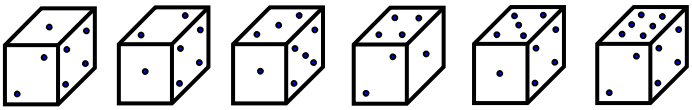
$\boldsymbol{S_1}$ $\boldsymbol{S_2}$

Рис. **1.49.** Возможные состояния монеты на поверхности стола

В случае состояния $\boldsymbol{S_1}$ при взгляде на монету можно увидеть герб (т.е. *орел*), а в случае состояния $\boldsymbol{S_2}$ при взгляде на монету можно увидеть цифру (т.е. *решку*). У монеты может быть и неопределенное состояние — это в том случае, когда ее берут со стола■

***Пример* 1.31** (см. [**35**, с. 24-25])

Игральный кубик (т.е. игральная кость) после броска (рис. 1.50) на стол может находиться в 1 из 6 состояний: $\boldsymbol{S_1}$, $\boldsymbol{S_2}$, $\boldsymbol{S_3}$, $\boldsymbol{S_4}$, $\boldsymbol{S_5}$, $\boldsymbol{S_6}$.



$\boldsymbol{S_1}$ $\boldsymbol{S_2}$ $\boldsymbol{S_3}$ $\boldsymbol{S_4}$ $\boldsymbol{S_5}$ $\boldsymbol{S_6}$

Рис. **1.50.** Возможные состояния кубика на поверхности стола

В момент броска или в то время, пока кубик находится в руке, или в то время, пока он еще движется по поверхности стола, кубик имеет неопределенное состояние■

Практика убедительно показывает, что для реальных объектов (систем) бывает достаточно трудно сходу понять, что же является именно состоянием физической системы. Приведенные выше примеры были достаточно упрощенными. Дадим несколько хорошо известных задач для самостоятельного размышления на эту тему.

***Задача* 1.1** (см. [**35**, с. 26])

В скольких состояниях может находиться канцелярская кнопка, лежащая на столе?

Ответ: 1, *2*, 3, 4, 5, 6.

***Задача* 1.2** (см. [**35**, с. 26])

В скольких состояниях может находиться на столе тело цилиндрической формы с диаметром основания $\boldsymbol{R}$ и высотой $\boldsymbol{L}$?

Ответ: 1, 2, *3*, 4, 5, 6.

***Задача* 1.3** (см. [**35**, с. 26])

При игре нескольких участников со спичечным коробком существуют следующие правила:

если коробок падает этикеткой вверх, то дается 1 очко;

если коробок падает на боковую грань, то дается 5 очков;

если коробок падает на торец, то дается 10 очков;

если коробок падает этикеткой вниз, то все набранные в данной серии бросаний очки сгорают и ход переходит к другому участнику игры. Требуется определить число различных состояний коробка после его падения.

Ответ: 1, 2, 3, *4*, 5, 6.

***Задача* 1.4** (см. [**35**, с. 27])

Три раза подбрасывают кубик, интересуясь при этом суммарным числом выпавших шестерок.

Сколько здесь возможных различных состояний?

Ответ: 1, 2, 3, *4*, 5, 6, 7.

***Задача* 1.5** (см. [**35**, с. 27])

Три раза подбрасывают кубик, интересуясь при этом суммарным числом выпавших очков.

Сколько здесь возможных различных состояний?

Ответ: 8, 10, 11, 12, 13, 14, 16, 18, 20, *31*, 64, 128.

Сделаем одно важное, но существенное замечание относительно состояния системы. Выше предполагалось, что состояния системы (кубика, монеты, диода, транзистора, триггера, элемента ИЛИ, комбинационной схемы, ЦВМ и т.п. объектов) — это все состояния именно *классической системы,* т.е. системы, подчиняющейся законам *классической физики*.

Определение 1.89

Состояние [**63**, с. 189] — совокупность количественных значений параметров, описывающих объект, и качественных признаков объекта. Номенклатура этих параметров и признаков, а также пределы допускаемых их изменений устанавливаются документацией на объект. С точки зрения надежности различают *исправное* и *неисправное* состояния, *работоспособное* и *неработоспособное*, а также *предельное* состояние.

Определение 1.90

Работоспособное состояние (работоспособность) [**63**, с. 188] — состояние объекта, при котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствуют требованиям нормативно-технической и (или) конструкторской документации.

Определение 1.91

НЕработоспособное состояние (неработоспособность) [**63**, с. 186] — состояние объекта, при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции, не соответствует требованиям нормативно-технической и (или) конструкторской документации.

Определение 1.92

Исправное состояние (исправность) [**63**, с. 184] — состояние объекта, при котором он соответствует требованиям нормативно-технической и (или) конструкторской документации.

Определение 1.93

НЕисправное состояние (неисправность) [**63**, с. 186] — состояние объекта, при котором он не соответствует хотя бы одному из требований нормативно-технической и (или) конструкторской документации.

Определение 1.94

Предельное состояние [**63**, с. 187] — состояние объекта, при котором его дальнейшее применение по назначению недопустимо или нецелесообразно, либо восстановление его исправного или работоспособного состояния невозможно или нецелесообразно.

Состояния *классической системы*, например логического элемента ИЛИ, можно классифицировать так, как представлено на рис. 1.51. Действительно, на практике элемент ИЛИ может быть либо в исправном состоянии, либо в неисправном состоянии. Может иметь место так называемый *отказ* элемента. Иногда (кроме отказа) специалисты по *теории надежности* выделяют *сбой* элемента (подразумевая под этим *самоустраняющейся* отказ).

Если элемент ИЛИ не исправен, то он может все время выдавать на выходе логический нуль (т.е. быть в состоянии залипания в нуль), или логическую единицу (т.е. быть в состоянии залипания в единицу), или же выдавать на выход что-то совсем другое.

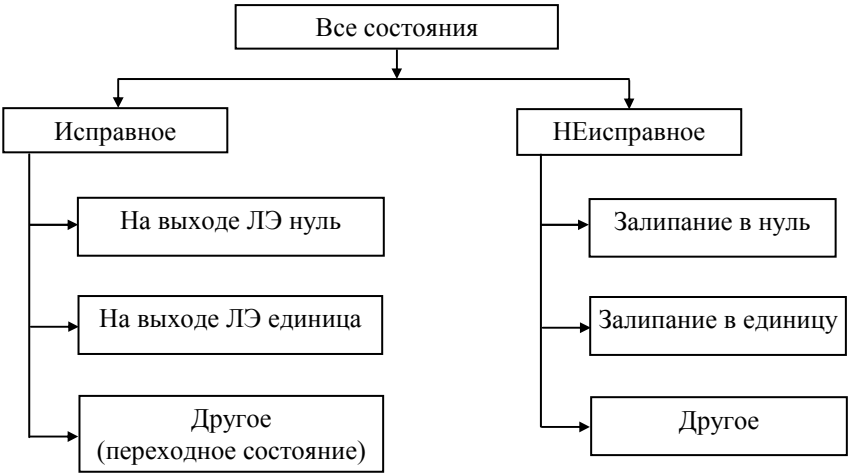


Рис. **1.51.** Возможная классификация состояний элемента ИЛИ

Если элемент ИЛИ исправен, то он (после выполнения всех переходных процессов) правильно выдает на выходе логический нуль или логическую единицу.

В моменты времени, когда еще не завершились все переходные процессы в элементе, он может работать не в соответствии со своей таблицей истинности.

Квантовый объект, например одиночный кубит, может быть (как и ЛЭ ИЛИ) в *исправном* или в *неисправном* состоянии. Одиночный кубит как *квантовый объект* уже может находиться или в *чистом* состоянии, или в *смешанном* состоянии. В чистом состоянии состояние кубита можно представить как *суперпозицию* других чистых состояний. Кубит может находиться в *базисном* состоянии. Если кубит не одиночный (т.е. имеется несколько кубитов или иными словами имеется уже *квантовая система*), то у кубита может возникнуть состояние, которое называется *сцепленным* (или перепутанным) состоянием.

Состояния *квантовой системы*, например системы из двух кубитов, можно классифицировать так, как представлено на рис. 1.52.

Рис. **1.52.** Возможная классификация состояний квантовой системы из 2-х кубитов

Изменение состояния системы (модели)

Далее будем полагать, как и в работе [**35**, с. 27], что состояние системы остается без изменения на последовательных пронумерованных и следующих один за другими интервалах времени:

$$\boldsymbol{T}=\{\boldsymbol{T}_1, \boldsymbol{T}_2, \boldsymbol{T}_3,\ldots, \boldsymbol{T}_i,\ldots, \boldsymbol{T}_n\},$$

которые не перекрываются между собой. На практике иногда удобно начинать нумеровать интервалы времени не с 1, а с 0, т.е. удобно вводить интервал времени $\boldsymbol{T}_0$. Будем считать, что в моменты времени между этими интервалами состояние *классической* системы может изменяться некоторым *случайным* образом. Рассмотрим простой пример.

***Пример* 1.32** (см. [**35**, с. 27])

Монета, лежащая *орлом* к верху на поверхности стола, находится в состоянии $\boldsymbol{S}_1$ (рис. 1.53**а**) в течение интервала времени $\boldsymbol{T}=\boldsymbol{T}_1$.

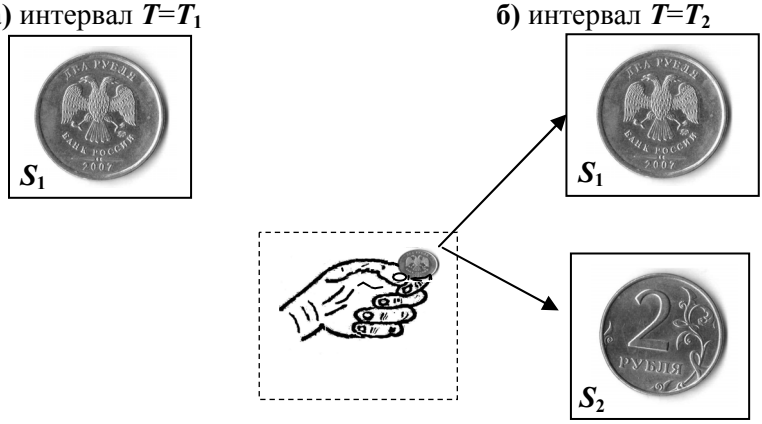


Рис. **1.53.** Монета в состоянии $\boldsymbol{S}_i$ на интервале времени $\boldsymbol{T}=\boldsymbol{T}_i$

Затем берут эту монету со стола в руку, подбрасывают в воздух, ждут, пока она кувыркается в воздухе и не упадет на поверхность стола, перейдя в очередное состояние, соответствующее следующему интервалу времени (рис. 1.53**б**). В результате такого подбрасывания монета может оказаться (рис. 1.53**б**) в одном из двух состояний: $\boldsymbol{S}_1$ (*орел*) или $\boldsymbol{S}_2$ (*решка*), которое затем уже не меняется на интервале времени $\boldsymbol{T}=\boldsymbol{T}_2$■

Диаграмма переходов системы (модели)

Для того чтобы получить диаграмму переходов *классической* системы из одного состояния в другое в различные последовательные интервалы времени, поступают следующим образом. Покажем это для случая *примера* 1.30. Для этого достаточно просто изменить рис. 1.53**б**, как показано на рис. 1.54 [**35**, с. 28].

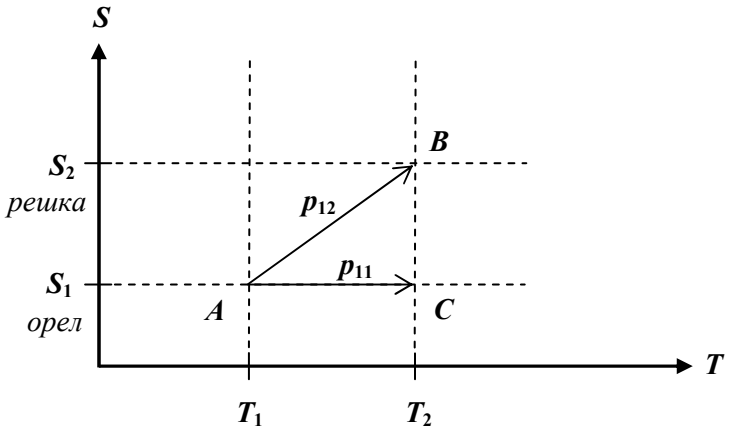


Рис. **1.54.** Диаграмма 2-х переходов для монеты

Процессы

На диаграмме переходов стрелками принято [**35**, с. 28] обозначать возможные процессы, изменяющие состояния *классической* системы (модели). Договорились (см. [**35**, с. 28]), что процесс начинается и заканчивается каким-то состоянием системы, причем сам процесс характеризуется некоторой *вероятностью процесса*. Процессы, которые невозможны (т.е. не могут иметь место), обычно на диаграмме не показывают. В рассматриваемых простых примерах такие процессы обычно имеют **нулевую** вероятность.

Для случая *примера* 1.30 возможны 2 процесса, которые характеризуются вероятностями $\boldsymbol{p_{11}}$ и $\boldsymbol{p_{12}}$.

После реализации 1-го процесса (т.е. выполнен переход $A \to \mathrm{C}$) выпадает *орел* (отметим, что до этого монета лежала *орлом* вверх) и монета переходит в состояние $\boldsymbol{S_1}$ (точнее, остается в этом состоянии $\boldsymbol{S_1}$). Такой переход из 1-го состояния во 1-е состояние осуществляется с вероятностью $\boldsymbol{p_{11}}$.

После реализации 2-го процесса (т.е. выполнен переход $A \to B$) выпадает *решка* (отметим, что до этого монета лежала *орлом* вверх) и монета переходит в состояние $\boldsymbol{S_2}$ (точнее, монета меняет состояние $\boldsymbol{S_1}$ на состояние $\boldsymbol{S_2}$). Такой переход из 1-го состояния во 2-е состояние осуществляется с вероятностью $\boldsymbol{p_{12}}$.

На практике вероятности процессов получить бывает не всегда просто. В некоторых случаях эти вероятности являются заданными, либо их достаточно не сложно получить из некоторых соображений симметрии и равновозможности исходов опыта или из иных соображений. В ряде случаев на помощь приходят методы математической статистики. Например, для идеальной монеты вероятности процессов соответственно равны $\boldsymbol{p_{11}}= \boldsymbol{p_{12}}=0.5$ и не зависят от исходного состояния монеты, которое было до ее броска, а для идеальной игральной кости (кубика) эти вероятности есть 1/6.

Другим важным понятием в диаграммной технике при вычислении вероятностей является *траектория*.

Траектория системы (модели)

На диаграмме переходов принято выделять *траекторию системы*, которая (см. [**35**, с. 29]) задается фиксированным набором $\boldsymbol{S}$ состояний *классической* системы в следующие друг за другом интервалы времени $\boldsymbol{T}$. Рассмотрим некоторые простые примеры.

***Пример* 1.33** (см. [**35**, с. 29-31])

Построим все возможные траектории для 2-х бросков игральной кости (кубика), в результате которых сумма очков равна 5. На рис. 1.55 показаны состояния $\boldsymbol{S_i}$ и соответствующая им сумма $\boldsymbol{i}$ выпавших очков на игральной кости. Из рис. 1.55 хорошо видно, что в данном случае система может переходить из одного состояния в другое по следующим 4-м траекториям:

траектория 1: $\{ \boldsymbol{S_0}, \boldsymbol{S_1}, \boldsymbol{S_5} \}$;
траектория 2: $\{ \boldsymbol{S_0}, \boldsymbol{S_2}, \boldsymbol{S_5} \}$;
траектория 3: $\{ \boldsymbol{S_0}, \boldsymbol{S_3}, \boldsymbol{S_5} \}$;
траектория 4: $\{ \boldsymbol{S_0}, \boldsymbol{S_4}, \boldsymbol{S_5} \}$.

Таким образом, из начального состояния $\boldsymbol{S_0}$ в состояние $\boldsymbol{S_5}$ (т.е. из точки $\boldsymbol{O}$ в точку $\boldsymbol{E}$) можно попасть только по этим 4 траекториям■

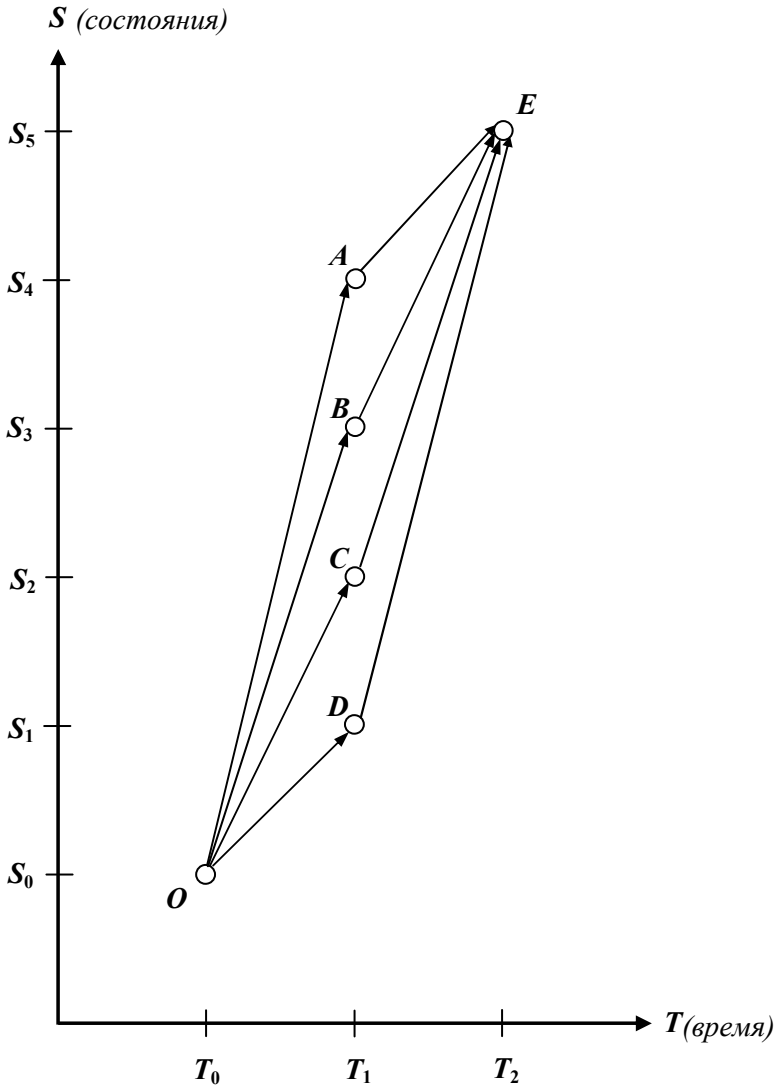


Рис. **1.55.** Диаграмма переходов для 2-х бросков кубика

***Пример* 1.34** (см. [**35**, с. 31])

Построим все возможные переходы и некоторые траектории для 3-х бросков монеты, при условии, что нас интересует суммарное количество выпавших *орлов* (*гербов*). На рис 1.56 показаны состояния S_i и соответствующее им число i выпавших *орлов* для монеты. Из рис. 1.56 хорошо видно, что в данном случае система может переходить из одного состояния в другое по многим траекториям: например, в состояние S_1 (точка C) система может попасть следующими путями:

траектория 1: $\{ S_0, S_1, S_1, S_1 \}$;
траектория 2: $\{ S_0, S_0, S_1, S_1 \}$;
траектория 3: $\{ S_0, S_0, S_0, S_1 \}$.

Из начального состояния S_0 в состояние S_3 (т.е. из точки O в точку A) можно попасть только по одной единственной траектории: $\{ S_0, S_1, S_2, S_3 \}$. Для идеальной монеты $p_{00}= p_{01}= p_{11}= p_{12}= p_{22}= p_{23}=1/2$ ■

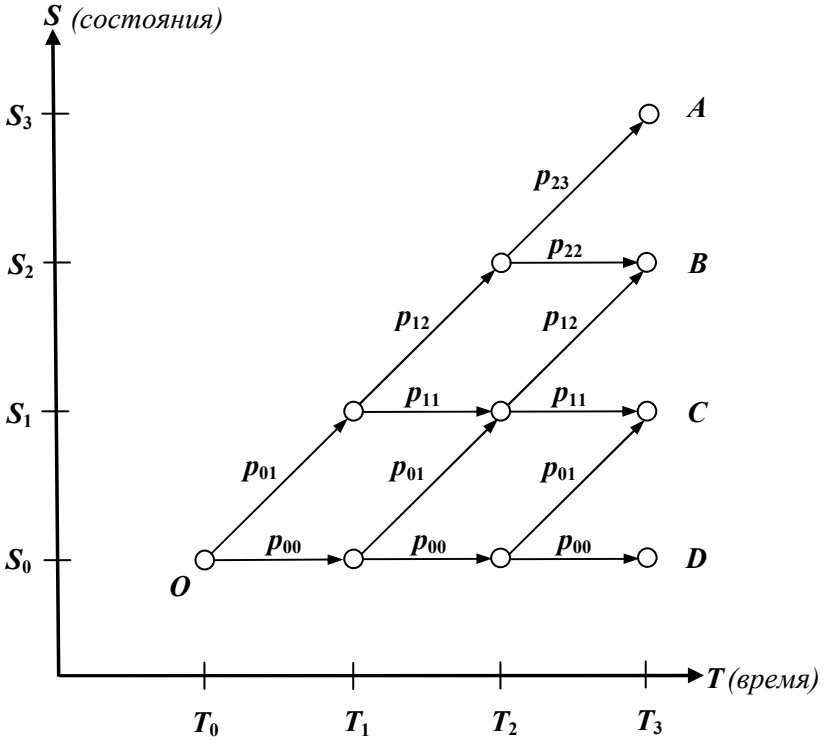


Рис. **1.56.** Диаграмма переходов для 3-х бросков монеты

Правило 1.1 (см. и ср. [**35**, с.33; **62**, с.51])

Вероятность перехода системы по траектории из одного положения (состояния) в другое положение (состояние) равна ***произведению*** *вероятностей всех процессов, связывающих между собой состояния, принадлежащие данной траектории* ■

Правило 1.2 (см. и ср. [**35**, с.323; **62**, с.41])

Вероятность перехода системы из начального положения (состояния) в конечное положение (состояние) равна ***сумме*** *вероятностей переходов по всем возможным траекториям, связывающим эти положения (состояния)* ■

ОТМЕТИМ. Специалисты отмечают [**35**, с.59], что ДТ является достаточно удобным инструментом для решения задач *теории вероятностей*. Больше всего она подходит в том случае, когда есть последовательность событий, которые происходят в промежутках времени, следующих один за другим. Иногда реальную задачу можно представить как такую последовательность событий.

ВАЖНО ПОМНИТЬ (см. [**35**, с. 59]). С помощью теории вероятностей можно по заданным вероятностям *элементарных событий* вычислить вероятность некоторого конкретного сложного события. При этом на вопрос, откуда берутся сами вероятности *элементарных событий*, эта теория ответа не дает. В некоторых случаях эти вероятности можно получить с помощью другой теории — *математической статистики*.

ОТМЕТИМ [**35**, с.23]. Диаграммная техника требует рассматривать происходящие процессы с системой, как развивающиеся во времени. При этом *пространство* элементарных событий есть застывший и неизменный во времени набор элементарных событий.

Кроме диаграммной техники существует еще другой метод вычисления вероятности заданного сложного события с помощью *дерева событий*. При построении диаграммы переходов число ветвей (от числа интервалов и числа состояний) растет значительно медленнее, чем для *дерева событий*. Принято, что на диаграмме переходов все траектории для интересующего события (т.е. конечного состояния системы) сходятся в одной единственной точке.

Рассмотрим следующий пример.

***Пример* 1.35** (см. и ср. [**35**, с. 59-60])

Игральную кость (кубик) бросают три раза подряд и наблюдают за числом выпавших шестерок. При этом интересуются выпадением только 1-й шестерки при трех бросках кубика.

Построим *дерево событий* и *диаграмму переходов* и затем сравним их между собой.

Для трех бросков идеального кубика, когда интересуются выпадением только 1-й шестерки, дерево событий (рис. 1.57**а**) и диаграмма переходов (рис. 1.57**б**) представлены на рис. 1.57.

На дереве событий (см. рис. 1.57**а**) приняты следующие обозначения: событие $\boldsymbol{U}$ – не выпало ни одной шестерки, а событие $\boldsymbol{V}$ – выпало 3 шестерки. Событию, когда выпала только 1 шестерка, соответствуют 3 точки $\boldsymbol{G}$, $\boldsymbol{M}$, $\boldsymbol{Z}$ на рис. 1.57**а**, а на рис. 1.57**б** только одна точка $\boldsymbol{C}$, соответствующая конечному состоянию системы $\boldsymbol{S_1}$.

На диаграмме переходов (рис. 1.57**б**) приняты следующие обозначения. Состоянию $\boldsymbol{S_i}$ соответствует число $\boldsymbol{i}$ выпавших шестерок для кубика. В начальный момент времени $\boldsymbol{T_0}$ число выпавших шестерок есть нуль, так как еще не было совершено ни одного броска кубика. Начальному состоянию системы $\boldsymbol{S_0}$ (точка $\boldsymbol{O}$) соответствует выпадение ни одной шестерки. Если шестерка при очередном броске кубика не выпадает, то система остается в этом состоянии $\boldsymbol{S_0}$ на протяжении очередного интервала времени, например $\boldsymbol{T_1}$, $\boldsymbol{T_2}$ или $\boldsymbol{T_3}$.

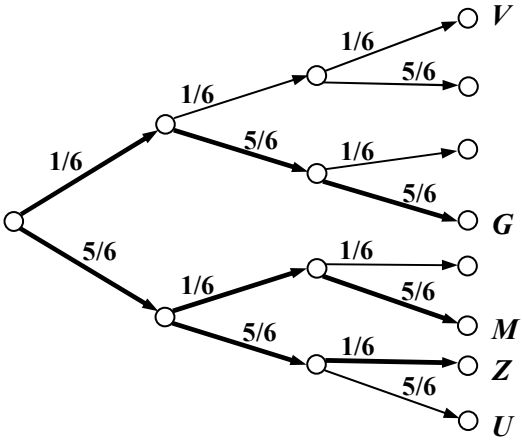
Так как кубик правильный, то вероятности процессов при выпадении шестерки (одинаковы) и есть 1/6, а при невыпадении шестерки (т.е. выпадении любой другой цифры) есть 5/6. Значения этих вероятностей и показаны на диаграмме переходов и на дереве событий.

Заметим, что при построении диаграммы переходов на рис. 1.57**б** число ветвей растет в *арифметической* прогрессии (т.е. 2, 4, 6,…), а при построении дерева событий на рис. 1.57**а** это число ветвей растет в *геометрической* прогрессии (т.е. 2, 4, 8,…).

На этом закончим обсуждение данного примера■

Рассмотрим далее достаточно простые и наглядные примеры вычисления вероятности перехода системы из одного состояния в другое с помощью диаграммной техники.

а)



б)

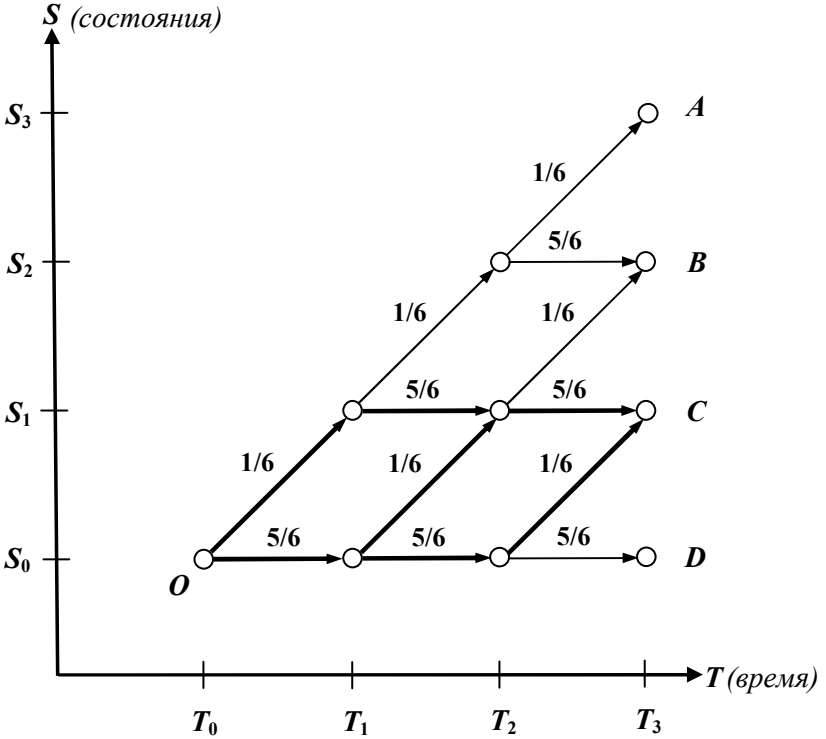


Рис. **1.57.** Дерево событий **а)** и диаграмма переходов **б)**

***Пример* 1.36** (см. [**35**, с. 32-33,44-45])

Четыре буквы разрезной азбуки **М**, **М**, **А**, **А** положены в мешок, откуда их вынимают наудачу (т.е. случайным образом) и располагают одну за другой в порядке, в котором они появляются. Требуется определить вероятность $P_{\mathbf{МАМА}}$ появления слова **МАМА**.

Решение

1). Введем состояния системы: $\boldsymbol{S_0}$ – начальное; $\boldsymbol{S_1}$ – состояние неудачи, когда требуемое слово не получится; $\boldsymbol{S_2}$ – первая буква в слове **М**; $\boldsymbol{S_3}$ – две первых буквы в слове **МА**; $\boldsymbol{S_4}$ – три первых буквы в слове **МАМ**; $\boldsymbol{S_5}$ – четыре первых буквы в слове **МАМА**.

2). Построим диаграмму, укажем вероятности процессов и выясним, какие траектории могут иметь место (рис. 1.58).

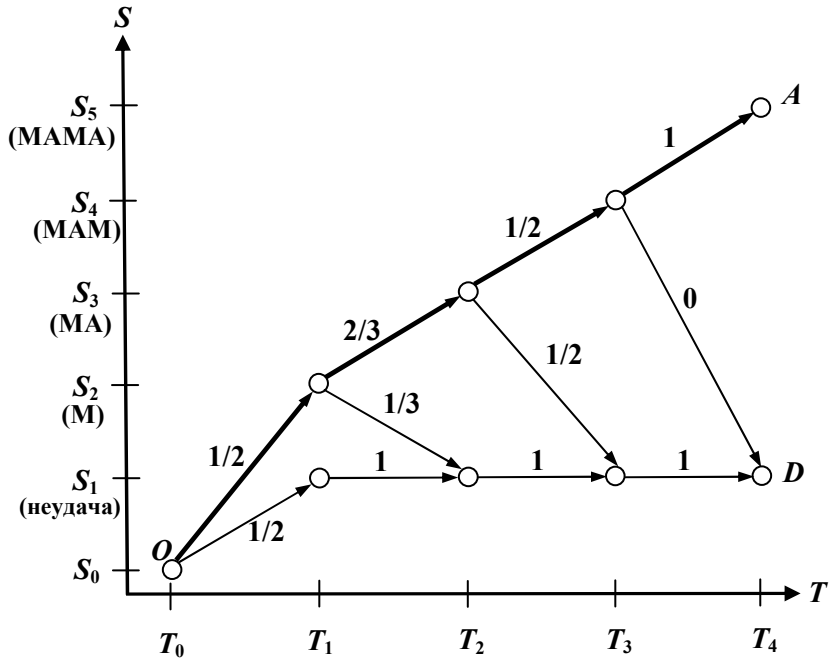


Рис. **1.58.** Диаграмма переходов (слово **МАМА**)

3). Имеется только 1 траектория из точки $\boldsymbol{O}$ в точку $\boldsymbol{A}$ ($O \to A$). Тогда искомая вероятность есть $P_{\mathbf{МАМА}}=(1/2)\cdot(2/3)\cdot(1/2)\cdot 1=1/6$.

4). И тем самым задача решена■

***Пример* 1.37** (см. [**35**, с. 50-52])

В случае бросания 2-х игральных костей (кубиков) сумма выпавших очков заключена между 2 и 12. Сумма в 9 очков может быть получена из цифр 1, 2, 3, 4, 5, 6 двумя возможными способами: **9**=3+6=4+5. Сумма в 10 очков также может быть получена двумя способами: **10**=4+6=5+5. Требуется определить, какая сумма появляется чаще, 9 или 10, или же они появляются одинаково часто?

Решение

1). Введем состояния системы $\boldsymbol{S_i}$, где $\boldsymbol{i}$ – сумма выпавших очков, причем начальное состояние есть $\boldsymbol{S_0}$, а конечные – $\boldsymbol{S_9}$ и $\boldsymbol{S_{10}}$.

2). Будем полагать, что результат бросания 2-х правильных кубиков эквивалентен 2-м бросаниям одного правильного кубика. Построим диаграмму (для суммы 9, см. рис. 1.59**а** и для суммы 10, см. рис. 1.59**б**), укажем вероятности процессов и выясним, какие траектории могут иметь место (рис. 1.59). Кубик правильный, а значит, все вероятности процессов одинаковы и есть 1/6.

3). Требуется определить вероятности P_9 и P_{10}, где P_9 – вероятность перехода ($O \to A$, см. рис. 1.59**а**) системы из начального положения (т.е. состояния $\boldsymbol{S_0}$) в конечное положение (т.е. в состояние $\boldsymbol{S_9}$), а P_{10} – вероятность перехода ($O \to D$, см. рис. 1.59**б**) системы из начального положения $\boldsymbol{S_0}$ в конечное положение $\boldsymbol{S_{10}}$.

4). Вычислим P_9. Согласно диаграмме (рис. 1.59**а**) из точки $\boldsymbol{O}$ в точку $\boldsymbol{A}$ можно прийти только по 4 следующим траекториям:

траектория 1: { $\boldsymbol{S_0}$, $\boldsymbol{S_6}$, $\boldsymbol{S_9}$ }; траектория 2: { $\boldsymbol{S_0}$, $\boldsymbol{S_5}$, $\boldsymbol{S_9}$ };
траектория 3: { $\boldsymbol{S_0}$, $\boldsymbol{S_4}$, $\boldsymbol{S_9}$ }; траектория 4: { $\boldsymbol{S_0}$, $\boldsymbol{S_3}$, $\boldsymbol{S_9}$ }.

Применяем *Правило* 1.1 для вычисления вероятности перехода системы по каждой траектории. В данном случае эти вероятности одинаковы и есть $P_{\text{траектории}}=(1/6)\cdot(1/6)=1/36$.

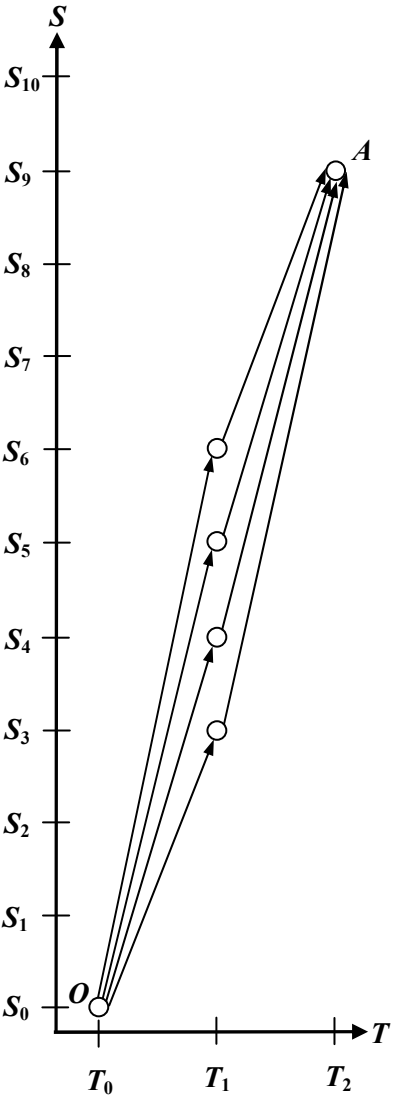
Применяем *Правило* 1.2 для вычисления вероятности P_9 перехода системы из состояния $\boldsymbol{S_0}$ в состояние $\boldsymbol{S_9}$. В данном случае эта вероятность есть $P_9=P(O \to A)=(1/36)+(1/36)+(1/36)+(1/36)=4/36=1/9$.

5). Вычислим P_{10}. Согласно диаграмме (рис. 1.59**б**) из точки $\boldsymbol{O}$ в точку $\boldsymbol{D}$ можно прийти только по 3 траекториям. Из *Правила* 1.2 следует, что $P_{10}=P\left(O \to D\right)=(1/36)+(1/36)+(1/36)=3/36=1/12$.

6). Получаем, что $P_9>P_{10}$.

7). И тем самым задача решена■

а) Сумма в 9 очков



б) Сумма в 10 очков

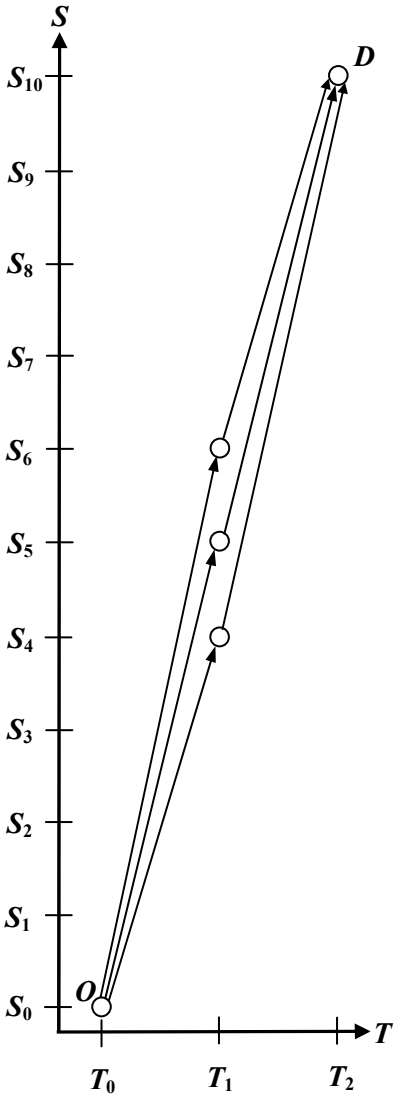


Рис. **1.59.** Диаграммы переходов для 2-х кубиков

***Пример* 1.38**

Ковбой Джон 3 раза стреляет из кольта по консервной банке. Вероятность его удачного выстрела (т.е. попадания в банку) есть p=0.5 . Требуется найти вероятность того, что в банке будет ровно одна пробоина (см. [**35**, с. 35]).

Решение (см. [**35**, с. 35-37] и ср. с решением из ***Примера* 1.29**)

1). Введем состояния системы S_i, где i – число пробоин в банке, причем начальное (точка O) есть S_0, а конечное – S_1 (точка C).

2). Построим диаграмму, укажем вероятности процессов и выясним, какие траектории могут иметь место (рис. 1.60). При 1-м выстреле возможны следующие 2 исхода:

- с вероятностью p в банке появится одна пробоина;
- с вероятностью (1/2)=1–p пробоина в банке НЕ появится;

Все вероятности процессов одинаковы и есть 1/2.

3). Требуется определить вероятность P_1 – вероятность перехода системы ($O \to C$, см. рис. 1.60) из состояния S_0 в S_1 (точка C).

4). Вычислим P_1. Согласно диаграмме (рис. 1.60) из точки O в точку C можно прейти только по 3-м следующим траекториям:

траектория 1: { S_0, S_1, S_1, S_1 };
траектория 2: { S_0, S_0, S_1, S_1 };
траектория 3: { S_0, S_0, S_0, S_1 }.

Применяем *Правило* 1.1 для вычисления вероятности перехода системы по каждой траектории. В данном случае эти вероятности одинаковы и есть $P_{\text{траектории}}$=(1/2)·(1/2)·(1/2)=1/8.

Применяем *Правило* 1.2 для вычисления вероятности P_1 перехода системы из состояния S_0 в состояние S_1. В данном случае эта вероятность есть $P_1 = P\left(O \to C\right)$ =(1/8)+(1/8)+(1/8)=(3/8)=0.375 .

5). Получаем, что P_1 =0.375 .

6). И тем самым задача решена■

ВАЖНО ПОМНИТЬ. Диаграммная техника тесно связана с квантовыми вычислениями и особенно с *амплитудой вероятности* [**33**], рассматриваемой далее. Более сложное ее развитие связано с интегралами по траекториям [**62**], применяемыми в физике.

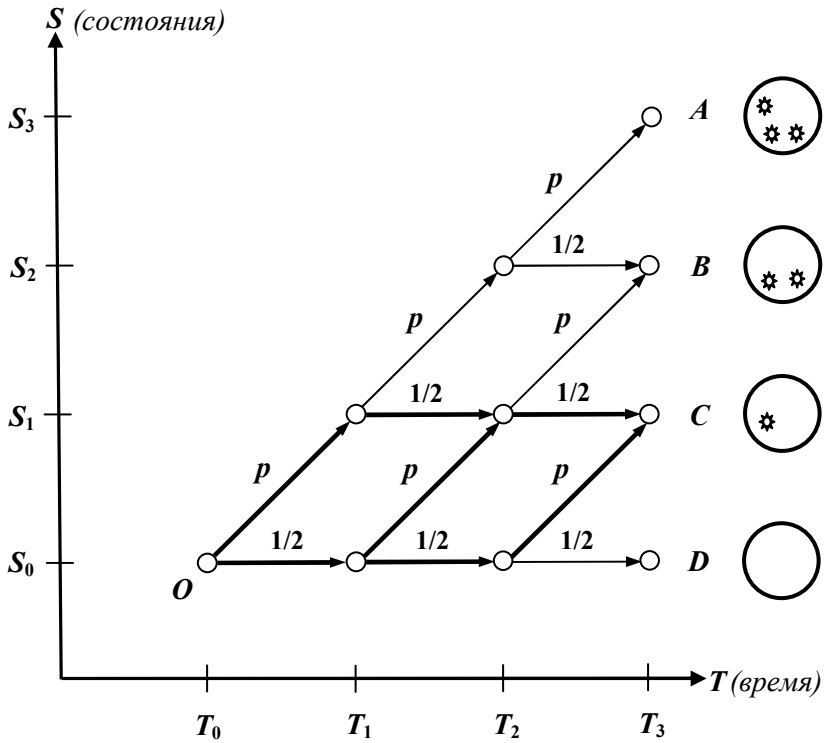


Рис. **1.60.** Диаграмма переходов для 3-х выстрелов из кольта

ОТМЕТИМ [**35**, с.37]. Диаграмма переходов на рис. 1.60 является достаточно избыточной для решения ***Примера* 1.36**. На практике иногда имеет смысл использовать несколько упрощенную (так называемую частную) диаграмму, содержащую только необходимые траектории для получения конечного результата.

ОТМЕТИМ. Те процессы, которые невозможны (т.е. не могут иметь место и, как правило, имеют нулевую вероятность), обычно на диаграмме стрелками не показывают. В основе *Правил* 1.1, 1.2 лежат теоремы сложения и умножения вероятностей.

Перейдем к рассмотрению такого очень важного понятия как *измерение* состояния классической системы.

Диаграмма переходов вероятностных логических элементов

Рассмотрим подробнее элемент ***R*** — *вероятностный* логический элемент НЕ, который представлен на рис. 1.61**а**.

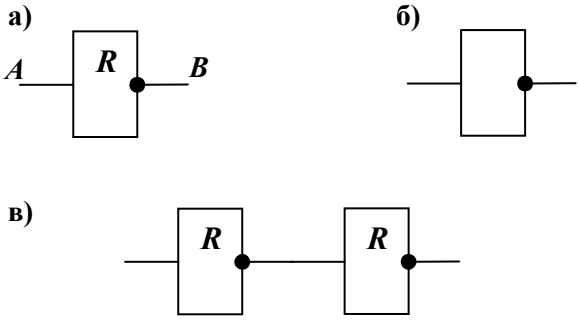


Рис. **1.61.** Логический элемент НЕ

Этот логический элемент случайно преобразует входной сигнал ***A*** (т.е. 0 или 1) в выходной сигнал ***B*** (т.е. 0 или 1) в соответствии со следующими вероятностями p_{AB}:

p_{00} — вероятность преобразования 0 в 0;
p_{01} — вероятность преобразования 0 в 1;
p_{10} — вероятность преобразования 1 в 0;
p_{11} — вероятность преобразования 1 в 1;

причем $\sum_{B=0}^{1}\{p_{AB}\}=1$. Иногда такой элемент специалисты [**33**] называют случайным переключателем. Работа этого вероятностного элемента подчиняется *классическим законам* физики.

В случае, когда $p_{01} = p_{10} = 0$, $p_{00} = p_{11} = 1$, данный элемент является уже детерминированным и в точности совпадает с ЛЭ НЕ (рис. 1.61**б**), рассмотренным ранее. В других случаях данный элемент является устройством со случайным поведением.

Если имеется несколько таких вероятностных ЛЭ, например, как на рис. 1.61**в**, то они работают независимо друг от друга (т.е. логика работы одного элемента никак не зависит от работы другого такого же элемента, соединенного с ним в одной комбинационной схеме).

Рассмотрим следующий пример.

***Пример* 1.39**

Два вероятностных логических элемента НЕ соединены так, как на рис. 1.61**в**. Вероятности p_{AB} известны $p_{01} = p_{10} = p_{00} = p_{11} = 0.5$. Требуется построить диаграмму переходов и найти вероятность того, что на выходе будет 1, если на вход подан 0 (см. и ср. [**33**]).

Решение

1). Введем состояния системы S_i, где i – число 0 или 1, причем начальное (точка O) есть S_0, а конечное – S_1 (точка C).

2). Построим диаграмму, укажем вероятности процессов и выясним, какие траектории могут иметь место (рис. 1.62).
Все вероятности процессов одинаковы и есть 1/2.

3). Требуется определить вероятность P_{01} – вероятность перехода системы ($O \to C$, см. рис. 1.62) из состояния S_0 в S_1 (точка C).

4). Вычислим P_{01}. Согласно диаграмме (рис. 1.62) из точки O в точку C можно прейти только по 2-м следующим траекториям:

траектория 1: { S_0, S_1, S_1 };
траектория 2: { S_0, S_0, S_1 }.

Применяем *Правило* 1.1 для вычисления вероятности перехода системы по каждой траектории. В данном случае эти вероятности одинаковы и есть $P_{\text{траектории}} = p_{01}\, p_{11} = p_{00}\, p_{01} = (1/2)\cdot(1/2) = 1/4$.
Применяем *Правило* 1.2 для вычисления вероятности P_{01} перехода системы из состояния S_0 в состояние S_1. В данном случае эта вероятность есть $P_{01} = P\left(O \to C\right) = (1/4)+(1/4) = (1/2)$ или

$$P_{01} = p_{01}\, p_{11} + p_{00}\, p_{01} = p_{01}(p_{11} + p_{00}) = p_{01}(0.5 + 0.5) = p_{01} \cdot 1 = p_{01}.$$

5). Получаем, что $P_{01} = 0.5$.

6). Аналогично для $P_{00} = P\left(O \to D\right)$ можно вычислить, что

$$P_{\text{траектории}} = p_{01}\, p_{10} = p_{00}\, p_{00} = (1/2)\cdot(1/2) = 1/4.$$
$$P_{00} = P\left(O \to D\right) = (1/4)+(1/4) = (1/2) \text{ или}$$
$$P_{00} = p_{01}\, p_{10} + p_{00}\, p_{00} = p_{00}(0.5 + 0.5) = p_{00} \cdot 1 = p_{00}.$$

А также, что

$$P_{10} = P\left(I \to D\right) = (1/4)+(1/4) = (1/2) = p_{10}.$$
$$P_{11} = P\left(I \to C\right) = (1/4)+(1/4) = (1/2) = p_{11}.$$

7). И тем самым задача решена■

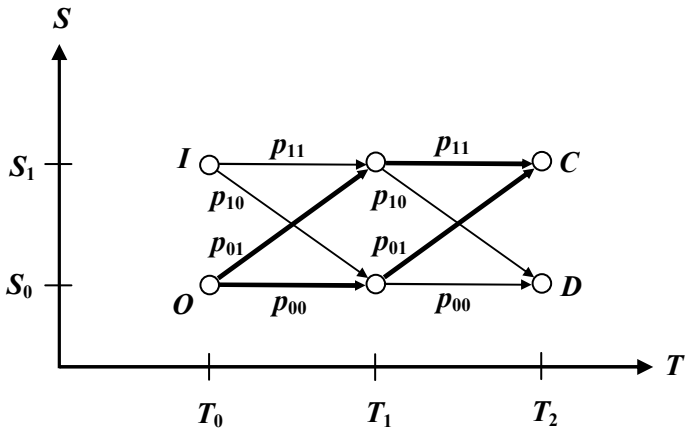


Рис. **1.62.** Диаграмма переходов для 2-х элементов ***R***

ОТМЕТИМ. С точки зрения логики работы, два последовательно соединенных элемента ***R*** эквивалентны одному элементу ***R***, если $p_{01}= p_{10}= p_{00}= p_{11}= 1/2$.

ВАЖНО ПОМНИТЬ (см. [**33**; **17**, с. 41-42]). Два последовательно соединенных *квантовых* элемента, например элементы $\sqrt{\boldsymbol{not}}$ (или элементы *Адамара* (рис. 1.63**б**), обозначаемые на *квантовых* схемах (рис. 1.63**а**) как ***H***), уже не приводят к аналогичному эффекту, несмотря на то, что для *квантового* элемента ***H*** и $\sqrt{\boldsymbol{not}}$ выполняется $p_{01}=p_{10}=p_{00}=p_{11}=1/2$. Понять, почему так происходит, можно, используя не сами вероятности, а *амплитуды вероятности* и диаграммную технику.

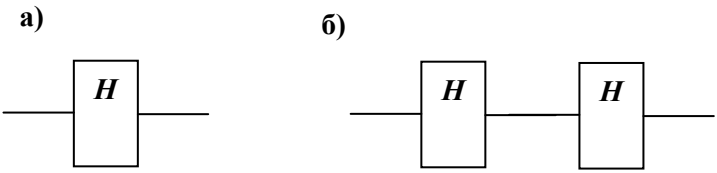


Рис. **1.63.** Квантовый элемент *Адамара*

Выводы (резюме) по разделу 1.4

1. **Под опытом** (*экспериментом*, *испытанием*) понимается некоторая воспроизводимая совокупность (комплекс) условий, в которых наблюдается то или другое явление, фиксируется тот или иной результат. Если при повторении опыта (комплекса условий) варьируется его результат (событие может произойти или не произойти), то говорят об *опыте со случайным исходом*.
2. Опыт может протекать независимо от человека. Человек выступает в роли наблюдателя или фиксатора происходящего, и от него зависит только решение, что наблюдать и какие параметры фиксировать (измерять).
3. Каждое осуществление ***комплекса условий*** называют реализацией. Этот комплекс условий не определяет всех необходимых требований, при которых осуществляется событие. Включены в него лишь основные требования, а второстепенные НЕ учитываются или НЕ могут быть учтены в силу различных причин и меняются от опыта к опыту.
4. **Случайным событием** (или просто событием) называют всякий факт, который в опыте со *случайным исходом* может произойти или не произойти, и обозначают прописными (большими) буквами латинского алфавита, например $\boldsymbol{A}$.
5. **Фундаментальные условия,** при которых определяются *случайные события,* это:
   - опыт можно повторять много раз;
   - исход опыта НЕпредсказуем;
   - относительная частота **случайного** события у с т о й ч и в а (при увеличении числа опытов она устойчиво колеблется около определенного значения – это определение не очень точно).
6. Если $P(\boldsymbol{A})=0$, то это еще не означает, что событие $\boldsymbol{A}$ является **НЕвозможным** событием; если $P(\boldsymbol{A})=0$, то событие может произойти, но вероятность этого есть НУЛЬ (так, если $\boldsymbol{A}$ – это событие есть попадание в точку из интервала (0,1)); из $P(\boldsymbol{A})=0$ следует только то, что при неограниченном повторении опытов (т.е. увеличении объема выборки) событие $\boldsymbol{A}$ будет появляться сколь угодно редко.

7. Если $P(\boldsymbol{A})=1$, то это еще не означает, что событие $\boldsymbol{A}$ является *достоверным* событием: например, если $\boldsymbol{A}$ – событие, состоящее в попадании в точку из интервала (0;4), то $P(\boldsymbol{A})=0$, но $P(\bar{\boldsymbol{A}})=1$, так как $P(\boldsymbol{A})+P(\bar{\boldsymbol{A}}) \equiv 1$ и $\bar{\boldsymbol{A}}$ есть **НЕдостоверное** событие, хотя $P(\bar{\boldsymbol{A}})=1$.
8. ***Несовместные* события** — несколько событий называются *несовместными* в данном опыте, если никакие два из них не могут появиться вместе.
9. **Зависимые события** — событие $\boldsymbol{A}$ называется *зависимым от события* $\boldsymbol{B}$, если вероятность события $\boldsymbol{A}$ меняется в зависимости от того, произошло событие $\boldsymbol{B}$ или нет, т.е. $P(\boldsymbol{A}|\boldsymbol{B}) \neq P(\boldsymbol{A})$.
10. **Независимые события** — два события называются НЕ*зависимыми*, если появление одного из них НЕ изменяет вероятности появления другого; несколько событий называются НЕ*зависимыми*, если любое из них НЕ зависит от любой совокупности остальных.
11. В теории вероятностей используют понятие пространства $\boldsymbol{\Omega}$ *элементарных событий*. Для этого все возможное множество исходов некоторого **опыта** представляют в виде *элементарных событий* так, чтобы все они были ***НЕсовместными*** событиями и при этом составляли *полную группу событий* (т.е. $P(\boldsymbol{\Omega}) \equiv 1$).
12. **Элементарное событие** — исходное понятие. В определении вероятностного пространства непустое множество $\boldsymbol{\Omega}$ называется *пространством элементарных событий*, а его любая точка $\omega \in \boldsymbol{\Omega}$ называется *элементарным событием*.
13. Каждый неразложимый исход эксперимента (опыта) представляется одним и только одним элементарным событием. Набор (т.е. множество или совокупность) всех **ЭС** в теории вероятностей принято называть пространством *элементарных событий.*
14. При неформальном подходе $\boldsymbol{\Omega}$ описывает множество всех исходов некоторого случайного эксперимента и ω соответствует элементарному исходу (эксперимент заканчивается **одним** и **только одним** элементарным исходом; эти исходы **неразложимы** и **взаимно исключают** друг друга).

15. При неформальном подходе исход испытания называется событием. Все те события, что могут произойти в результате выполнения комплекса условий, составляют *достоверное событие* **Ω**. Те из событий, что **нельзя разложить** на составляющие их события, есть *элементарные события*.
16. Любое событие ***B*** из *пространства элементарных событий* **Ω можно составить** из *элементарных событий*.
17. Каждый **неразложимый** исход (идеализированного) опыта представляется одним и только одним ЭС. Совокупность всех ЭС называют *пространством* ЭС, а сами ЭС называют **точками** этого пространства. Все события, связанные с данным опытом, могут быть описаны с помощью ЭС.
18. Теорема сложения. Вероятность появления одного из двух несовместных событий, безразлично какого, равна сумме вероятностей этих событий ■
19. Теорема умножения. Вероятность совместного появления двух событий равна произведению вероятности одного из них на условную вероятность другого, вычисленную в предположении, что первое событие уже наступило ■
20. Теория вероятностей позволяет решать задачи, связанные с нахождением вероятностей по известным формулам и доказанным теоремам.
21. С помощью теории вероятностей можно по заданным вероятностям *элементарных событий* вычислить вероятность некоторого конкретного сложного события. При этом на вопрос, откуда берутся сами вероятности *элементарных событий*, эта теория ответа не дает. В некоторых случаях эти вероятности можно получить с помощью другой теории — *математической статистики*.
22. Само *пространство* элементарных событий есть застывший и неизменный во времени набор элементарных событий. Диаграммная техника рассматривает происходящие процессы с системой, как развивающиеся во времени.
23. Суть метода **диаграммной техники** состоит в следующем. Водится понятие *системы* (или *модели*). Эта система (модель) может находиться в каких-то *состояниях*. Выделяют два состояния системы (модели): *начальное* и *конечное*. Происходит изменение состояния системы (модели) в ре-

зультате какого-то *процесса*. В конкретное состояние система (модель) может прийти различными путями (или *траекториями*). При вычислениях применяются два правила.

24. Правило 1.1. *Вероятность перехода системы по траектории из одного положения (состояния) в другое положение (состояние) равна* ***произведению*** *вероятностей всех процессов, связывающих между собой состояния, принадлежащие данной траектории* ■
25. Правило 1.2. *Вероятность перехода системы из начального положения (состояния) в конечное положение (состояние) равна* ***сумме*** *вероятностей переходов по всем возможным траекториям, связывающим эти положения (состояния)* ■
26. Диаграммная техника тесно связана с квантовыми вычислениями и особенно с *амплитудой вероятности*. Более сложное ее развитие связано с интегралами по траекториям, применяемыми в физике. Два последовательно соединенных *квантовых* элемента *Адамара* не приводят к такому же эффекту, как 2 вероятностных элемента ***R***. Понять, почему так происходит, можно, используя не сами вероятности, а *амплитуды вероятности* и диаграммную технику.
27. Предполагается, что состояния системы (кубика, монеты, диода, транзистора, триггера, элемента ИЛИ, комбинационной схемы, ЦВМ и т.п. объектов) — это все состояния именно *классической системы,* т.е. системы, подчиняющейся законам *классической физики*.
28. *Квантовый объект*, например одиночный кубит, может быть (как и ЛЭ ИЛИ) в *исправном* и в *неисправном* состоянии. Одиночный кубит как *квантовый объект* уже может находиться или в *чистом* состоянии или в *смешанном* состоянии. В чистом состоянии состояние кубита можно представить как *суперпозицию* других чистых состояний. Кубит может находиться в *базисном* состоянии. Если кубит не одиночный (т.е. имеется несколько кубитов или иными словами имеется уже *квантовая система*), то у кубита может возникнуть состояние, которое называется *сцепленным* (или перепутанным) состоянием.

1.5. Классический и квантовый алгоритмы

«…Какие еще задачи квантовые компьютеры могут решать быстрее, чем классические? Краткий ответ таков: мы не знаем. Разработать хороший квантовый алгоритм *трудно*.»

М. Нильсен, И. Чанг [**17**, с.26]

«Ключевое понятие информатики — *алгоритм*. Алгоритм — это точный рецепт выполнения какой-либо задачи.»

М. Нильсен, И. Чанг [**17**, с.163]

Содержание

Классический алгоритм. Квантовый алгоритм. Формальные признаки алгоритмов. Представление алгоритмов на практике. Программная и аппаратная реализация алгоритма. Эффективность алгоритма.

Понятие классического и квантового алгоритма

Само слово *алгоритм* — фонетическое трансформирование слова *аль Хорезми* (имени *Хорезми Мухаммед бен Муса* — узбекского математика и астронома IX в.). Сразу отметим [**95**, с. 16], что написание *алгори**ф**м* и *алгори**т**м* — это правильные написания (раньше было принято писать *алгорифм*, а сейчас — *алгори**т**м*).

Понятие *алгоритма* в самом общем виде относится к основным первоначальным понятиям математики, для него не допускаются определения в терминах более простых понятий [**93**, с. 202-206].

Возможные существующие уточнения понятия *алгоритма* приводят [**93**, с.205] к сужению такого понятия. В 1936 г. независимо и почти одновременно в работах *А. Черча*, *С.К. Клини, А.М. Тьюринга*, *Э.Л. Поста* была решена проблема уточнения общего понятия *алгоритма* [**92**, с. 10].

В работах *А.А. Маркова, А.Н. Колмогорова* и *В.А.Успенского* были разработаны важные уточнения понятия алгоритма.

Приведем далее только (выборочно) некоторые определения *алгоритма* и его важные свойства.

Определение 1.95

Алгоритм [**87**, с. 5] — это текст, который в определенных обстоятельствах может привести к однозначному развитию событий — процессу выполнения алгоритма.

Понятие алгоритма, определяемое требованиями (***а***), (***б***), (***в***), (*г*), (***д***), представленными ниже (как полагает известный специалист *А.И. Мальцев* в [**91**, с. 10]), является не строгим и называется *интуитивным*.

Свойство (***а***) (*А.И. Мальцев*)

Алгоритм [**91**, с. 10] — это процесс последовательного построения величин, идущий в дискретном времени таким образом, что в начальный момент задается исходная конечная система величин, а в каждый следующий момент система величин получается по определенному закону (программе) из системы величин, имевшихся в предыдущий момент времени (*дискретность алгоритма*).

Свойство (***б***)

Система величин [**91**, с. 10], получаемых в какой-то (не начальный) момент времени, однозначно определяется системой величин, полученных в предшествующие моменты времени (*детерминированность алгоритма*).

Свойство (***в***)

Закон [**91**, с. 10] получения последующей системы величин из предшествующей должен быть простым и локальным (*элементарность шагов алгоритма*).

Свойство (*г*)

Если способ [**91**, с. 10] получения последующей величины из какой-нибудь заданной величины не дает результата, то должно быть указано, что надо считать результатом алгоритма (*направленность алгоритма*).

Свойство (***д***)

Начальная система величин [**91**, с. 10] может выбираться из некоторого потенциально бесконечного множества (*массовость алгоритма*).

Определение 1.96 (*А.А. Марков*)
Алгорифм [**92**, с. 9] — точное предписание, определяющее вычислительный процесс, ведущий от варьируемых исходных данных к искомому результату.

Определение 1.97 (*А.А. Марков*)
Алгорифм [**92**, с. 135] есть предписание, однозначно определяющее ход некоторых конструктивных процессов.

Определение 1.98 (*Д.Э. Кнут*)
Алгоритм [**94**, с. 29-31] — не просто свод конечного числа правил, задающих последовательность выполнения операций при решении той или иной специфической задачи. Помимо этого, он имеет пять важных особенностей: *конечность*, *определенность*, *ввод*, *вывод*, *эффективность*.

ОТМЕТИМ. Понятие *алгоритма с оракулом* [**95**, с. 98-101] было также рассмотрено исследователями классических алгоритмов. Квантовые алгоритмы могут также содержать *оракул*, например, известный квантовый алгоритм поиска *Л. Гровера* [**17**, с. 311-314].

ОТМЕТИМ. Существуют *вероятностные* классические алгоритмы, у которых очередной шаг их работы (выполнения) зависит от некоторого *случайного* (псевдослучайного) числа. В каком-то смысле можно полагать, что специфические квантовые алгоритмы могут обладать некоторым свойством *вероятностных* классических алгоритмов.

Формальные признаки алгоритмов
Разные определения алгоритма в той или иной форме содержат некоторые общие требования, предъявляемые к алгоритму. Приведем наиболее важные из них:

- **Детерминированность** (определенность) [**94**, с. 30] — каждый шаг алгоритма должен быть точно определен; действия, которые необходимо произвести, должны быть строго и недвусмысленно определены в каждом возможном случае.

- **Завершаемость** (конечность) [**94**, с. 29] — алгоритм всегда должен заканчиваться после конечного числа шагов.

- **Массовость** — алгоритм можно применить к множеству входных данных (потенциально бесконечного множества).

ОТМЕТИМ. В зависимости от уточнения понятия алгоритма набор его признаков уточняется и корректируется.

В случае квантового алгоритма все гораздо сложнее. Теория квантовых алгоритмов пока еще не разработана так хорошо, как теория классических алгоритмов.

Точного исчерпывающего определения квантового алгоритма, наверное пока еще не существует.

Некоторые специалисты полагают [**17**, с.224], что квантовые алгоритмы должны удовлетворять дополнительному условию — квантовые алгоритмы должны быть лучше, чем известные классические алгоритмы.

Для того чтобы создавать хорошие квантовые алгоритмы на практике, разработчику необходимы [**17**, с.224] "*особая* интуиция и *особые* ухищрения".

Представление алгоритмов на практике

На практике алгоритмы представляют обычно следующим образом:

- в виде схем алгоритмов согласно ГОСТ 19.701-90 [**96**];
- в виде словесного описания;
- на специальном алгоритмическом языке;
- в виде специальных графических схем устройств.

ОТМЕТИМ. Квантовые алгоритмы обычно представляют в виде словесного описания и в виде квантовой схемы (например, как на рис. 1.48, 1.49). Для изображения квантовых схем используют *язык квантовых схем* [**17**, с.224].

Эффективность алгоритма

В кибернетике специалистами принято, что эффективность алгоритма можно оценивать по числу выполняемых им операций (шагов). При этом иногда существует известная проблема в выборе этих самых операций. Эффективность алгоритма можно оценивать числом самых трудоемких операций, а теми операциями, что требуют не очень значительных ресурсов — пренебрегать (т.е. просто не учитывать). Иногда для неучтенных операций пытаются дать некоторые оценки с известной точностью или просто верхние или нижние оценки. Другая проблема (в теории сложности вычислений [**17**, с. 185]) связана с тем, что на разных вычислительных средствах на практике может потребоваться и разный объем ресурсов (оперативной и внешней памяти, частота работы процессора, время решения задачи и т.п. ресурсы). Последняя проблема решается следующим образом. Пусть (см. [**17**, с. 185-186]) на вход вычислителя подают n битов данных. В теории сложности различают два существенно разных по эффективности класса задач по использованию для их решений ресурсов. Объем одних ресурсов (для задач 1-го класса) ограничен сверху некоторым многочленом от n (т.е. задача требует *полиномиальных* ресурсов), а объем других ресурсов (для задач 2-го класса) ограничен сверху некоторой функцией от n, которая растет быстрее, чем любой многочлен от n (т.е. задача требует *экспоненциальных* ресурсов). На практике (по аналогии с задачами и ресурсами для их решения) соответственно выделяют *полиномиальные* и *экспоненциальные* алгоритмы.

Определение 1.99

Задача *легкая*, *простая*, *решаемая* [**17**, с. 186] — если для ее решения существует *полиномиальный* алгоритм.

Определение 1.100

Задача *трудная*, *сложная*, НЕ*решаемая* [**17**, с. 186] — если для ее решения наилучший возможный алгоритм требует *экспоненциального* объема ресурсов.

ОТМЕТИМ [**17**, с. 186]. Деление задач на *полиномиальные* и *экспоненциальные* — грубая классификация. Так на практике решение некоторой задачи алгоритмом за $2^{n/1000}$ операций (т.е. алгоритм

экспоненциальный), может быть более предпочтительней, чем алгоритм ее решения за n^{1000} операций (так как только при большом числе n ($n \approx 10^8$) *полиномиальный* алгоритм становится предпочтительнее *экспоненциального* алгоритма).

Необходимо отметить первое очень важное обстоятельство. Исторически сложилось так [**17**, с. 186], что именно *полиномиальные* алгоритмы были существенно быстрее, чем *экспоненциальные* алгоритмы (при этом имеется малое число исключений в пользу *экспоненциальных* алгоритмов).

Второе, тоже очень важное, обстоятельство связано (как говорят специалисты [**17**, с. 186]) со следующей *сильной формой тезиса Черча-Тьюринга*.

Тезис Черча-Тьюринга (сильная форма)
Любая вычислительная модель может быть смоделирована на вероятностной машине Тьюринга с не более чем полиномиальным увеличением числа операций ■

Определение 1.101
Алгоритм из класса **BPP** [**33**, с. 55] — это такой эффективный (быстрый) алгоритм, который на любом входе дает правильный ответ с вероятностью, превышающей некоторый порог $\delta > 1/2$.

ОТМЕТИМ [**33**, с. 54-55]. В случае класса **BPP** (*вероятностное вычисление за полиномиальное время с ограниченной вероятностью ошибки*), в общем-то, нельзя проверить правильность ответа, но можно повторять вычисления k раз и брать в качестве окончательно ответа тот, который повторяется чаще других (увеличивая значение k, добиваются вероятности правильного ответа близкой 1 с заданной точностью). В теории вычислительной сложности полагают, что если задача из класса **BPP**, то она не сложна или *практически* разрешима, а если не из класса **BPP**, то эта задача трудная или НЕ*решаемая* на реальных вычислителях.

ВАЖНО ПОМНИТЬ (см. [**33**, с. 55]). В вероятностной машине (вычислителе) вероятность выхода получают с помощью *вероятностей*, а в квантовой машине (вычислителе) — *амплитуд* вероятностей.

В теории сложности рассматриваются следующие важные классы задач — **P**, **NP**, **PSPACE**, **NPI**, **BPP** и **BQP**. В несколько произвольной (грубой и неточной) форме эти классы кратко можно охарактеризовать следующим образом [**17**, с.66,67,198,202,255,338]:

- **P** — класс задач, которые можно быстро решить на классическом компьютере;
- **NP** — класс задач, *решения* которых можно быстро проверить на классическом компьютере (выделяют **NP**-полные задачи как подкласс задач **NP**; алгоритм решения конкретной **NP**-полной задачи может быть с небольшими издержками адаптирован для решения любой другой задачи из класса **NP**);
- **PSPACE** — класс задач, которые можно решить при использовании ресурсов, небольших по пространственному размеру («малый» компьютер), но не обязательно по времени (допустимы «длительные» вычисления);
- **BPP** — класс задач, которые можно решить с использованием вероятностных алгоритмов за *полиномиальное* время, если в решении допускается ограниченная вероятность ошибки (скажем, 1/4);
- **NPI** — промежуточный класс между **P** и **NP**-полными задачами, не являющимися ни разрешимыми за полиномиальное время, ни **NP**-полными (если сделать предположение, что $\mathbf{P} \neq \mathbf{NPI}$, то можно доказать, что существует непустой класс задач **NPI**);
- **BQP** — класс задач, которые можно решить с ограниченной вероятностью ошибки с помощью квантовой схемы полиномиального размера (**BQP** — квантовый аналог класса **BPP**).

ОТМЕТИМ [**17**, с. 67]. Задачи из класса **BPP** эффективно разрешимы на классическом вычислителе (компьютере). Полагают, что класс **PSPACE** строго больше, чем классы **P** и **NP** в совокупности (причем это пока не доказано).

ОТМЕТИМ [**17**, с. 66]. Класс **P** является подмножеством класса **NP** (поскольку предполагается, что сама возможность решения задачи подразумевает возможность самой проверки возможных решений). Пока неизвестно, можно ли квантовые вычислители (компьютеры) использовать для быстрого решения всех задач из класса **NP**.

ОТМЕТИМ [**17**, с. 197]. Ни про одну задачу пока не доказано, что она из класса **NPI**.

ВАЖНО ПОМНИТЬ [**33**, с. 57-58]. Классическая вероятностная машина (вычислитель) следует по *единственному* и случайно выбранному пути вычисления. Квантовый вычислитель (компьютер) может следовать по *многим* разным путям и притом одновременно, а сам выход определяется интерференцией всех этих путей.

Значительным результатом квантовой теории сложности является тот факт [**17**, с. 256-257], что **BQP** $\subseteq$ **PSPACE**, причем ясно, что **BPP** $\subseteq$ **BQP** и пока не известно, совпадают ли классы **PSPACE** и **BPP**. Если кому-нибудь удастся доказать, что **BPP** $\neq$ **BQP**, то это будет в общем означать, что квантовый вычислитель эффективнее классического.

На рис. 1.64 представлено условное изображение соотношения классов сложности между собой. Специалисты отмечают [**17**, с. 68], что пока неизвестно, как **BQP** соотносится с классами **P**, **NP** и **PSPACE**. Пока известно, что квантовый вычислитель способен эффективно решать все задачи из класса **P**. Можно полагать, что класс **BQP** расположен между **PSPACE** и **P** (см. рис. 1.64).

Класс задач **NPI** важен для исследования квантовых вычислений. Специалисты полагают [**17**, с. 198], что это связано с их желанием для задач не из класса **P** обнаружить быстрые квантовые алгоритмы, а также и то, что (как полагают многие) квантовые вычислители не смогут эффективно решать все задачи **NP**.

Для оценки эффективности квантовых алгоритмов будем выделять в них некоторые повторяющиеся элементы (циклы). В словесном описании квантового алгоритма повторяющиеся элементы — это число циклов (итераций), повторяющих одни и те же операции (шаги), а в виде квантовой схемы — это число повторяющихся одних и тех же квантовых элементов на изображении этой квантовой схемы. Например, в квантовой схеме, реализующей известный квантовый алгоритм поиска *Л. Гровера*, таким элементом является число возможных обращений к оракулу (или число итераций Гровера).

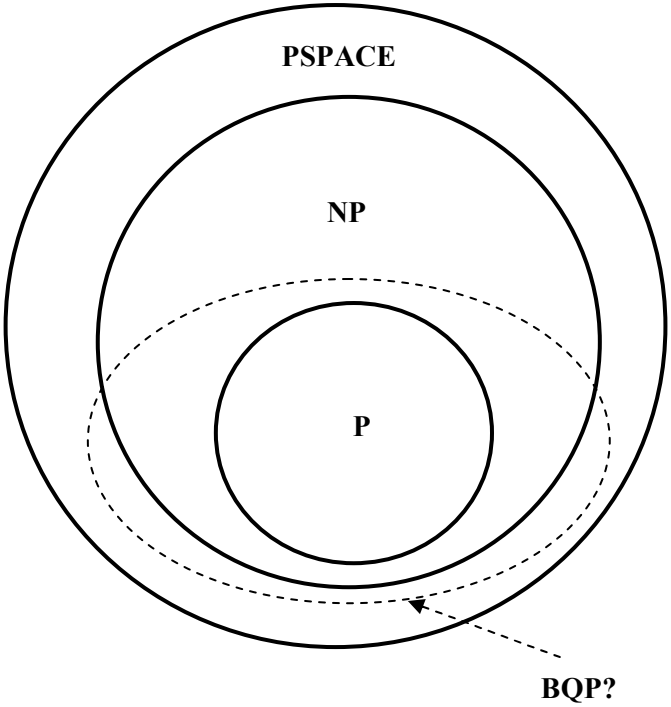


Рис. **1.64.** Классы сложности [**17**, с. 67]

Квантовые алгоритмы (т.е. квантовые схемы) могут давать конечный результат как с вероятностью 1, так и с вероятностью меньше 1. Например [**98**, с. 105], квантовый алгоритм поиска *Л. Гровера* работает так, что искомое состояние системы, удовлетворяющее условию поиска после выполнения измерения, будет определено с вероятностью, по крайней мере, не меньше чем 1/2. Это свойство квантовых алгоритмов делает их похожими на вероятностные алгоритмы. Однако в отличие от вероятностных алгоритмов, квантовые алгоритмы могут выполнять вычисления параллельно (им присущ так называемый **квантовый параллелизм** и **интерференция**, связанная с **амплитудами** вероятностей).

Программная и аппаратная реализация алгоритма

В кибернетике специалистами принято, что алгоритм может быть реализован на практике как *аппаратно*, так и *программно*.

В случае программной реализации по заданному алгоритму (который решает требуемую задачу) разрабатывают на выбранном языке программирования *программу*, реализующую этот алгоритм. Для того чтобы получить решение задачи, необходимо выполнить эту программу на некотором вычислительном средстве (например, ЭВМ), естественно, что вычислительное средство должно быть способно выполнять эту программу для получения требуемого конечного результата, а сама программа должна быть отлажена.

В случае аппаратной реализации по заданному алгоритму (который решает требуемую задачу) разрабатывают на выбранной технической базе *устройство*, реализующее этот алгоритм. Для того чтобы получить решение задачи, необходимо запустить это устройство (например, АВМ или реализованную (собранную) комбинационную схему на классических логических элементах) в действие (например, включить это устройство и подать входные воздействия), естественно, что устройство должно быть способно выполнять действия согласно алгоритму для получения требуемого конечного результата, а само устройство должно быть отлажено и работоспособно (исправно).

Рассмотрим следующий простой пример.

***Пример* 1.40**

Есть емкость с двумя кранами для заполнения ее жидкостью. Есть устройство, которое управляет этими двумя кранами и необходимые датчики, показывающее состояния кранов. Открыт должен быть только один кран или все краны должны быть закрыты (иначе через какое-то время может произойти авария). Краны могут независимо от устройства открываться, но при этом срабатывают датчики, по которым устройство может определить состояние крана и затем при необходимости закрыть его. Требуется предложить алгоритм ***Alg*1**, решающий эту задачу (алгоритм управления кранами). Необходимо реализовать ***Alg*1** аппаратно и программно и дать представление этого алгоритма несколькими способами.

Решение

1). Алгоритм ***Alg*1** управления кранами в виде *словесного описания* содержится в тексте условия данного примера. Перепишем его в следующем виде.

Шаг-1. Начать выполнять алгоритм.
Выяснить состояния кранов.

Шаг-2. По состоянию кранов принять решение по следующему правилу:
если закрыты 2 крана или открыт только 1 кран,
то перейти к Шагу-4;
если открыты 2 крана, то перейти к Шагу-3;

Шаг-3. Выдать сигнал о закрытии одного из кранов.

Шаг-4. Закончить выполнение алгоритма.

2). На рис. 1.65 представлена схема алгоритма ***Alg*1** в виде специально принятых графических символов.

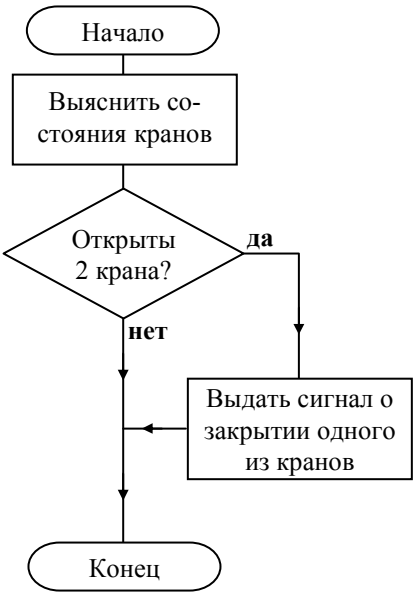


Рис. **1.65.** Схема алгоритма ***Alg*1**

3). Введем некоторую логическую переменную x_1 и свяжем с ней состояния 1-го крана, предаваемые датчиками. Если $x_1=0$, то 1-й кран закрыт, а иначе – открыт. Введем еще логическую пере-

менную x_2 и свяжем с ней состояния 2-го крана, предаваемые датчиками. Если x_2=0, то 2-й кран закрыт, а иначе – открыт.
Работа устройства описывается ЛФ $f(x_1, x_2)$ от двух переменных x_1 и x_2 со следующей таблицей истинности:

x_1	x_2	$f(x_1, x_2)$	**Примечание**
0	0	0	Краны не закрывать
0	1	0	
1	0	0	
1	1	1	Сигнал о закрытии одного из кранов

Выполним синтез комбинационной схемы, реализующей ЛФ с этой таблицей истинности. Получим (как ранее было описано) следующую формулу в виде СДНФ:

$$f(x_1, x_2) = \overline{x}_1 \,\&\, \overline{x}_2$$

и по ней комбинационную схему, представленную на рис. 1.66.

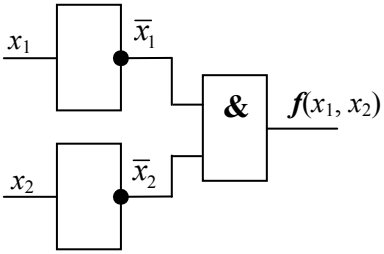


Рис. **1.66.** Схема устройства управления кранами

4). Программная реализация алгоритма ***Alg*1** в виде функции на языке Си [**97**] выглядит следующим образом:

```
Alg1{
        int i;

        i=kran();   /*выяснить число i открытых кранов*/

        if(i==2) zakritkran(1);   /*если i=2, то закрыть 1 кран*/
      }
```

5). Таким образом, получено словесное описание алгоритма, представлена схема этого алгоритма и его программная реализация, выполнен синтез устройства в виде комбинационной схемы.

6). И тем самым задача решена■

Далее во избежание возможных недоразумений (при рассмотрении уже конкретных квантовых алгоритмов) будем представлять квантовый алгоритм в виде некоторого словесного описания (без представления самой схемы алгоритма) с последующей его аппаратной реализацией на квантовых элементах (кубитах и гейтах). Под разработкой квантового алгоритма будем понимать разработку квантовой схемы, реализующей решение заданной задачи.

Выводы (резюме) по разделу 1.5

1. Понятие *алгоритма* (*алгори**ф**ма*) относится к основным первоначальным понятиям математики и не допускает определения в терминах более простых понятий. Уточнения понятия *алгоритма* приводят к сужению такого понятия.
2. **Алгорифм** — точное предписание, определяющее вычислительный процесс, ведущий от варьируемых исходных данных к искомому результату.
3. Алгоритмы представляют обычно в виде: словесного описания, специальных графических схем устройств, на специальном алгоритмическом языке, как схемы алгоритмов.
4. Алгоритм может быть реализован на практике как *аппаратно*, так и *программно*.
5. Точного исчерпывающего определения квантового алгоритма пока не существует. Квантовый алгоритм может давать конечный результат с вероятностью 1, или меньше 1.
6. Далее квантовый алгоритм будем представлять в виде словесного описания с последующей его аппаратной реализацией на кубитах и гейтах. Под разработкой этого алгоритма будем понимать разработку квантовой схемы (на *языке квантовых схем*), реализующей решение заданной задачи.
7. Классический вероятностный компьютер следует по *единственному*, случайно выбранному пути вычисления. Квантовый компьютер — *многими* разным путям одновременно.
8. Для оценки эффективности квантовых алгоритмов будем выделять в них повторяющиеся элементы (т.е. число повторяющихся одних и тех же квантовых элементов на изображении квантовой схемы).
9. Квантовые алгоритмы могут давать конечный результат как с вероятностью 1, так и с вероятностью меньше 1.

1.6. Квантовый компьютер. Сравнительная таблица

«Квантовый компьютер — это устройство, обрабатывающее информацию квантово-механическим когерентным способом.»

И. Чанг, Л. Вандерсипен, К. Жу, Д. Леюнг, С. Ллойд [**99**]

«…можно ли сделать какие-либо обобщения относительно производительности квантовых компьютеров по сравнению с классическими? Что именно делает квантовые компьютеры эффективнее классических, если, конечно, это на самом деле так? Задачи какого класса можно эффективно решать на квантовом компьютере и как этот класс соотносится с классом задач, эффективно решаемых на классическом компьютере? Одной из самых интригующих особенностей квантовых вычислений и квантовой информации является то, насколько *мало* известно об ответах на эти вопросы! Необходимость их лучшего понимания представляет собой великий вызов будущему.»

М. Нильсен, И. Чанг [**17**, с.27]

«…Именно это практическое применение квантовых компьютеров — взлом криптографических кодов — в значительной степени стимулировало интерес к квантовым вычислениям и квантовой информации.»

М. Нильсен, И. Чанг [**17**, с.31]

Содержание

Квантовый компьютер. Сравнительная таблица характеристик квантового и классического вычислителей. Краткий анализ признаков квантового вычислителя.

Идею квантовых вычислений впервые [**72**] предложил в 1980 г. российский математик *Ю.И. Манин* в работе [**87**]. Эта идея стала очень активно обсуждаться после того [**72**], как была опубликована в 1982 г. статья [**88**] американского физика-теоретика нобелевского лауреата *Р. Фейнмана.*

Понять идею квантового компьютера можно с помощью принципиальной схемы его работы, представленной на рис. 1.67.

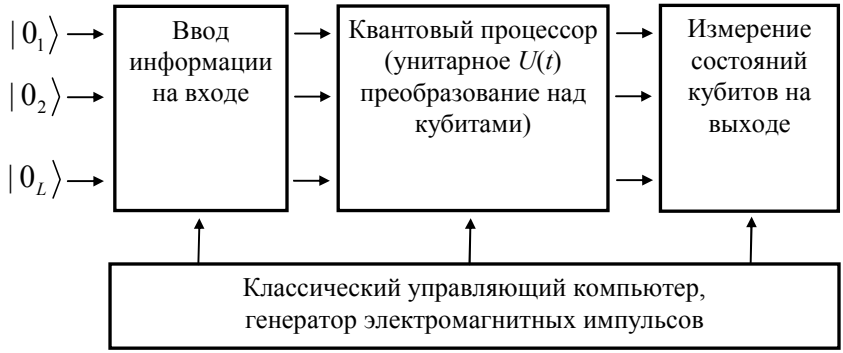


Рис. **1.67.** Схема квантового компьютера [**72**]

Квантовый компьютер содержит следующие основные блоки. Это квантовый регистр — набор из L кубитов. На рис. 1.67 кубиты представлены как $|0_i\rangle$, где i — это номер i–го кубита.

В начале (до операции ввода информации) все кубиты находятся в так называемом основном базисном состоянии $|0_1\rangle, |0_2\rangle, ..., |0_L\rangle$, т.е. если провести грубую аналогию с классическим компьютером, то все L триггеров установлены в 0 (т.е. содержат логические нули). Такая операция называется *инициализацией* квантового регистра, в результате которой приготовляется исходное базисное состояние.

Затем выполняется операция ввода требуемой информации в соответствии с той задачей, которую требуется решить. Для осуществления этого кубиты подвергаются некоторому селективному воздействию. Такое воздействие на практике может выполняться, например [**72**], посредством импульсов внешнего электромагнитного поля, путем управления этого воздействия уже с помощью традиционной классической ЭВМ (т.е. классическим управляющим компьютером, как показано на рис. 1.67).

Далее содержимое квантового регистра обрабатывается квантовым процессором путем выполнения последовательности *унитарных* преобразований (над содержимым квантового регистра) под управлением классической ЭВМ. По завершению всех унитарных преобразований квантовый регистр будет содержать уже новые

данные (т.е. кубиты будут в некотором измененном квантовом состоянии), которые и будут содержать результат квантовых вычислений. Отметим [**72**], что унитарная операция (преобразование) является элементарным шагом квантовых вычислений.

На завершающем этапе работы квантового компьютера выполняются измерения состояний кубитов квантового регистра. Поскольку измерение разрушает квантовое состояние, то на практике требуется каким-то образом собирать заданную статистику, например, путем многократного повторения квантовых вычислений с последующим измерением состояний кубитов на выходе (рис. 1.67).

Очень кратко суть квантовых вычислений можно представить как *инициализацию* квантового регистра, затем — запись в него исходных данных (в зависимости от решаемой задачи), после этого выполняются необходимые унитарные преобразования над содержимым квантового регистра и в заключение производятся измерения содержимого квантового регистра. В случае необходимости вся эта последовательность действий может повторяться несколько раз (для того чтобы набрать статистику) и затем уже делается вывод о полученном окончательном решении для данной задачи.

У квантового компьютера есть одна важная особенность, состоящая в следующем [**73**, с. 5]. Пока выполняются сами вычисления, доступ "квантового программиста" (исследователя) к их результатам ограничен. Для того чтобы осуществить доступ к результатам работы квантового компьютера, необходимо произвести специальный процесс *измерения*, который согласно квантовой механике воздействует на состояние квантовой системы (квантового регистра, кубита), искажая это состояние.

Согласно [**73**, с. 11] *Постулату измерения* в квантовой механике любое устройство (прибор) обладает *связанным ортогональным базисом*. Именно по отношению к этому базису и производится само квантовое измерение. Процесс измерения квантового состояния с помощью этого прибора (*измерителя*) преобразует его в какой-то один из *связанных* базисных векторов этого измерителя. Причем вероятность того, что квантовое состояние измерено именно как базисный вектор, есть квадрат нормы проекции первоначального состояния на этот базисный вектор. После измерения квантового состояния оно становится таким состоянием, каким оно

получилось в результате этого измерения. Пока первоначальное состояние не станет одним из базисных векторов *измерителя*, процесс измерения будет изменять состояние квантовой системы.

В классическом компьютере доступ к результатам не представляет серьезной проблемы. Действительно, классический программист может выводить на устройства отображения не только конечный результат, но и промежуточные результаты, что, в конечном счете, и используется при отладке программы и для устранения ошибок в ней.

Большинство квантовых алгоритмов содержат такие операции, как [**73**, с. 6] *последовательное преобразование квантового состояния,* за которым следует операция *измерения*.

Теория квантовых вычислений накладывает ограничения на преобразования, которые можно производить над кубитами. Так, все эти преобразования должны быть [**73**, с. 6] *обратимыми*. Специалисты [**73**, с. 6] полагают, что любой *классический* алгоритм можно сделать обратимым и затем выполнить его на квантовом компьютере за достаточно приемлемое время.

Состояние квантовой системы меняется не только из-за процесса измерения. Специалисты считают [**73**, с. 20], что любое *унитарное* преобразование соответствует допустимой эволюции квантовой системы и наоборот. Поэтому в квантовых вычислениях будут рассматриваться именно *унитарные* преобразования, которые можно описать с помощью унитарных матриц.

Квантовые логические элементы (гейты) выполняют именно унитарные преобразования, поэтому с такими элементами можно связать (поставить в соответствие) соответствующие унитарные матрицы. В классической ЭВМ логическому элементу соответствовала также своя матрица — таблица истинности.

Квантовый вычислитель выполняет квантовые вычисления с помощью квантовой сети из гейтов, реализующих унитарные преобразования. В некотором приближении это похоже на нейронную сеть нейрокомпьютера или на комбинационную схему с триггерами классической ЭВМ.

Далее будем полагать, что квантовый алгоритм представлен именно квантовой схемой.

На рис. 1.68 представлена квантовая схема для реализации квантового алгоритма, обменивающая состояния двух кубитов на трех

элементах (гейтах) CNOT [**17**, с.45], а также использующая 2 измерителя. В результате работы этой схемы верхний кубит, содержащий $|a\rangle$, будет содержать $|b\rangle$, а нижний кубит, содержащий $|b\rangle$, будет содержать $|a\rangle$.

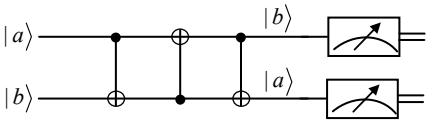


Рис. **1.68.** Пример квантовой схемы для обмена 2-х кубитов

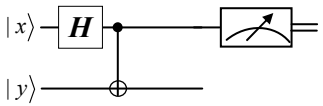


Рис. **1.69.** Пример квантовой схемы, создающей состояния Белла

На рис. 1.69 представлена квантовая схема для реализации квантового алгоритма, создающая состояния Белла (ЭПР-состояния) для 2-х кубитов [**17**, с.49], а также использующая однокубитовый гейт Адамара ***H***, гейт CNOT и один измеритель.

В табл. 1.27 представлены отличительные признаки 2-х вычислителей. Эта таблица подводит некоторый важный итог рассмотренным выше предварительным сведениям из кибернетики, необходимым для понимания квантовых вычислений.

Вдумчивый и настойчивый читатель уже подготовлен к тому, чтобы начать воспринимать далее более сложные для понимания сведения из квантовой механики, необходимые для изучения основных идей работы квантового вычислителя.

Дальнейшая главная задача — научиться понимать подобные квантовые схемы (см. рис. 1.68, 1.69), уметь выполнять их *анализ* и *синтез*.

Для того чтобы понимать квантовые схемы, необходимо владеть основными знаниями теории квантовой механики, которые будут кратко рассмотрены далее. Разбор известных квантовых алгоритмов позволит еще глубже вникнуть в суть проблемы квантовых вычислений.

Таблица 1.27. Сравнительные характеристики двух разных вычислителей (квантового и классического вычислителя)

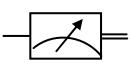
Признак (характеристика)	Вычислитель		Примечание
	Классический	**Квантовый**	
Измерение	Осциллограф, вольтметр, индикаторы, светодиоды и т.п.	Измеритель 	Приборы для определения состояния элемента (триггера, кубита), системы
Конечный результат работы	Это измерение выхода ЛЭ, *комбинационной схемы* (КС); повторные измерения не изменяют их состояние и не разрушают физические процессы, протекающие в их физической реализации	Это всегда измерение состояния квантового регистра; процесс ***измерения*** разрушает текущее состояние квантового объекта (системы), используемого для физической реализации ЛЭ (гейта)	Разный подход к получению конечного результата
Промежуточный результат работы	Получить возможно; выполняют при отладке схемы	Получение затруднено, вызывает проблемы, связанные с разрушением текущего состояния квантового объекта (системы)	Разные возможности в получении промежуточного результата
Таблица вход-выход	Таблица истинности	Унитарная матрица	Аналогом таблицы истинности для гейта является *унитарная матрица*

Таблица 1.27(продолжение)

Аналитическое представление преобразования вход-выход	Формула ЛФ	Умножение вектора на унитарную матрицу	Для аналитического представления преобразования *вход-выход* используется разный математический аппарат
Преобразование вход-выход	Логическая функция (ЛФ)	Унитарное преобразование (УП)	Вычисление значения выхода по входу выполняют разными инструментами (ЛФ или УП)
Элементы	Логические элементы (ЛЭ): ИЛИ-НЕ, И-НЕ, И, ИЛИ, другие	Гейты: CNOT, *вентиль Тоффоли*, *Фредкина* и другие гейты [**17**, с.15-17]	Логические элементы собранные в сеть позволяют выполнить требуемые вычисления
Реализация элементов	ЛЭ реализуют различными способами, с помощью переключателей, диодов и т.п.	Гейты реализуют на ионных ловушках и другим образом	В зависимости от реализации различают квантовые и классические логические элементы
Нетривиальный элемент	Существует только один нетривиальный однобитовый элемент НЕ [**17**, с.40]	Есть много нетривиальных элементов НЕ (т.е. NOT) [**17**, с.40]	Наличие многих нетривиальных элементов позволяет эффективнее выполнять вычисления
Элемент хранения единицы данных (информации)	***RS*** триггер и другие триггеры	Квантовый триггер (кубит)	Квантовый объект может быть в *суперпозиции,* а ***RS*** триггер — нет. Система кубитов может быть в *перепутанном* состоянии
Регистр	Классический регистр, содержит ***RS*** триггеры	Квантовый регистр содержит *квантовые триггеры* (кубиты)	Устройство для хранения данных

Таблица 1.27 (продолжение)

Информация	Классическая информация (подчиняется законам классической физики) [**19**]	Квантовая информация (подчиняется законам *квантовой механики*) [**19**]. Это общее название для вех видов деятельности, связанных с обработкой информации на основе *квантовой механики* и обозначает изучение элементарных задач по обработке *квантовой информации* [**18**, с.78-80]	Специалисты полагают, что *квантовая теория информации* шире *классической теории информации* [**18**, с.79]. Специалисты полагают [**17**, с.659], что *квантовая теория информации* имеет принципиальную особенность, состоящую в том, что сами квантовые состояния рассматриваются именно как *информация* и при этом изучаются с теоретико-информационной точки зрения.
Измерение информации	**Бит** — количество информации в ответе на вопрос, допускающий два равновероятных ответа [**1**, с.200]. Количество информации измеряется энтропией (например, в битах)	**Кубит** (*qubit* – quantum bit) — квантовый объект. Количество информации, представленной кубитом, *если мы не измеряем его*, определить не так просто [**17**, с.36]	Принципиально разный смысл вкладывается в *кубит* по сравнению с *бит* и разный подход к измерению количества информации
Состояние	Используются классические состояния	Используют квантовые состояния	Наличие квантовых состояний позволяет эффективно выполнять вычисления

Таблица 1.27 (продолжение)

Вычислительный базис(ВБ)	Иногда принято, что напряжение +(2.4÷5) вольта соответствует **1**, а напряжение, не превышающее +0.5 вольт — **0** [**39**, с.98]	Специальные состояния $\|0\rangle$ и $\|1\rangle$ – состояния ВБ, которые образуют ортонормированный базис векторного пространства [**17**, с.34]	ВБ – это те (обычно два) устойчивые состояния некоторой физической системы, которые приняты для физической реализации на практике **0** или **1**
Базис как система логических функций	Базисом является функция Пирс (ИЛИ-НЕ) или функция Шеффера (И-НЕ) [**30**, с.51]	Базисом является набор из однокубитовых гейтов и элемента CNOT [**17**, с.244]	Наличие такого базиса позволяет потенциально реализовать заданное действие (логическую функцию или унитарное преобразование)
Число входов и выходов	ЛЭ может иметь число входов, не совпадающих с числом выходов	У гейта число входов всегда равно числу выходов	Для обратимости в общем-то необходимо совпадение числа входов и выходов
Схема устройства	Цифровая схема, комбинационная схема	Квантовая схема, составленная по особым правила [**17**, с.45-47]	Есть различия в интерпретации схем, но есть и много общего
Аналоговое, цифровое	Может быть как ЦВМ, АВМ или как ГВМ	Квантовый вычислитель (КВ) в некотором смысле можно (с осторожностью) полагать, что он есть ГВМ	В КВ одна информация представлена дискретно в виде отдельных (дискретных) *кубитов*, а другая — непрерывно в виде непрерывных амплитуд вероятностей

Таблица 1.27 (окончание)

Обратимость вычислений	Обычно не обратим	Обратим (унитарные квантовые элементы всегда обратимы [**17**, с.44])	Обратимость вычислений позволяет снизить выделение тепла
Вычисление вероятности	Используют теорию вероятностей	Используют понятие амплитуды вероятности и диаграммную технику	В квантовом случае используют дополнительные правила вычисления вероятности
Вид результата	Детерминированный алгоритм дает однозначный результат, а вероятностный — с какой-то вероятностью	Результат может быть получен как с вероятностью 1, так и меньше 1	В отличие от вероятностных алгоритмов квантовым алгоритмам присущ квантовый параллелизм и интерференция
Исход эксперимента (опыта)	Каждый неразложимый исход опыта представляется одним и только одним элементарным событием ω (ЭС) из $\mathbf{\Omega}$ (пространство ЭС) [**35**, с.16]. Опыт заканчивается *одним* и *только одним* ЭС; эти ЭС *неразложимы и взаимно исключают* друг друга [**50**, с. 816]	Используется понятие НЕ*различимости* альтернатив [**90**, с.237] или *интерферирующих* альтернатив [**62**, с.25-31]	В квантовом случае используют дополнительно еще НЕразличимые (*интерферирующие*) альтернативы

На этом закончим рассмотрение предварительных необходимых и важных сведений из кибернетики и перейдем в книге 2 к более подробному изучению самих основ квантовых вычислений, используемых в квантовом компьютере.

Задачи

a) Придумайте задачи на применение диаграммной техники. Постарайтесь, чтобы эти задачи были по возможности оригинальными (необычными). Постарайтесь решить их. Сформулируйте трудности, которые встретились на пути к этому решению. Дайте анализ возникшим трудностям.

b) Придумайте для задачи (с правильным решением) ее неправильное решение на применение диаграммной техники. Дайте сравнительный анализ этих решений.

c) Используя диаграммную технику, решить следующую задачу. На вход радиолокационного устройства с вероятностью $\boldsymbol{p}$ поступает смесь полезного сигнала с помехой, а с вероятностью $(1-\boldsymbol{p})$ — только одна помеха. Если поступает полезный сигнал с помехой, то устройство регистрирует наличие какого-то сигнала с вероятностью $\boldsymbol{p_1}$; если только помеха, то устройство регистрирует наличие какого-то сигнала с вероятностью $\boldsymbol{p_2}$. Известно, что устройство зарегистрировало наличие какого-то сигнала. Найти вероятность того, что в его составе имеется полезный сигнал (см. [**59**, с. 69] задача №3.33. Ответ: $\boldsymbol{pp_1}/[\boldsymbol{pp_1}+(1-\boldsymbol{p})\,\boldsymbol{p_2}]$).

d) Используя диаграммную технику, решить следующую задачу. Юноша собирается сыграть 3 теннисных матча с родителями на пари. По условиям пари он должен победить 2 раза подряд. Порядок матчей может быть следующим: **I)** отец – мать – отец; **II)** мать – отец – мать. Юноше нужно решить, какой порядок для него предпочтительней, учитывая, что отец играет лучше матери (см. [**35**, с. 46] пример №2.12. Ответ: порядок **II)** предпочтительней).

e) Три стрелка произвели залп, причем две пули поразили мишень. Найти (используя диаграммную технику) вероятность того, что третий стрелок поразил мишень, если вероятности попадания в мишень первым, вторым и третьим стрелками соответственно равны 0.6; 0.5 и 0.4 (см. [**44**, с. 36] задача №107. Ответ: $10/19\approx 0.526$).

f) Решить задачу из *Примера* **1.23** с применением диаграммной техники.

g) Решить задачу из *Примера* **1.24** с применением диаграммной техники.

h) Решить задачу из *Примера* **1.25** с применением диаграммной техники.

i) Решить задачу из *Примера* **1.26** с применением диаграммной техники.

j) Четыре буквы разрезной азбуки **М**, **м**, **а**, **а**, из которых только одна буква **М** прописная, а все остальные буквы строчные, наудачу (т.е. случайно) извлекаются из мешка одна за другой. Требуется (используя диаграммную технику) найти вероятность появления слова **Мама** (см. [**35**, с. 45-46], задача №2.8. Ответ: $1/12 \approx 0.08333$).

k) Используя диаграммную технику, определить вероятность того, что при 3-х бросках кубика (правильной игральной кости) хотя бы один раз выпадет шестерка (см. [**35**, с. 54], задача №2.13. Ответ: $91/216 \approx 0.4213$).

l) Решить задачу из *Примера* **1.39** с применением диаграммной техники при условии что $\boldsymbol{p_{01}}=0.2$; $\boldsymbol{p_{00}}=0.8$; $\boldsymbol{p_{10}} = 0.3$; $\boldsymbol{p_{11}} =0.7$.

Список используемой литературы (источники)

1. Тарасов Л.В. Закономерности окружающего мира. В 3 кн. Кн.2: Вероятность в современном обществе.–М.:ФИЗМАТЛИТ, 2004.–360с.

2. Мишулина О.А. Основные понятия статистической теории информации.–М.:МИФИ, 2000.–92с.

3. Шеннон К. Работы по теории информации и кибернетики.–М.:Иностранная литература, 1963.–829с.

4. Яглом А.М., Яглом И.М. Вероятность и информация.–М.:Наука, 1973.–512с.

5. Петрович Н. Т. Люди и биты. Информационный взрыв: что он несет. – М.: Знание, 1986. –(см. http://n-t.ru/ri/pt/lb03.htm).

6. Стратонович Р.Л. Теория информации.–М.:Советское радио, 1975.–424с.

7. Чурсин Н. Н. Популярная информатика. –К.: Техника, 1982. –(http://n-t.ru/ri/ch/pi02.htm).

8. Информатика. Базовый курс /Под ред. В.С. Симоновича.–СПб.:Питер, 2005.–640с.

9. Винер Н. Кибернетика, или управление и связь в животном и машине. – 2-е изд. –М.: Наука; Главная редакция изданий для зарубежных стран, 1983.-344с. –(см. http://ihtik.lib.ru/dreamhost_anytehnika_8janv2007.html; http://grachev62.narod.ru/Cybern/contents.htm).

10. ГОСТ 7.0-99. Межгосударственный стандарт. Система стандартов по информации, библиотечному и издательскому делу. Информационно-библиотечная деятельность, библиография. Термины и определения.– Взамен ГОСТ 7.0-84, ГОСТ 7.26-80; Введен с 01.07.2000.–Минск: ИПК Изд. стандартов, 1999.–23с.

11. ГОСТ 7.73-96. Межгосударственный стандарт. Система стандартов по информации, библиотечному и издательскому делу. Поиск и распространение информации. Термины и определения.–Взамен ГОСТ 7.27-80; Введен с 01.01.1998.–Минск: ИПК Изд. стандартов, 1997.–19с.

12. Воройский Ф.С. Информатика. Новый систематизированный толковый словарь-справочник (введение в современные информационные и телекоммуникационные технологии в терминах и фактах).–М.: ФИЗМАТЛИТ, 2003.–760с.

13. Лопатников Л.И. Экономико-математический словарь.–М.:Наука, 1987.–509с.

14. Терминологический словарь по научной информации (1281 термин на 8 языках).–М.:ВИНИТИ 1966.–507с.

15. Мартин Дж. Организация баз данных в вычислительных системах. – М.:Мир, 1980.–662с.

16. ГОСТ Р 51275-99. Государственный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на Информацию. Общие положения.–Введен впервые; Введен с 01.01.2000.–М.: ИПК Изд. стандартов, 2004.–9с. –(http://protect.gost.ru/v.aspx?control=7&id=131855).
17. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация.–М.: Мир, 2006.–824с.–(Nielsen M.A., Chuang I.L. Quantum Computation and Quantum Information.–M.: Cambridge University Press, 2000.–704p.).
18. Физика квантовой информации /Под ред. Д. Боумейстера, А. Экерта, А. Цайлингера /Пер. с англ.–М.: Постмаркет, 2002.–376с.
19. Нильсен М. Правила для сложного квантового мира // В мире науки.–2003. –№3(март).–(http://www.sciam.ru/2003/3/inform.shtml).
20. Вентцель Е.С. Теория вероятностей.–М.:Высшая школа, 2001.–576с.
21. Фейнман Р. Характер физических законов /Пер. с англ.-2-е изд. испр.–М.:Наука, 1987.–160с.
22. Колмогоров А.Н. Три подхода к определению понятия количество информации //Проблемы передачи информации т.I, вып.1, 1965, с. 3–11.–(Новое в жизни, науке, технике. Сер.: Математика, кибернетика №1, 1991, с.24-29).–(http://www.kolmogorov.info/tri_podhoda.html).
23. Стенограмма доклада А. Н. Колмогорова «Понятие «информация» и основы теории вероятностей».–(Колмогоров и кибернетика /Редакторы-составители: Д. А. Поспелов, Я. И. Фет.–Новосибирск: ИВМиМГ (ВЦ) СО РАН, 2001. – 159 с.).–(http://mmedia.nsu.ru/infohistbd/CGI/BROKER.EXE?EL=3145+MODE=VIEW+PARAM=BOOK_INTERFACE).
24. Данилов Ю.А. Джон фон Нейман. –Новое в жизни науки и техники. Знание. Сер.: Математика, кибернетика, №4, 1981. –(http://ega-math.narod.ru/Reid/Neumann.htm).
25. Яковлев В.П., Кондрашин М.П. Элементы квантовой информатики.–М.: МИФИ, 2004.–80с.
26. Килин С.Я. Квантовая информация //Успехи физических наук, 1999.–Т.169.–№5.–с.507–527.–(http://www.symplex.ru/shop.php?cid=122; http://www2.symplex.ru/16/4/KKI_1999.djvu).
27. Дьюдни А. К. Еще раз об аналоговых устройствах //В мире науки, 1985.–№8.–с.91-97.–(http://www.symplex.ru/shop.php?cid=122; http://www2.symplex.ru/16/4/KKI_1999.djvu).
28. Ермолин А. Как добывают знания // Путеводитель В МИРЕ НАУКИ для школьников. Ресурсы сайта (Математика), 1999.–(http://ermine.narod.ru/MATH/STAT/KNMINING/knowledge_mining.htm).
29. Мигдал А.Б. Квантовая физика для больших и маленьких.–М.:Наука, 1989.–144с.

30. Семененко В.А., Скуратович Э.К. Арифметико-логические основы компьютерной схемотехники.–М.: Академический проект, 2004.–144с.
31. Савельев А.Я. Арифметические и логические основы цифровых автоматов.–М.: Высшая школа, 1980.–255с.
32. Керного В.В., Бабушкин Ю.М. Математические машины непрерывного действия. –Минск: Вышэйшая школа, 1968.–284с.
33. Дойч Д., Экерт А., Лупачини Р. Машины, логика и квантовая физика //*Математическое* просвещение, 2001. – Сер.3 –Вып.5. – С.47-60.).– (http://files.school-collection.edu.ru/dlrstore/d62fb03e-a780-11dc-945c-d34917fee0be/index.html).– (Deutcsh D., Ekert A., Lupacchini R. Machines, Logic and Quantum Physics //arXiv:math.HO/9911150, v.1, 19 Nov., 1999.– (http://quantum3000.narod.ru/papers/edu/deutcsh_machines.zip).
34. Кулик С.Д. Теория принятия решений (элементы теории проверки вероятных гипотез): учебное пособие.–М.: МИФИ, 2007.–152с.
35. Никитин Н.В., Уваров А.Ю. Диаграммная техника в теории вероятностей: учебное пособие.–М.: МИФИ, 1994.–64с.
36. Japanese Platinum. Образовательная коллекция [электронный ресурс] /1С, ММТ, ДО.– Электр. дан., прог. 2003.–1 CD-ROM диск.–Загл. с этикетки диска.–(Мультимедийные курсы иностранных языков. Программа комплексного обучения японскому языку.)
37. Фомичев В.С. Формальные языки, грамматики и автоматы.– (http://www.eltech.ru/misc/LGA_2007_FINAL/Index.html).
38. Интегральные микросхемы. Справочник /Под ред. Б.В. Тарабрина.–М.: Радио и связь, 1983.–528с.
39. Лыскова В.Ю., Ракитина Е.А. Логика в информатике. Методическое пособие.–М.: Лаборатория Базовых Знаний, 2004.–160.
40. Дрибинская И. Г. Арифметические устройства. Сумматоры.– http://school.ort.spb.ru/library/koi/v_sum.htm.
41. Аналоговые и цифровые интегральные микросхемы Справочное пособие /Под ред. С.В. Якубовского.–М.: Радио и связь, 1985.–432с.
42. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения.–М.:Наука, 1988.–480с.
43. Феллер В. Введение в теорию вероятностей и ее приложения. В 2 т.– Т.1.–М.:Мир, 1984.–528с.
44. Гмурман В.Е. Руководство к решению задач по теории вероятностей и математической статистике.–М.:Высш. школа, 1979.–400с.
45. Скворцов В.В. Теория вероятностей? — это интересно!–М.:Мир, 1993.–120с.
46. Севастьянов Б.А. Вероятностные модели.–М.:Наука, 1992.–176с.
47. Хелстром К. Квантовая теория проверки гипотез и оценивания.–М.: Мир, 1979.–344с.

48.Колмогоров А.Н. Основные понятия теории вероятностей.–М.:ФАЗИС, 1998.–142с.
49. Левин Б.Р. Теоретические основы статистической радиотехники.–3-е изд. перераб. и доп.–М.: Радио и связь.–1989.–656с.
50. Вероятность и математическая статистика: Энциклопедия.— М.:Большая Российская Энциклопедия, 1999.–910с.
51. Смирнов Н.В., Дунин-Барковский И.В. Краткий курс математической статистики для технических приложений.–М.:Физматгиз,1959.–436с.
52. Хинчин А.Я. Математические основания квантовой статистики.–М.:ГИТТЛ,1951.–256с.
53. Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся втузов.–М.:Наука, 1986.–544с.
54. Гнеденко Б.В. Очерк по истории теории вероятностей.–М.:УРСС, 2001.–88с.
55. Шведов А.С. Теория вероятностей и математическая статистика: Учебное пособие для вузов.–М.:Изд. дом ГУ ВШЭ, 2005.–254с.
56. Белько И.В., Свирид Г.П. Теория вероятностей и математическая статистика. Примеры и задачи.–Минск.:Новое знание, 2002.–251с.
57. Тернер Д. Вероятность, статистика и исследование операций: Пер. с англ. /Под ред. А.А. Рывкина.–М.:Статистика, 1976.–432с.–(Сер.:Библиотечка иностранных книг для экономистов и статистиков).
58. Мишулина О.А. Вероятностные основы кибернетики (часть 1).–М.:МИФИ, 1973.–100с.
59. Вентцель Е.С., Овчаров Л.А. Прикладные задачи теория вероятностей.–М.: Радио и связь, 1983.–416с.
60. Гмурман В.Е. Теория вероятностей и математическая статистика.–М.:Высш. школа, 2001(2003).–400(479)с.
61. Надежность и эффективность в технике: Справочник. В 10 т. Том 2.–М.: Машиностроение, 1987.–280с.
62. Фейнман Р., Хибс А. Квантовая механика и интегралы по траекториям.–М.:Мир, 1968.–383с.
63. Надежность и эффективность в технике. Справочник в 10 т. Том 1: Методология. Организация. Терминология.–М.: Машиностроение, 1986.–224с.
64. Анисимов А.В., Артамонов А.Б., Лебедев А.Н. и др. Аналоговые и гибридные вычислительные машины.–М.: Высшая школа, 1984.–320с.
65. Виттенберг И.М., Левин М.Г., Шор И.Я. Программирование аналого-цифровых вычислительных систем: Справочник.–М.: Радио и связь, 1989.–288с.
66. Пейтон А. Дж., Волш В. Аналоговая электроника на операционных усилителях.–М.: БИНОМ, 1994.–352с.

67. Каташкин В.И., Каташкина Л.Н., Огородова И.К., Соловьев Л.С., Суханов А.А., Чалый В.Д. Программирование АВМ при решении обыкновенных дифференциальных уравнений.–М.: МИФИ, 1976.–114с.
68. ГОСТ 23335-78, ГОСТ 23335-78. Государственные стандарты СССР. Машины вычислительные аналоговые и аналого-цифровые. Обозначения уловные графические элементов и устройств в схемах моделирования. Правила выполнения схем моделирования.–Введен с 01.01.1980.–М.: Изд. стандартов, 1979.–12с.
69. Математическая энциклопедия.–М.:Советская энциклопедия, 1982.–Т.3.–(ст. Множеств теория).
70. Паун Г., Розенберг Г., Саломаа А. ДНК-компьютер. Новая парадигма вычислений.–М.:Мир, 2004.–528с.
71. Фейнман Р. Квантовомеханические компьютеры //Квантовый компьютер и квантовые вычисления /Пер. с англ. под ред. В.А. Садовничего.–Ижевск: Ред. журн. Регулярная и хаотическая динамика, 1999.–Т2.–С.125–156.
72. Валиев К.А., Кокин А.А. От кванта к квантовым компьютерам// Природа, 2002.–№12. –С.28-34.–(http://vivovoco.rsl.ru/VV/JOURNAL/NATURE/12_02/28-36_02-12.PDF).
73. Риффель Э., Полак В. Основы квантовых вычислений //Квантовые компьютеры и квантовые вычисления, 2000.–Том 1.–№1.–С.4-57.–(http://ics.org.ru/rus?menu=mi_pubs&abstract=247).
74. Кулик С.Д. Схемотехнические решения для реализации квантового компьютера //Научная сессия МИФИ-2006. Сборник научных трудов в 16 т. Т.12:Информатика и процессы управления. Компьютерные системы и технологии.–М.: МИФИ, 2006.–Т.12.–С.52-53.
75. Кулик С.Д. Квантовая программа, квантовая база данных и квантовый компьютер //Научная сессия МИФИ-2007. Сборник научных трудов в 17 т. Т.12:Информатика и процессы управления. Компьютерные системы и технологии.–М.: МИФИ, 2007.–Т.12.–С.101-103.
76. Кулик С.Д. Реализация идеи алгоритма Гровера в виде квантовой программы на языке **QL+** для квантового компьютера //Научная сессия МИФИ-2008. Сборник научных трудов в 15 т. Т.13:Автоматизированные системы обработки информации и управления. Электронные измерительные системы.–М.: МИФИ, 2008.–Т.13.–С.78-80.
77. Кулик С.Д. Свидетельство на программу Российской Федерации №2007614120 “Квантовая программа v.1.0” (**SBella**)/ С.Д. Кулик (Россия).–Заявка №2007613120; Заяв. 31.07.2007; Зарегистр. 26.10.2007; Опубл. Бюл. №4(61).–Ч.2.–С.303.– (РОСПАТЕНТ).
78. Кулик С.Д. Свидетельство на базу данных Российской Федерации №2007620341 "Квантовая база данных v.1.0" (**Q-DB**)/ С.Д. Кулик

(Россия). – Заявка № 2007620244; Заяв. 07.08.2007; Зарегистр. 05.10.2007; Опубл. Бюл. №1(62).–С.269.–(РОСПАТЕНТ).
79. Галушкин А. И. Нейрокомпьютеры и их применение на рубеже тысячелетий в Китае. В 2-х томах. Т.1. – М.: Горячая линия–Телеком, 2004. – 367с. – (Серия: Нейрокомпьютеры и их применение. Вып. 12).
80. Галушкин А. И. Нейрокомпьютеры и их применение на рубеже тысячелетий в Китае. В 2-х томах. Т.2. – М.: Горячая линия–Телеком, 2004. – 464с. – (Серия: Нейрокомпьютеры и их применение. Вып. 12).
81. Галушкин А.И. Теория нейронных сетей: Учебное пособие для вузов.–М.:ИПРЖР, 2000.–416с.–(Нейрокомпьютеры и их применение. Кн.1).
82. Галушкин А.И. Нейронные сети: история развития теории: Учебное пособие для вузов.–М.:ИПРЖР, 2001.–840с.–(Нейрокомпьютеры и их применение. Кн.5).
83. Нейрокомпьютеры в информационных и экспертных системах. Кн. 27 /Под ред. А.И. Галушкина и С.Д. Кулика.–М.: Радиотехника, 2007.–120с.
84. Кулик С.Д. Биометрические системы идентификации личности для автоматизированных фактографических информационно-поисковых систем //Нейрокомпьютеры: разработка и применение.–М.: Радиотехника, 2003.–№12.–С.52-65.
85. Кулик С.Д. Применение нейронных сетей в автоматизированных фактографических информационно-поисковых системах //Нейрокомпьютеры: разработка и применение.–М.: Радиотехника, 2002.–№5-6. – С.3-12.
86. Вентура Д., Мартинец Т. Квантовая ассоциативная память //Нейрокомпьютеры: разработка и применение.–М.: Радиотехника, 2002. –№9-10. – С.34-53.
87. Манин Ю.И. Вычислимое и невычислимое.–М.:Советское радио, 1980.–128с.
88. Фейнман Р. Моделирование физики на компьютерах //Квантовый компьютер и квантовые вычисления /Пер. с англ. под ред. В.А. Садовничего.–Ижевск: Ред. журн. Регулярная и хаотическая динамика, 1999.–Т.2. –С.96–124.
89. Цыганков В.С., Сементин С.А., Кучеренко А.О. Квантовые компьютеры (учебно-методическое пособие) .–Ростов на Дону:РГУ, 2001.–53с.–(http://window.edu.ru/window_catalog/files/r20122/rsu424.pdf; http://window.edu.ru/window/library?p_rid=20122).
90. Тарасов Л.В. Закономерности окружающего мира. В 3 кн. Кн.3: Эволюция естественно-научного знания.–М.:ФИЗМАТЛИТ, 2004.–440с.
91. Мальцев А.И. Алгоритмы и рекурсивные функции.–М.:Наука, 1986.–368с.
92. Марков А.А., Нагорный Н.М. Теория алгорифмов.–М.:Наука, 1984.–432с.

93. Математическая энциклопедия.–М.:Советская энциклопедия, 1977.–Т.1.–(ст. Алгоритм).
94. Кнут Д. Искусство программирования для ЭВМ. Том 1: Основные алгоритмы.–М.:Мир, 1976.–736с.
95. Успенский В.А., Семенов А.Л. Теория алгоритмов: основные открытия и приложения.–М.:Наука, 1987.–288с.
96. ГОСТ 19.701-90 (ИСО 5807-85). Государственный стандарт СССР. Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения.– Взамен 19.002-80, ГОСТ 19.003-80; Введен с 01.01.1992.– (http://cert.obninsk.ru/gost/282/282.html).
97. Уэйт М., Прата С. Язык Си. –М.: Мир, 1988.–512с.
98. Гровер Л.К. Квантовая механика помогает найти иголку в стоге сена //Квантовые вычисления: за и против. Квантовый компьютер и квантовые вычисления. Том 1 /Пер. с англ. под ред. В.А. Садовничего.–Ижевск: Ред. журн. Регулярная и хаотическая динамика, Издательский дом Удмуртский университет, 1999.–С.101–109.– (Grover L.K. Quantum Mechanics helps in searching for a needle in a haystack.-(http://arxiv.org/abs/quant-ph/9706033)).
99. Чанг И., Вандерсипен Л., Жу К., Леюнг Д., Ллойд С. Экспериментальная реализация квантового алгоритма //Квантовые вычисления: за и против. Квантовый компьютер и квантовые вычисления. Том 1 /Пер. с англ. под ред. В.А. Садовничего.–Ижевск: Ред. журн. Регулярная и хаотическая динамика, Издательский дом Удмуртский университет, 1999.–С.130–140.
100. Айсерт Й., Уилкенс М., Левенштайн М. Квантовые игры и квантовые стратегии //Квантовые вычисления: за и против. Квантовый компьютер и квантовые вычисления. Том 1 /Пер. с англ. под ред. В.А. Садовничего. – Ижевск: Ред. журн. Регулярная и хаотическая динамика, Издательский дом Удмуртский университет, 1999.–С.158–167.
101. Нейман Дж., Моргенштерн О. Теория игр и экономическое поведение.–М: Наука, 1970.–708с.

Список рекомендуемых источников для самостоятельной работы

1. Яковлев В.П., Кондрашин М.П. Элементы квантовой информатики.–М.: МИФИ, 2004.–80с.

2. Nielsen M.A., Chuang I.L. Quantum Computation and Quantum Information.–M.: Cambridge University Press, 2000.–704p.–(Нильсен М., Чанг И. Квантовые вычисления и квантовая информация.–М.: Мир, 2006.–824с.).

3. Колмогоров А.Н. Основные понятия теории вероятностей.–М.:ФАЗИС, 1998.–142с.

4. Феллер В. Введение в теорию вероятностей и ее приложения. В 2 т.–М.:Мир, 1984.

5. Вентцель Е.С. Теория вероятностей.–М.:Высшая школа, 2001.–576с.

6. Яглом А.М., Яглом И.М. Вероятность и информация.–М.:Наука, 1973.–512с.

7. Мишулина О.А. Основные понятия статистической теории информации.–М.:МИФИ, 2000.–92с.

8. Кулик С.Д. Теория принятия решений (элементы теории проверки вероятных гипотез): учебное пособие.–М.: МИФИ, 2007.–152с.

9. Никитин Н.В., Уваров А.Ю. Диаграммная техника в теории вероятностей: учебное пособие.–М.: МИФИ, 1994.–64с.

10. Фейнман Р. Характер физических законов /Пер. с англ.–2-е изд., испр.–М.:Наука, 1987.–160с.

11. Мигдал А.Б. Квантовая физика для больших и маленьких.–М.:Наука, 1989.–144с.

12. Фейнман Р. Квантовомеханические компьютеры //Квантовый компьютер и квантовые вычисления /Пер. с англ. под ред. В.А. Садовничего. – Ижевск: Ред. журн. Регулярная и хаотическая динамика, 1999.–Т2.–С.125–156.

13. Фейнман Р., Хибс А. Квантовая механика и интегралы по траекториям.–М.:Мир, 1968.–383с.

14. Тарасов Л.В. Закономерности окружающего мира. В 3 кн. Кн.3: Эволюция естественно-научного знания.–М.:ФИЗМАТЛИТ, 2004.–440с.

СПИСОК СОКРАЩЕНИЙ

АВМ — *аналоговая вычислительная машина*;
АЭС — *атомная электростанция*;
АСОИУ — *автоматизированная система обработки информации и управления*;
АФИПС — *автоматизированная фактографическая информационно-поисковая система*;

БД — *база данных*;

В — *вольт*;
ВБ — *вычислительный базис*;
ВМ — *вычислительная машина*;
ВЫХ — *выход*;

ГС — *генеральная совокупность*;
ГВМ — *гибридная вычислительная машина*;
ГОСТ — *государственный стандарт*;

ДТ — *диаграммная техника*;
ДНК — *дезоксирибонуклеиновая кислота*;
ДНФ — *дизъюнктивная нормальная форма*;

ИС — *информационная система*;

КВ — *квантовый вычислитель*;
КС — *комбинационная схема*;
КНФ — *конъюнктивная нормальная форма*;

ЛФ — *логическая функция*;
ЛЭ — *логический элемент*;

МС — *математическая статистика*;

НПВ — *не представляется возможным принять решение*;

ОЗУ— *оперативно-запоминающее устройство*;
ОУ — *операционный усилитель*;

ПГС — *полная группа событий*;
ПГПНС — *полная группа попарно несовместных событий*;

см — *сантиметр*;
СВ — *случайная величина*;
СС — *случайное событие*;
СДНФ — *совершенная дизъюнктивная нормальная форма*;
СКНФ — *совершенная конъюнктивная нормальная форма*;
СССР — *Союз Советских Социалистических Республик*;

ТВ — *теория вероятностей*;
ТКВ — *теория квантовых вычислений*;

УП — *унитарное преобразование*;

ФД — *фактографические данные*;
ФИ — *фактографическая информация*;
ФС — *физическая система*;
ФБД — *фактографическая база данных*;
ФПВ — *формула полной вероятности*;

ЦВМ — *цифровая вычислительная машина*;

ЭД— *элементарная дизъюнкция*;
ЭК — *элементарная конъюнкция*;
ЭС — *элементарные события*;
ЭВМ — *электронно-вычислительная машина*;
ЭПР — *А.Эйнштейн, Б. Подольский, Н. Розен*;
ЭЦВМ — *электронная цифровая вычислительная машина*.

Сергей Дмитриевич Кулик
Александр Викторович Берков
Валерий Петрович Яковлев

ВВЕДЕНИЕ В ТЕОРИЮ КВАНТОВЫХ ВЫЧИСЛЕНИЙ
(методы квантовой механики в кибернетике)
Книга 1

Учебное пособие

Редактор *Е.Е. Шумакова*
Оригинал-макет подготовил *С.Д. Кулик*

Подписано в печать 31.10.2008. Формат 60x84 1/16
Печ. л. 13,25. Уч.-изд.л. 13,25. Тираж 150 экз.
Изд. № 1/1. Заказ №

Московский инженерно-физический институт
(государственный университет),
115409, Москва, Каширское ш., 31.

Типография издательства "Тровант",
г. Троицк Московской области