ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение
высшего профессионального образования

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ

И. Л. Ерош, М. Б. Сергеев, Н. В. Соловьев

ДИСКРЕТНАЯ МАТЕМАТИКА

Учебное пособие для вузов

Допущено УМО вузов
по университетскому политехническому образованию
в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности 230201 (071900) «Информационные системы и технологии» направления подготовки 230200 «Информационные системы»

Санкт-Петербург
2005

УДК 519.2(075)
ББК 22.176я73
Е78

Ерош И. Л., Сергеев М. Б., Соловьев Н. В.
Е78 Дискретная математика: Учеб. пособие /СПбГУАП. СПб., 2005.
144 с.: ил.
ISBN 5-8088-0169-9

Учебное пособие содержит как традиционные разделы дискретной математики: теорию множеств, булеву алгебру, комбинаторику, теорию графов, – так и ряд разделов, которые обычно не входят в учебники по дискретной математике, но исключительно важны для специалистов в области вычислительной техники, а именно: теорию дискретных групп, теорию чисел, теорию разрядных вычислений.

Пособие ориентировано на студентов технических университетов, аспирантов и преподавателей дисциплины «Дискретная математика».

Рецензенты:
кафедра радиосистем Санкт-Петербургского
электротехнического университета;
кандидат технических наук *В. Н. Сасковец*

Утверждено
редакционно-издательским советом университета
в качестве учебного пособия

ISBN 5-8088-0169-9

ПРЕДИСЛОВИЕ

Дискретная математика (дискретный анализ) занимается изучением финитных (конечных) свойств объектов, которые возникают как в различных разделах математики, так и в ее технических приложениях. Под конечными свойствами понимаются их ограниченность или перечислимость. Важными отличиями разделов дискретной математики от классических разделов непрерывной математики являются отсутствие понятия непрерывности и предела последовательности.

То, что в разделах дискретной математики рассматриваются конечные свойства объектов, совсем не означает, что при исследовании не встречаются бесконечные совокупности объектов или их конфигураций, однако, как правило, эти бесконечности являются счетными. В то время как в непрерывной математике бесконечности, как правило, континуальные.

Разделы дискретной математики всегда существовали в математике, но стали выделяться в самостоятельную дисциплину в связи с развитием средств связи и появлением компьютеров.

К разделам дискретной математики обычно относят:

математическую логику,
теорию алгоритмов,
булеву алгебру,
теорию конечных автоматов,
теорию дискретных групп,
теорию графов,
комбинаторику.
теорию чисел и еще много других разделов.

Характерными примерами приложений различных разделов дискретной математики являются:

методы распознавания образов, основанные на теории принятия решений,
криптографические протоколы.
теория кодирования информации,
теория сложности алгоритмов и т.д.

В настоящем учебном пособии рассматриваются только несколько разделов дискретной математики, которые, на взгляд авторов, наиболее востребованы для специалистов в области вычислительной техники и систем связи.

1. ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ

1.1. Понятие о множестве. Принадлежность элемента множеству

Основными понятиями теории являются *элементы* и *множество*. Эти понятия считаются общеизвестными и не определяются, так как, если попытаться определить их, например, так: *множество элементов есть их совокупность*, – тогда нужно дать понятие *совокупности*. Например, *совокупность элементов есть некоторый их набор*, что потребует дать определение *набора* элементов. Такие вложенные определения будут повторяться до бесконечности. Поэтому, говоря о некотором множестве, лучше всего пояснить это на примерах. Таким же неопределяемым понятием является *элемент*. Например, множество студентов конкретной группы можно обозначить через M. Каждый студент этой группы является элементом множества M.

Принадлежность некоторого элемента a множеству M записывается так: $a \in M$, и читается «элемент a принадлежит множеству M». Непринадлежность элемента b множеству M обозначается: $b \notin M$. Например, студент Иванов (a) принадлежит множеству студентов некоторой группы ($a \in M$), а студент Петров (b) не принадлежит этой группе ($b \notin M$).

1.2. Способы задания множеств

Для того чтобы задать некоторое множество, нужно или перечислить все элементы, принадлежащие этому множеству, или сформулировать правило определения принадлежности. Например, множеству гренадеров будут принадлежать новобранцы с благообразными лицами, рост которых не менее 2-х метров.

Рассмотрим примеры задания множеств.

1. Множеству M_1 принадлежат элементы a, b, c, d, e. Это множество задано перечислением его элементов.

2. Множество Z_+ всех натуральных чисел (включая 0).

3. Множество Z всех целых чисел.

4. Множество R всех действительных чисел.

5. Множество C всех комплексных чисел.

6. Множество K всех кватернионов.

Множества 2 – 6 заданы общими свойствами своих элементов.

7. Множество M_7 всех решений уравнения $\sin x = 1$. Известно, что решения этого уравнения имеют вид: $\pi/2 + 2k\pi$, где k – произвольный элемент множества целых чисел (Z).

8. Множество M_8 всех студенческих групп первого курса некоторого университета.

Особенностью M_8 является то, что сами студенческие группы являются множествами конкретных студентов, т. е. M_8 является множеством множеств.

Мощностью множества M называется число его элементов (обозначается $|M|$).

Любая совокупность элементов некоторого множества M называется его *подмножеством*.

1.3. Основные операции над множествами

Над множествами можно выполнять некоторые операции. Например:

1. *Объединение* множеств (обозначается $\cup$).

Пусть имеются два множества: M_1 с элементами $\{a, b, c, d\}$ и M_2 с элементами $\{b, c, e, p\}$. Объединением множеств M_1 и M_2 является множество M_3, элементами которого будут как элементы множества M_1, так и элементы множества M_2. В дальнейшем будем писать: $M_1 = \{a, b, c, d\}$, $M_2 = \{b, c, e, p\}$, $M_3 = M_1 \cup M_2 = \{a, b, c, d, e, p\}$.
В общем виде результат объединения множеств A и B записывается так: $A \cup B = \{x \mid x \in A$ или $x \in B\}$.

2. *Пересечение* множеств (обозначается $\cap$).

Пересечением множеств M_1 и M_2 является множество M_4, элементами которого будут элементы, принадлежащие одновременно как множеству M_1, так и множеству M_2. Для предыдущего примера $M_4 = M_1 \cap M_2 = \{b, c\}$. В общем виде результат пересечения множеств A и B записывается так: $A \cap B = \{x \mid x \in A$ и $x \in B\}$.

Если имеются два множества: $A = \{a, b, c, d, e\}$ и $B = \{1, 2, 3\}$, а их пересечение не содержит ни одного элемента, точнее, содержит пустое множество элементов, то это обозначается так: $A \cap B = \varnothing$.

3. *Разностью* множеств A и B (обозначается $A \backslash B$) называется множество всех тех и только тех элементов A, которые не содержатся в B. В общем виде разность обозначатся: $A \backslash B = \{x \mid x \in A$ и $x \notin B\}$. Для рассматриваемого примера (п. 1.) $M_1 \backslash M_2 = \{a, d\}$.

4. Если для множеств M_i можно указать некоторое универсальное множество U, такое, что M_i являются подмножествами этого множества, то для каждого M_i можно указать *дополнение* до U, которое обозначается $\overline{M}_i$ и определяется как $U \backslash M_i$. Пусть, например, A – множество девочек в некотором классе, B – все ученики данного класса. Тог-

да дополнением множества девочек до всего множества учеников класса будет $\bar{A} = B \backslash A$ – множество мальчиков этого класса.

Рассмотрим следующую задачу. В цехе предприятия работают 15 человек, из них 6 человек имеют дипломы наладчиков станков с ЧПУ (I), 8 имеют дипломы слесарей (II) и 5 – фрезеровщиков (III), 3 человека имеют одновременно дипломы наладчиков станков с ЧПУ и слесарей, 2 человека имеют дипломы наладчика станков с ЧПУ и фрезеровщика, 4 человека имеют дипломы слесаря и фрезеровщика и 1 человек имеет все три вида дипломов. Сколько работников цеха не имеют ни одного вида из этих трех дипломов (они могут иметь дипломы инженера, но сейчас нас это не интересует). Сколько работников цеха имеют ровно по два диплома? Сколько работников цеха имеют только один из дипломов? Можно задать и другие вопросы и получить на них ответы. Удобно представить задачу в виде следующей диаграммы (рис. 1.1). Весь прямоугольник соответствует множеству работников цеха.

Мощность множества работников цеха $|U| = 15$. Мощность объединения пар множеств $|\mathrm{I} \cup \mathrm{II}| = 6+8-3 = 11$, $|\mathrm{I} \cup \mathrm{III}| = 6+5-2 = 9$, $|\mathrm{II} \cup \mathrm{III}| = 8+5-4 = 9$.

Ответ на первый вопрос дает мощность дополнения объединенных множеств I, II и III до U, т. е. $|U \setminus (\mathrm{I} \cup \mathrm{II} \cup \mathrm{III})| = 15-6-8-5+3+2+4-1 = 4$.

Ответ на второй вопрос можно записать так:

$|\mathrm{I} \cap \mathrm{II}| + |\mathrm{I} \cap \mathrm{III}| + |\mathrm{II} \cap \mathrm{III}| - 3 \times |\mathrm{I} \cap \mathrm{II} \cap \mathrm{III}| = 3+2+4-3 = 6$.

Ответ на третий вопрос можно записать так:

$|\mathrm{I}| - |\mathrm{I} \cap \mathrm{II}| - |\mathrm{I} \cap \mathrm{III}| + |\mathrm{I} \cap \mathrm{II} \cap \mathrm{III}| = 6-3-2+1 = 2$. Столько человек имеют один диплом наладчика станков с ЧПУ.

$|\mathrm{II}| - |\mathrm{I} \cap \mathrm{II}| - |\mathrm{II} \cap \mathrm{III}| + |\mathrm{I} \cap \mathrm{II} \cap \mathrm{III}| = 8-3-4+1 = 2$. Столько человек имеют один диплом слесаря.

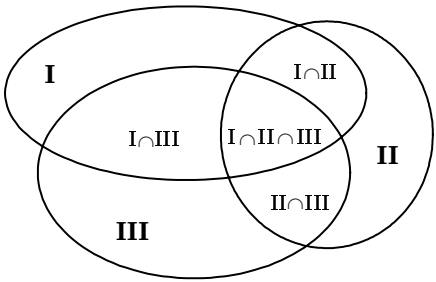


Рис. 1.1. Операции над множествами

$|\text{III}|-|\text{I}\cap\text{III}|-|\text{II}\cap\text{III}|+|\text{I}\cap\text{II}\cap\text{III}| = 5-2-4+1 = 0$. Столько человек имеют один диплом фрезеровщика.

Итак, 6 человек имеют по одному диплому, 4 человека по 2, 1 человек имеет все три диплома и 4 человека не имеют дипломов. Всего $6+4+1+4 = 15$.

Аналогично находятся ответы и на другие вопросы задачи.

5. *Прямым произведением* множеств A и B (обозначается $A\times B$) являются множества всех пар (ab), где $a \in A$ и $b \in B$. Пусть, например, $A = \{a, b, c\}$ и $B = \{1, 2\}$, тогда элементы прямого произведения имеют вид: $A \times B = \{a1, a2, b1, b2, c1, c2\}$. Множество $R \times R = R^2$ – множество точек плоскости, R^n – множество точек n-мерного действительного пространства.

Пусть A – конечное множество, элементами которого являются символы (буквы, цифры, знаки препинания, знаки операций). Такие множества обычно называют *алфавитами*. Элементы множества A^n называют *словами* длины n в алфавите A. Множество всех слов в алфавите A – это множество $A^1\cup A^2\cup A^3\cup\ldots\cup A^n$.

1.4. Мощность множества и число подмножеств любого множества

Теорема 1. Пусть $A_1, A_2, \ldots, A_n$ – конечные множества и $|A_i| = m_i$, тогда мощность множества $A_1 \times A_2 \times \ldots \times A_n$ равна произведению мощностей $m_1 m_2 \ldots m_n$.

Для $n = 1$ теорема очевидна. Пусть она выполняется для некоторого n. Докажем методом математической индукции, что она выполняется и для $n+1$. Возьмем любой вектор $(a_1, a_2, \ldots, a_n)$ и припишем справа a_{n+1}. Число элементов увеличится в количество раз, равное мощности множества A_{n+1}.

Теорема 2. Если для конечного множества A $|A| = n$, то число всех подмножеств множества A равно 2^n.

Пример. $A = \{a, b, c\}$. Подмножества будут иметь вид: $\{\varnothing\}$, $\{a\}$, $\{b\}$, $\{c\}$, $\{ab\}$, $\{ac\}$, $\{bc\}$, $\{abc\}$, т. е. 8.

1.5. Понятие об алгебрах

Функцию типа $\varphi: M^n \to M$ будем называть n-арной операцией на множестве M. Множество M вместе с заданными на нем операциями $\Omega = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ называется *алгеброй*, M – несущим или основным множеством, Ω – сигнатурой. Не следует путать алгебру с *линейной* алгеброй. В разд. 3 будет дано определение линейной алгебры и рассмотрены примеры линейных алгебр.

1.6. Задачи для контрольной

1. Множество $A = \{1, 2, 5, 7, 8\}$, $B = \{2, 6, 9\}$. Найдите объединение, пересечение и разности множеств.

2. Множество $A = \{a, b, c, d, e\}$, $B = \{p, q, r, s\}$. Найдите объединение, пересечение и разности множеств.

3. В группе 35 студентов, из них 21 знают английский, 15 знают немецкий, 8 знают и английский и немецкий. Покажите физический смысл объединения, пересечения, дополнения и разности множеств.

4. Имеются 3 множества: $A = \{1, 2, 3\}$, $B = \{a, d\}$, $C = \{A, B, C, D\}$. Найти мощность множества прямого произведения $A \times B \times C$. Найти число подмножеств каждого множества и их прямого произведения.

5. Множество $U = \{1 - 100\}$. Множество P – все числа, кратные 5, Q – все числа, кратные 7. Найдите пересечение множеств, объединения, дополнения и разности множеств. Определите мощности всех множеств.

6. Сколько разных слов длины, не превышающей 5, может быть подано на вход цифрового устройства, если входной алфавит состоит из двух букв {0, 1}? Слово длины 0 – одно, длины 1 – два (0 и 1), длины 2 – четыре, длины 3 – восемь, длины 4 – шестнадцать, длины 5 – тридцать два. Если к этой сумме прибавить 1, получим 64. Всего на вход устройства может быть подано $2^6 - 1$ разных слов. Найдите количество разных слов длины, не превышающей 7, 8, 9, 10, n.

Литература

1. Александров, П. С. Введение в общую теорию множеств и функций / П. С. Александров. М.; Л.: 1948.

2. Кузнецов, О. П. Дискетная математика для инженера / О. П. Кузнецов, Г. М. Адельсон-Вельский. М.: Энергоатомиздат, 1988. 480 с.

2. БУЛЕВА АЛГЕБРА. КОМБИНАЦИОННЫЕ СХЕМЫ

Булевы функции (функции алгебры логики) описывают логику работы цифровых устройств, называемых комбинационными схемами.

Цифровые устройства (цифровые автоматы) обычно делятся на два класса: автоматы без памяти (однотактные автоматы, комбинационные схемы) и автоматы с памятью (многотактные автоматы). Комбинационные схемы составляют основу дискретных вычислительных и управляющих устройств. Они могут выполнять как самостоятельные функции: преобразователей кодов, дешифраторов и т. п., так и входить в состав цифровых автоматов с памятью, реализуя функции переключения элементов памяти в новые состояния, выработку логических и управляющих сигналов. Сами элементы памяти также могут быть реализованы в виде комбинационных схем с обратными связями.

В настоящем разделе в краткой форме изложены основные понятия и методы построения однотактных цифровых устройств контроля и управления, логика работы которых описывается булевыми функциями. Теория анализа и синтеза многотактных цифровых устройств (автоматов с памятью) обычно излагается в курсе «Теория конечных автоматов».

2.1. Понятие о булевых функциях. Булевы функции одного и двух аргументов

Булевыми функциями (функциями алгебры логики) называют функции, аргументы которых, так же как и сама функция, принимают только два значения: 0 или 1. Алгебра логики является разделом математической логики, в которой изучаются методы доказательства истинности (1) или ложности (0) сложных логических конструкций, составленных из простых высказываний, на основе истинности или ложности последних.

Алгебра Буля оказалась очень удобным и эффективным математическим аппаратом для анализа и синтеза комбинационных схем. Булевы функции определяют логику работы комбинационных схем вида (рис. 2.1).

Рассмотрим частные случаи комбинационных схем.

Пусть $n = 1$, тогда входной сигнал x может принимать только два значения: 0 и 1, а выходной сигнал $F(x)$ может обеспечивать 4 различные реакции на выходе. Таблица, в которой каждому набору входных

Рис. 2.1. Общий вид комбинационной схемы с одним выходом, где x_1–x_n, $F \in \{0, 1\}$

Таблица 2.1

x	F_0	F_1	F_2	F_3
0	0	0	1	1
1	0	1	0	1

сигналов сопоставляется значение выходного сигнала, называется *таблицей истинности* функции.

Для комбинационных схем с одним входом таблицы истинности всех описывающих логику работы схемы булевых функций примут вид (табл. 2.1).

F_0 = const 0; $F_1 = x$ – функция повторения x; F_3 = const 1; F_2 – инверсия аргумента x, обозначаемая $\neg x$ или $\bar{x}$ и называемая иногда «*не x*», «*отрицание x*» или «*инверсия аргумента x*».

При $n = 2$ получаем таблицу истинности, в которой 16 различных функций двух аргументов (табл. 2.2).

Таблица 2.2

x_1	x_2	F_0	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}	F_{14}	F_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Среди функций двух аргументов имеются уже известные функции: F_0 и F_{15}, соответственно «константа 0» и «константа 1», функции, не зависящие от аргументов, иногда называемые «функции нуль аргументов».

Функции $F_3 = x_1$ и $F_5 = x_2$ – функции повторения соответственно аргументов x_1 и x_2. Функции $F_{12} = \neg x_1$ и $F_{10} = \neg x_2$ – функции инверсии соответственно аргументов x_1 и x_2. Эти функции считаются функциями одного аргумента.

Рассмотрим новые функции, которые впервые появляются в таблице функций двух аргументов.

F_1 – *конъюнкция* аргументов x_1 и x_2, обозначается: $F_1 = x_1 \,\&\, x_2 = x_1 \wedge x_2 = x_1 \cdot x_2 = x_1 x_2$. Допустимыми являются все виды приведенных обозначений, но поскольку эта функция называется «функция “И”» или «логическое умножение», то, как и в обычной алгебре, знак умножения часто опускается.

F_7 – *дизъюнкция* аргументов x_1 и x_2, обозначается: $F_1 = x_1 \vee x_2 = x_1 + x_2$. Обычно используют только первый вид обозначения, т. е. знак «+» практически не используется. Эта функция называется «функция "ИЛИ"» или «логическое сложение».

Для приведенных функций в таблице имеются инверсии. Так, $F_{14} = \overline{F}_1$, $F_8 = \overline{F}_7$, но поскольку функции F_{14} и F_8 играют очень важную роль в вычислительной технике, они имеют собственные названия, соответственно «*штрих Шеффера*» и «*стрелка Пирса*».

Новыми функциями также являются F_9 и F_6. Первая называется функцией совпадения (*эквиваленция*) и обозначается обычно: $F_9 = x_1 \equiv x_2$. В математической логике для этой функции используется другое обозначение, а именно: $x_1 \sim x_2$. Вторая функция является ее инверсией и называется функцией «*сложение по модулю* 2», т. е. $F_6 = \overline{F}_9$ или $\overline{(x_1 \equiv x_2)} = x_1 \oplus x_2$.

Функции F_{13} и F_{11} называются функциями *импликации* и обозначаются соответственно: $F_{13} = x_1 \to x_2$ и $F_6 = x_2 \to x_1$ (словесное обозначение F_{13}: «x_1 влечет x_2»; F_{11}: «x_2 влечет x_1»). Функции импликации играют очень важную роль в математической логике, так как описывают логику всех теорем достаточности, которые формулируются в виде: «Если выполняется условие A, то следует B». При построении комбинационных схем эти функции практически не используются.

Последние две функции из таблицы F_2 и F_4 являются инверсиями функций импликации, соответственно F_{13} и F_{11}.

2.2. Булевы функции трех аргументов

Функции трех аргументов задаются на 8 наборах. Количество функций трех аргументов равно $2^8 = 256$.

Среди функций трех аргументов встречаются функции нуль, одного и двух аргументов, а именно: константа 0 и константа 1, функции повторения аргументов, инверсии аргументов, дизъюнкции и конъюнкции трех аргументов, сложения по модулю 2 трех аргументов и т. п.

Одной из новых функций трех аргументов является *мажоритарная* функция. Таблица истинности этой функции имеет вид (табл. 2.3).

Функция M равна 1, если во входном наборе два или три аргумента принимают значение 1, и равна 0 в остальных случаях. Эта функция обладает корректирующей способно-

Таблица 2.3

X_1	X_2	X_3	M
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

стью, поэтому на заре развития вычислительной техники публиковались работы, в которых рекомендовалось все комбинационные схемы строить на мажоритарных элементах.

2.3. Булевы функции *n* аргументов. СДНФ и СКНФ

Булева функция n аргументов задается на 2^n наборах. Число таких функций равно 2^{2^n}. Если булева функция задана таблицей истинности, то она может быть представлена в аналитической форме с использованием операций конъюнкции, дизъюнкции и инверсии с помощью следующих правил:

– каждой единице в таблице истинности сопоставляется конъюнкция ранга n, где n – число аргументов функции; рангом конъюнкции называют число аргументов, входящих в конъюнкцию, причем в эту конъюнкцию аргумент входит без инверсии, если в соответствующем наборе он принимает значение 1, и с инверсией, если принимает значение 0;

– все полученные конъюнкции объединяются знаками дизъюнкции.

Например, для мажоритарной функции аналитическое выражение будет иметь вид

$$M = \overline{x}_1 x_2 x_3 \vee x_1 \overline{x}_2 x_3 \vee x_1 x_2 \overline{x}_3 \vee x_1 x_2 x_3. \qquad (2.1)$$

Аналитическое выражение функции вида (2.1) называют совершенной дизъюнктивной нормальной формой (СДНФ) функции, при этом под нормальной формой понимают выражение, в котором инверсии применяются только к отдельным аргументам, под совершенной формой понимают аналитическое выражение функции, когда во все конъюнкции входят все аргументы, т. е. все конъюнкции имеют ранг n.

Таблица 2.4

X_1	X_2	X_3	F	$\overline{F}$
0	0	0	1	0
0	0	1	0	1
0	1	0	1	0
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	0

Если в таблице истинности число нулей существенно меньше числа единиц, используют аналитическую запись в виде совершенной конъюнктивной нормальной формы (СДНФ). Она строится по следующим правилам:

– каждому нулю в таблице истинности сопоставляется дизъюнкция ранга n, где n – число аргументов функции; рангом дизъюнкции называют число аргументов, входящих в дизъюнкцию, причем в эту дизъюнкцию аргумент входит без инверсии, если в соответствующем наборе он принимает значение 0, и с инверсией, если принимает значение 1;

– все полученные дизъюнкции объединяются знаками конъюнкции.

Возьмем, например, функцию F, представленную следующей таблицей истинности (табл. 2.4).

СДНФ этой функции представляет собой шесть конъюнкций ранга 3, объединенных знаками дизъюнкции, т. е. достаточно громоздкое выражение. В то же время СКНФ этой функции будет выглядеть так:

$$F = (x_1 \vee x_2 \vee \neg x_3)(\neg x_1 \vee x_2 \vee x_3), \qquad (2.2)$$

т. е. содержит две дизъюнкции ранга 3, объединенные знаком конъюнкции.

2.4. Элементарные преобразования булевых выражений

Часто преобразование булевых выражений выполняется с целью упрощения последних или, как говорят, с целью их *минимизации*. Легко обосновываются следующие правила минимизации:

– поглощения: $x \vee xy = x$; $x(x \vee y) = x$;

– склеивания: $xy \vee x\neg y = x$;

– обобщенного склеивания: $xz \vee y\neg z \vee xy = xz \vee y\neg z$;

– $x \vee \neg xy = x \vee y$.

Покажем, как можно применить правило склеивания для минимизации мажоритарной функции. Легко показать, что $x \vee x = x$. Это означает, что, если функция представлена в дизъюнктивной форме, то всегда можно добавить любой член, причем сколько угодно раз. Тогда аналитическое выражение (2.1) можно переписать в следующем виде, повторив четвертую конъюнкцию еще дважды:

$$M = \neg x_1 x_2 x_3 \vee x_1 \neg x_2 x_3 \vee x_1 x_2 \neg x_3 \vee x_1 x_2 x_3 \vee x_1 x_2 x_3 \vee x_1 x_2 x_3. \qquad (2.3)$$

Повторение конъюнкции $x_1 x_2 x_3$ не меняет значения функции M. Тогда, склеивая 1-й и 4-й члены, 2-й и 5-й, 3-й и 6-й, получаем эквивалентное выражение

$$M = x_2 x_3 \vee x_1 x_3 \vee x_1 x_3. \qquad (2.4)$$

Выражение (2.4) будет дизъюнктивной нормальной, но уже не совершенной формой функции, так как в каждую из конъюнкций входят не все аргументы функции.

Преобразование булевых выражений с помощью приведенных правил поглощения, склеивания и обобщенного склеивания применяется достаточно редко, так как имеется более эффективный способ минимизации булевых функций, число аргументов которых не превышает 10.

Кроме того, также просто обосновывается преобразование, называемое *правилами де Моргана*:

$$\begin{aligned} \neg(x_1 x_2) &= \neg x_1 \vee \neg x_2; \\ \neg(x_1 \vee x_2) &= \neg x_1 \neg x_2. \end{aligned} \qquad (2.5)$$

Покажем, как применить правило де Моргана для вывода формулы СКНФ.

В табл. 2.4 имеется значение функции, инверсной к F, т. е. $\neg F$. Эта функция имеет только две единицы, поэтому СДНФ ее будет представлять собой две конъюнкции, каждая ранга три, объединенные знаком дизъюнкции:

$$\neg F = \neg x_1 \neg x_2 x_3 \vee x_1 \neg x_2 \neg x_3. \qquad (2.6)$$

Проинвертируем левую и правую части выражения (2.6) и применим к правой части правило де Моргана, тогда получим

$$F = (x_1 \vee x_2 \vee \neg x_3)(\neg x_1 \vee x_2 \vee x_3).$$

В результате получена формула СКНФ функции F.

2.5. Минимизация булевых функций с помощью диаграмм Вейча (карт Карно)

Диаграммы Вейча являются той же таблицей истинности булевой функции, только представленной в более компактной форме. Так, для функции трех аргументов, которая задается на 8 наборах, таблица истинности будет содержать 8 строк, а диаграмма Вейча – 8 клеток, причем каждая клетка в диаграмме Вейча соответствует некоторому набору (строке) в таблице истинности.

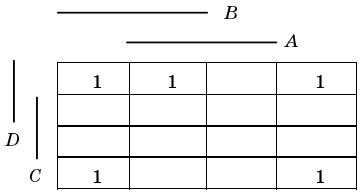
X_3 \ X_2 X_1				
	1	1	1	
		1		

Области в диаграмме Вейча обозначим следующим образом: подчеркнутые столбцы или строки будут соответствовать истинному значению аргумента, а не подчеркнутые – ложному. Тогда диаграмма Вейча мажоритарной функции которой примет вид

X_3 \ X_2 X_1				
	1	1	1	
		1		

Из полученной диаграммы Вейча легко выписывается минимальное выражение для мажоритарной функции: $F = x_2x_3 \vee x_1x_3 \vee x_1x_3$, которое полностью соответствует полученному выше в результате минимизации с помощью правила склеивания.

Возьмем некоторую функцию F четырех аргументов, диаграмма Вейча которой имеет вид



Эта функция принимает значение 1 на пяти наборах, отмеченных на диаграмме единицами. На остальных наборах функция принимает значение 0. СДНФ этой функции содержала бы 5 конъюнкций ранга 4 каждая, объединенные знаками дизъюнкций. Однако из диаграммы Вейча легко выписывается минимальное выражение функции в дизъюнктивной нормальной форме:

$$F = \overline{A}\,\overline{C} \vee B\,\overline{C}D.$$

Области в диаграмме Вейча обозначаются так, чтобы две соседние клетки соответствовали бы «склеивающимся» конъюнкциям (т. е. конъюнкциям, отличающимся значением только одного аргумента). Это обеспечивает наглядность минимизации.

В общем случае области в диаграммах Вейча для функций большого числа аргументов обозначаются *кодом Грэя*. Особенностью этого кода является то, что две соседние комбинации отличаются значением только одного аргумента. Обычный двоичный код этому условию не удовлетворяет. Код Грэя используется в цифровых кодовых датчиках, что позволяет сделать ошибку равномерной при случайных смещениях токосъемников, при этом ошибка равна 2^{-m}, где m – число двоичных разрядов кодового датчика. Это свойство кода Грэя используется для обозначения областей в диаграммах Вейча.

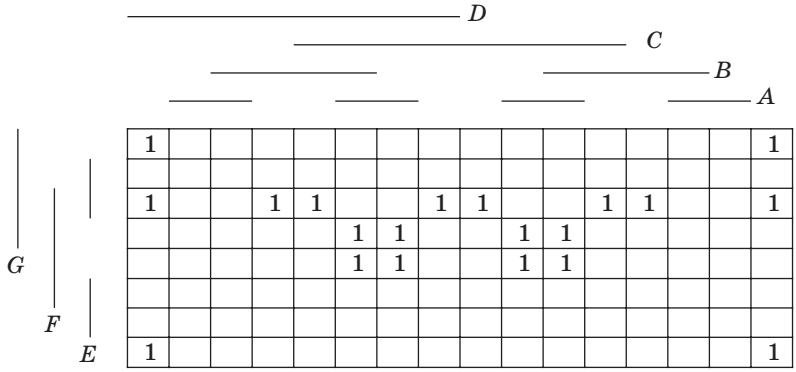
В табл. 2.5 приведен код Грэя для 4-х аргументов (разрядов). Если требуется построить код Грэя

Таблица 2.5

0000	0000
0001	0001
0010	0011
0011	0010
0100	0110
0101	0111
0110	0101
0111	0100
1000	1100
1001	1101
1010	1111
1011	1110
1100	1010
1101	1011
1110	1001
1111	1000

на меньшее число разрядов, то его легко получить из имеющейся таблицы путем «вырезания» соответствующей части. Так, в приведенной таблице жирным шрифтом показано, как получить двухразрядный код Грэя. Если требуется построить код Грэя на 5 разрядов, то код в таблице следует зеркально отразить вниз и добавить еще один старший разряд, причем в верхней половине таблицы в этом разряде будут стоять нули, а в нижней – единицы. Таким образом можно построить коды Грэя на любое число разрядов.

Пример. Минимизировать функцию семи аргументов, заданную диаграммой Вейча:



1															1
1			1	1			1	1			1	1			1
					1	1			1	1					
					1	1			1	1					
1															1

Минимальное выражение в дизъюнктивной нормальной форме имеет вид $F = AC\bar{}EF \vee \bar{}AEFG \vee \bar{}A\bar{}B\bar{}C\bar{}E\bar{}F$.

Примеры для практических занятий.

1. Доказать с помощью диаграмм Вейча равенства, которые использовались для минимизации (поглощения и склеивания, а также правило де Моргана).

2. Построить диаграммы Вейча для следующих функций и выписать минимальные выражения в дизъюнктивной нормальной форме:

а) $\bar{}ab\bar{}cd \vee \bar{}a\bar{}b\bar{}c\bar{}d \vee \bar{}ab\bar{}c\bar{}d \vee \bar{}a\bar{}b\bar{}cd \vee \bar{}a\bar{}bcd \vee \bar{}a\bar{}bc\bar{}d = ?$

b) $abc \vee ab\bar{}c \vee \bar{}abd \vee \bar{}bde = ?$

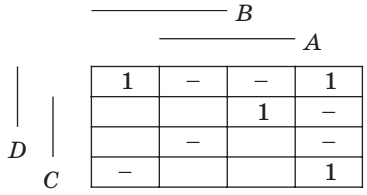
2.6. Минимизация частично определенных булевых функций

Диаграммы Вейча могут использоваться для минимизации не только так называемых полностью определенных логических функций (когда функция в таблице истинности принимает только два значения: 0 или 1), но и для случая частичных (не полностью) определенных функций). При построении реальных цифровых устройств контроля и управления комбинационные схемы описываются, как правило, не пол-

ностью определенными булевыми функциями. Очень часто функции не определены на большом числе наборов. В таблице истинности и, следовательно, в диаграммах Вейча такие функции кроме 0 и 1 будут содержать еще и «—». Это означает, что такой набор никогда на вход устройства не поступает. Следовательно, поведение комбинационной схемы при таком наборе не имеет значения, и на месте «—» может быть произвольно поставлена либо 1, либо 0. Этот процесс называется доопределением булевой функции. Доопределение булевой функции желательно выполнять так, чтобы получить возможно более простое выражение. В этом случае, как правило, реализованная комбинационная схема также оказывается более простой.

Пояснить наличие не полностью определенных булевых функций можно с помощь следующего простого примера. Известно, что устройство управления современным лифтом является цифровым. В 9-этажном доме это устройство должно помнить коды всех 9 этажей, во всяком случае, до тех пор, пока клиент не попадет на свой этаж. Память в цифровых устройствах реализуется с помощью элементарных автоматов (простых элементов памяти с двумя устойчивыми состояниями – триггеров). Если взять три триггера, то на них можно реализовать 8 различных комбинаций, и эти комбинации сопоставить этажам дома. В 9-этажном доме требуется использовать 9 различных комбинаций, следовательно, память этажей должна содержать 4 триггера. Но на 4-х триггерах можно реализовать 16 различных комбинаций, 9 из них сопоставить этажам, а остальные 7 окажутся не использованными. Очевидно, в таком устройстве управления существуют комбинации, которые никогда на вход устройства поданы быть не могут (в 9-этажном доме нельзя нажать кнопку 13-го этажа). Поведение устройства на этих наборах не имеет значения.

Пусть задана диаграмма Вейча некоторой не полностью определенной функции:

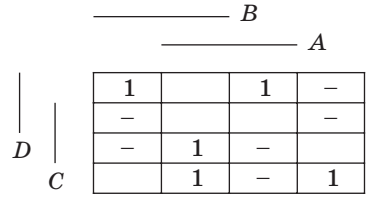


Приведенная функция имеет прочерки в шести клетках, в каждой из которых может быть поставлена как 1, так и 0. Следовательно, существует $2^6 = 64$ различных способа доопределения булевой функции. Однако из диаграммы легко выбрать наилучший, который дает следующий результат минимизации: $F = \overline{A}\,\overline{C} \vee \overline{B}D$.

Примеры для практических занятий.

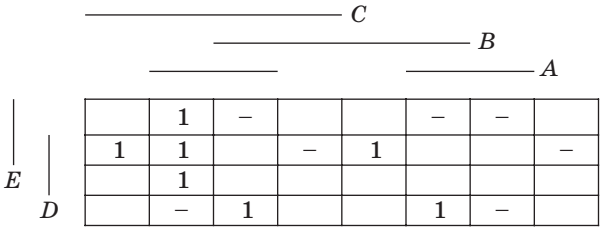
Доопределить функцию и выписать минимальное выражение из диаграмм Вейча:

a)



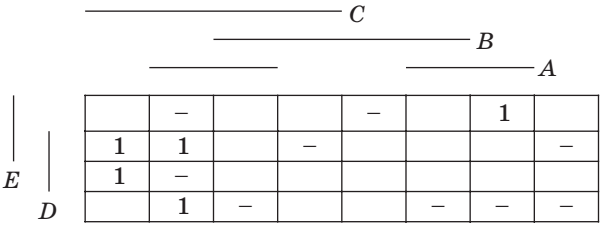
1		1	–
–			–
–	1	–	
	1	–	1

b)



	1	–			–	–	
1	1		–	1			–
	1						
	–	1			1	–	

c)



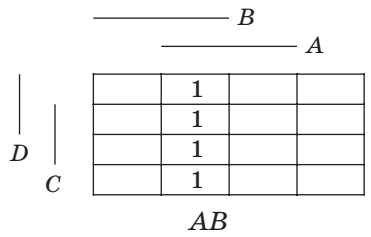
	–			–		1	
1	1		–				–
1	–						
	1	–			–	–	–

2.7. Проверка равенств в булевой алгебре

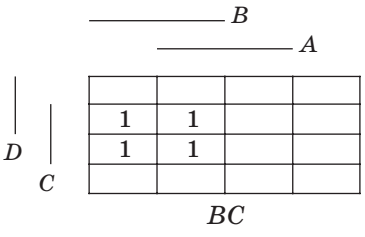
Для того чтобы доказать равенство двух функций в булевой алгебре, например $F(x_1, x_2, \ldots, x_n) = P(x_1, x_2, \ldots, x_n)$, необходимо и достаточно показать, что на всех наборах аргументов $x_1, x_2, \ldots, x_n$ левая часть равенства совпадает с правой частью. Таким образом, для доказательства равенства достаточно показать, что диаграммы Вейча левой и правой части совпадают. Например:

$$(AB \downarrow BC) \to BD = \neg(\neg B \vee \neg A \neg C \neg D).$$

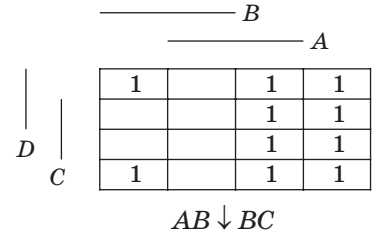
Для доказательства этого равенства построим диаграммы Вейча для левой и правой части равенства. При этом независимо от того, сколько аргументов имеется в выбранном фрагменте, будем строить диаграммы Вейча на полное число аргументов. В данном случае на 4 аргумента.



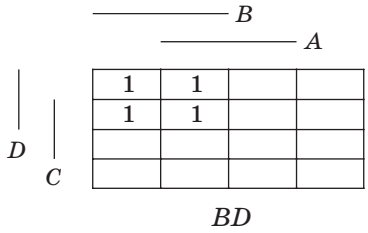
AB



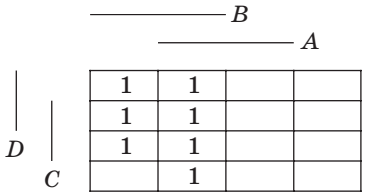
BC



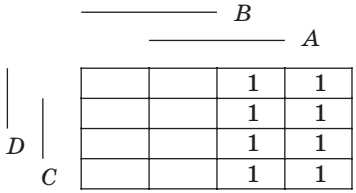
$AB \downarrow BC$



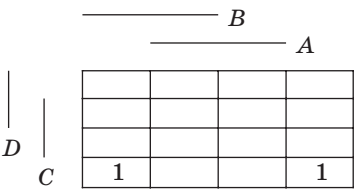
BD



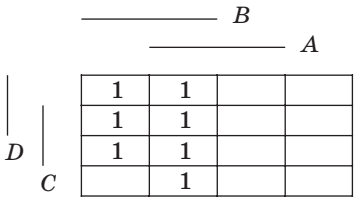
Эта диаграмма соответствует левой части равенства $(AB \downarrow BC) \to BD$.



$\overline{B}$



$\overline{A}\overline{C}\overline{D}$



Эта диаграмма соответствует правой части равенства $\overline{(}\overline{B} \vee \overline{A}\overline{C}\overline{D})$.

Поскольку диаграмма Вейча для левой части совпадает с диаграммой для правой, то имеет место приведенное выше равенство.

Для упрощения произвольных булевых выражений можно построить диаграмму Вейча этого выражения и выписать из полученной диаграммы аналитическое выражений в дизъюнктивной нормальной форме. Алгоритм упрощения можно представить следующим образом.

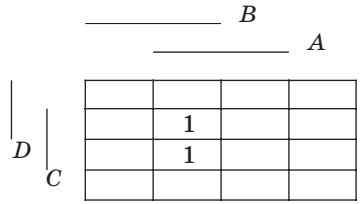
1. Подсчитать число аргументов, которые входят в выражение.

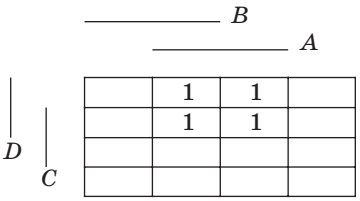
2. Для любого фрагмента упрощаемого выражения строить диаграмму Вейча на полное число аргументов.

3. Применять встречающиеся функции к диаграммам, которые соответствуют фрагментам.

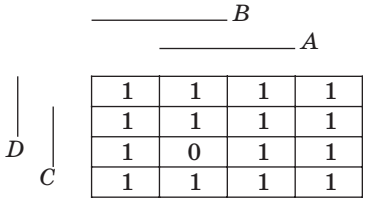
4. Из результирующей диаграммы выписать минимальное выражение в дизъюнктивной нормальной форме.

Пусть, например, требуется упростить булево выражение: $\neg(ABC \to AD) \oplus (BC \,/\, ACD)$. Число разных аргументов в этом выражении равно 4. Следовательно, все диаграммы будут строиться на 4 аргумента. Построим две диаграммы для конъюнкций ABC и AD.

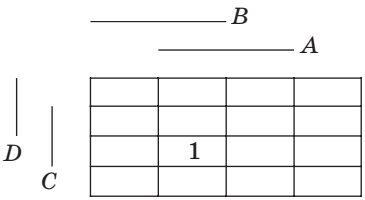




Из таблицы истинности двух аргументов (табл. 2.2) найдем таблицу функции «импликация». Построим диаграмму Вейча для результата: $ABC \to AD$ и проинвертируем результат.

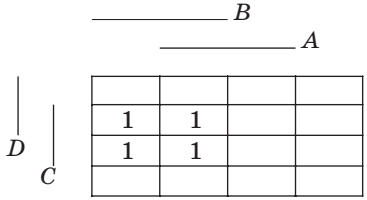


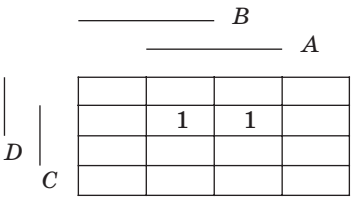
$ABC \to AD$



$\neg(ABC \to AD)$

Построим диаграммы Вейча для следующих конъюнкций: BC и ACD.





Из таблицы истинности двух аргументов найдем таблицу функции «штрих Шеффера», которая обозначается как /. Построим диаграмму Вейча для выражения (BC/ACD).

		B			
		A			
		1	1	1	1
		1	0	1	1
D		1	1	1	1
	C	1	1	1	1

Последней операцией является $\oplus$ – сумма по модулю 2. Эта функция равна 1, когда аргументы различаются, и 0, когда совпадают. Поэтому окончательный результат выглядит так:

		B			
		A			
		1	1	1	1
		1	0	1	1
D		1	0	1	1
	C	1	1	1	1

$$\neg(ABC \to AD) \oplus (BC \,/\, ACD) = \neg(ABC).$$

При минимизации выражения $M(AB \to C, ACD, BD \vee AC)$, где под $M(X, Y, Z)$ понимается мажоритарная функция от аргументов X, Y, Z, нужно построить диаграммы Вейча для выражений $AB \to C$, ACD и $BD \vee AC$, а затем диаграмму Вейча мажоритарной функции от этих трех аргументов.

2.8. Функционально полные наборы и базисные наборы

Функционально полным называется набор булевых функций $\{f_1, f_2, \ldots, f_n\}$ такой, что любая сколь угодно сложная булева функция может быть выражена в виде суперпозиции (сочетания) функций из этого набора.

Базисным называется такой функционально полный набор, из которого нельзя исключить ни одну булеву функцию без ущерба для его функциональной полноты.

Поскольку любая булева функция, заданная таблицей истинности, может быть представлена в виде СДНФ (или СКНФ), то функционально полный набор будет содержать функции $\{\&, \vee, \neg\}$. Данный набор не является базисным, так как из него можно исключить либо &, либо $\vee$, а недостающую функцию реализовать с помощью оставшихся функций. Напри-

мер, если из набора исключена &, то ее можно реализовать так: $AB = \neg(\neg A \vee \neg B)$. Если же из набора исключена функция $\vee$, то она может быть реализована так: $X \vee Y = \neg(\neg X \neg Y)$. Таким образом, получаем два функционально полных, причем базисных, набора: {&, $\neg$} и {$\vee$, $\neg$}.

Русский математик Жегалкин показал, что любая булева функция может быть представлена с использованием операций конъюнкции (&), сложения по модулю 2 ($\oplus$) и константы 1. Покажем, как функции набора представить в виде декомпозиции функций Жегалкина: $\neg A = A \oplus 1$; $A \vee B = \neg(\neg A \neg B) = (A \oplus 1)(B \oplus 1) \oplus 1 = AB \oplus A \oplus B \oplus 1 \oplus 1 = AB \oplus A \oplus B$.

Поэтому следующим функционально полным набором (базисным набором) будет набор функций Жегалкина: {&, $\oplus$, 1 }.

Аналогично можно показать, что набор {$\vee$, $\oplus$, 1} – базисный набор.

Выше было показано, что мажоритарная функция после минимизации имеет вид $M(X, Y, Z) = XY \vee XZ \vee YZ$. Если на один из входов мажоритарной функции, например Z, подать константу 1, то получим $M(X, Y, 1) = XY \vee X \vee Y = X \vee Y$, а если на этот же вход Z подать константу 0, то получим $M(X, Y, 0) = XY$. Поэтому получаем еще два базисных набора: {M, $\neg$, 1} и {M, $\neg$, 0}. Когда говорят о «мажоритарном базисе», то имеют в виду эти два набора (или их объединение: {M, $\neg$, 1, 0}, предполагая, что 1 и 0 реализуются «без затрат», а инверсия аргументов всегда присутствует, если комбинационная схема подключается к триггерным устройствам (элементарным автоматам), которые имеют как прямой, так и инверсные выходы.

На практике, как правило, используются базисные наборы, состоящие только из одной функции («штрих Шеффера» или «стрелка Пирса»): {/} и {↓}.

Набор «штрих Шеффера » реализует функцию $S(X, Y) = \neg(XY)$. Инверсия аргумента может быть получена с помощью элемента Шеффера так: $\neg X = \neg(XX)$. Конъюнкция требует использования двух элементов Шеффера: $XY = \neg(\neg(XY))$. Дизъюнкция может быть реализована с помощью трех элементов Шеффера: $X \vee Y = \neg(\neg X \neg Y)$.

Набор «стрелка Пирса» реализует функцию $P(X, Y) = \neg(X \vee Y)$. Инверсия аргумента может быть получена так: $\neg(X \vee X)$. Дизъюнкция может быть получена так: $X \vee Y = \neg(\neg(X \vee Y))$. Конъюнкция может быть получена так: $XY = \neg(\neg X \vee \neg Y)$.

Пример. Перевести в базис Шеффера и Пирса функцию, заданную в дизъюнктивной нормальной форме: $F = \neg AB \vee A \neg CD \vee \neg BD$.

В базисе Шеффера функция будет иметь вид $F = \neg(\neg(\neg AB) \vee \neg(A \neg CD) \vee \neg(\neg BD))$.

В базисе Пирса функция будет иметь вид $F = \neg\neg(\neg(\neg(A \vee \neg B) \vee \neg(\neg A \vee C \vee \neg D) \vee \neg(B \vee \neg D))$.

Примеры для самостоятельной работы.

Представить в базисах Шеффера и Пирса следующие функции (при необходимости предварительно упростить).

1. $AB\overline{CD} \vee \overline{B} \vee AP\overline{QS}\overline{T}$.
2. $\overline{(\overline{(ABC \vee BD)} \vee AC \vee \overline{ACD})}$.
3. $\overline{(XZ \vee \overline{(ZY \vee ZP)})}$.

2.9. Примеры реализации комбинационных схем

Редко задание на проектирование комбинационных схем формулируется в виде перечисления входных наборов и соответствующих им значений функции (таблиц истинности). Часто оно задается в виде некоторого словесного описания работы устройства (комбинационной схемы).

Пример 1. Построить однотактное устройство, реализующее следующий алгоритм работы. На вход устройства подается 5-разрядный двоичный код (X_1, X_2, X_3, X_4, X_5). На выходе вырабатывается 0, если число единиц в коде равно 0 или 1, и вырабатывается 1, если число единиц равно 4 или 5. Остальные случаи не предусмотрены, т. е. на остальных наборах можно проставить «–».

Построим диаграмму Вейча по данному описанию:

X_5 \ X_4	X_3	X_2	X_1					
	–	–	1	–	–	–	–	0
	–	1	1	1	–	1	–	–
	–	–	1	–	–	–	–	0
	0	–	–	–	0	–	0	0

Выпишем решение при очевидном способе доопределения и представим его в базисе Шеффера и Пирса: $F = X_2X_3 \vee X_4X_5 = \overline{(\overline{(X_2X_3)}\,\overline{(X_4X_5)})} = \overline{\overline{(\overline{(\overline{X_2} \vee \overline{X_3})} \vee \overline{(X_4 \vee \overline{X_5})})}}$.

Комбинационные схемы на несколько выходов строятся аналогичным образом, однако часто предпринимаются попытки провести совместную минимизацию схем, реализующих отдельные выходные сигналы. Примерами таких схем могут служить различные преобразователи кодов.

Пример 2. Построить однотактное устройство, преобразующее двоичный код в код Грэя.

Выпишем таблицу истинности 4-х разрядов кода Грэя.

X_4	X_3	X_2	X_1	Y_4	Y_3	Y_2	Y_1
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	1	1
0	0	1	1	0	0	1	0
0	1	0	0	0	1	1	0
0	1	0	1	0	1	1	1
0	1	1	0	0	1	0	1
0	1	1	1	0	1	0	0
1	0	0	0	1	1	0	0
1	0	0	1	1	1	0	1
1	0	1	0	1	1	1	1
1	0	1	1	1	1	1	0
1	1	0	0	1	0	1	0
1	1	0	1	1	0	1	1
1	1	1	0	1	0	0	1
1	1	1	1	1	0	0	0

Число диаграмм Вейча равно четырем, причем для Y_4 она тривиальная ($Y_4 = X_4$), а для остальных имеет вид:

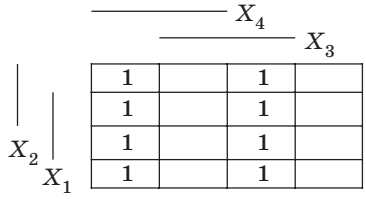
для Y_1: $Y_1 = \overline{X}_1 X_2 \vee X_1 \overline{X}_2 = X_1 \oplus X_2$;

X_2 \ X_4 X_3				
	1	1	1	1
X_1	1	1	1	1

для Y_2: $Y_2 = \overline{X}_2 X_3 \vee X_2 \overline{X}_3 = X_2 \oplus X_3$;

X_2 \ X_4 X_3				
	1			1
	1			1
		1	1	
X_1		1	1	

для Y_3: $Y_3 = X_3 \overline{X}_4 \vee \overline{X}_3 X_4 = X_3 \oplus X_4$.

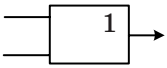


2.10. Изображение комбинационных устройств на функциональных схемах

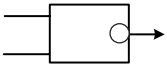
Для изображения комбинационных схем в различных базисах используются следующие обозначения отдельных элементов.

Изображение элемента «И »

Изображение элемента «ИЛИ»

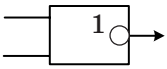


Изображение элемента «НЕ»

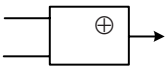


Изображение элемента «И-НЕ» («штрих Шеффера»)

Изображение элемента «ИЛИ-НЕ» («стрелка Пирса»)



Изображение элемента «⊕» (сумма по модулю 2)

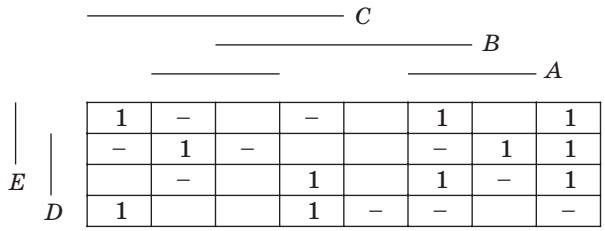


Упражнение. Нарисуйте функциональные схемы двух устройств в различных базисах, которые были синтезированы в подразд. 2.9.

2.11. Задачи для контрольной

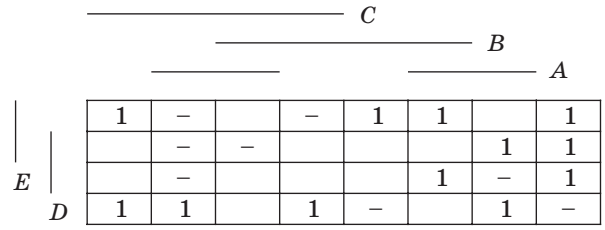
Ниже приводятся примерные задания для контрольной по булевой алгебре и комбинационным схемам.

1. Выпишите минимальное выражение в дизъюнктивной нормальной форме из диаграммы Вейча:



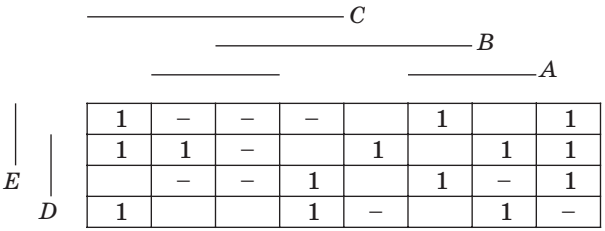
1	–		–		1		1
–	1	–			–	1	1
	–		1		1	–	1
1			1	–	–		–

2. Упростите выражение $\overline{(A\overline{B}\overline{C} \equiv \overline{A}B\overline{C})} / ((\overline{C} \vee \overline{A}\overline{B}) \downarrow (BC))$.
3. Представьте выражение в базисе Пирса двух аргументов:
$AB\overline{C} \vee \overline{D} \vee \overline{B}DE \vee \overline{A}D\overline{E}\overline{F} \vee \overline{A}E\overline{F}$.
4. Выпишите минимальное выражение из диаграммы Вейча:



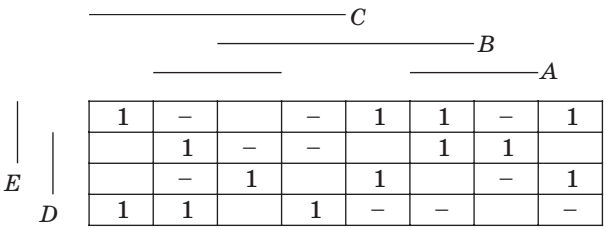
1	–		–	1	1		1
	–	–				1	1
	–				1	–	1
1	1		1	–		1	–

5. Упростите выражение $(AB\overline{C} \to \overline{A}B\overline{C}) \equiv (\overline{C} \oplus (\overline{A}\overline{B} \downarrow \overline{B}C))$.
6. Выпишите минимальное выражение из диаграммы Вейча:



1	–	–	–		1		1
1	1	–		1		1	1
	–	–	1		1	–	1
1			1	–		1	–

7. Представьте выражение в базисе Пирса трех аргументов:
$XY\overline{Z} \vee \overline{P} \vee \overline{X}\overline{P}Q \vee \overline{X}PQ\overline{L}\overline{M} \vee \overline{X}L\overline{M}$.
8. Упростите выражение $\overline{(A\overline{B} \to \overline{C} \equiv AB\overline{C})} / \overline{(\overline{C} \vee \overline{A}\overline{B} \oplus BC)}$.
9. Представьте выражение в базисе Пирса трех аргументов:
$A\overline{C}\overline{D} \vee \overline{D}E \vee \overline{A}\overline{D} \vee \overline{A}BCDE\overline{F} \vee \overline{A}BCDE\overline{F}$.
10. Выпишите минимальное выражение из диаграммы Вейча:



1	–		–	1	1	–	1
	1	–	–		1	1	
	–	1		1		–	1
1	1		1	–	–		–

11. Упростите выражение $\overline{(AB\overline{C} \oplus \overline{AB}C)} / (\overline{C} \vee (\overline{A}\overline{B} \downarrow \overline{BC}))$.

12. Представьте выражение в базисе Пирса двух аргументов: $A\overline{B}\overline{C}\overline{D} \vee \overline{B}\overline{D}E \vee \overline{A}\overline{D}\overline{E}\overline{F} \vee \overline{A \vee E}F$.

Литература

1. *Кузнецов, О. П.* Дискетная математика для инженера / О. П. Кузнецов, Г. М. Адельсон-Вельский. М.: Энергоатомиздат, 1988. 480 с.

2. *Ерош, И. Л.* Дискретная математика. Булева алгебра. Комбинационные схемы. Преобразования двоичных последовательностей: учеб. пособие / И. Л. Ерош. СПбГУАП. СПб., 2001. 38 с.

3. ЭЛЕМЕНТЫ ТЕОРИИ ДИСКРЕТНЫХ ГРУПП ПРЕОБРАЗОВАНИЙ

Теория групп является очень востребованным математическим разделом. Само понятие «группа» является основным при определении других математических моделей, в частности, колец и полей, а также линейных векторных пространств и линейных алгебр. Группы преобразований позволяют описывать различные изменения, которые происходят с объектами исследований. Линейные представления групп позволяют связать два, казалось бы, совершенно различных раздела дискретной математики: групповые преобразования и дискретный спектральный анализ.

Теория групп широко применяется при решении различных задач распознавания образов, а с помощью линейных представлений можно построить характеристики объектов, инвариантные к соответствующим преобразованиям, т. е. характеристики, не зависящие от некоторых изменений, которые происходят с объектами исследования.

3.1. Группы и другие математические модели

3.1.1. Определение и основные свойства групп

Пусть заданы множество U элементов x_1, x_2, x_3... ($x_i \subset U$) и некоторая бинарная операция $\bullet$. Операция $\bullet$ ставит в соответствие любым двум элементам x_i и x_j множества U некоторый третий элемент x_k из этого же множества, т. е. $x_i \bullet x_j = x_k$; $x_i, x_j, x_k \subset U$. В этом случае говорят, что множество U замкнуто относительно операции $\bullet$.

Множество U с бинарной операцией $\bullet$ называют *группой* и обозначают $(U, \bullet)$, если выполняются аксиомы:

1) *ассоциативности*: для любых трех элементов множества U $x_i \bullet x_j \bullet x_k = (x_i \bullet x_j) \bullet x_k = x_i \bullet (x_j \bullet x_k)$. Аксиома ассоциативности «разрешает» при выполнении бинарной операции $\bullet$ над тремя или большим числом элементов множества U расставлять скобки по своему усмотрению, так как результат при этом не меняется;

2) наличия в множестве U *нейтрального элемента* e, такого, что для любого элемента x множества U выполняется: $x \bullet e = e \bullet x = x$. Для числовых множеств в качестве нейтрального элемента e может выступать 0 (при операциях типа сложения) или 1 (при операциях типа умножения);

3) наличия *обратного* элемента: для любого элемента x множества U существует элемент, условно обозначаемый x^{-1}, принадлежащий U

и называемый обратным к x элементом, такой, что $x \bullet x^{-1} = x^{-1} \bullet x = e$, т. е. произведение прямого и обратного к нему элемента дает нейтральный элемент.

Если кроме того для любых элементов x_i и x_j множества U выполняется: $x_i \bullet x_j = x_j \bullet x_i$, то группа называется *коммутативной* или *абелевой*.

В некоторых случаях в множестве U с бинарной операцией $\bullet$ выполняется только первая аксиома (ассоциативности). В этом случае пару $(U, \bullet)$ называют *полугруппой*. Если при этом выполняется и вторая аксиома (аксиома о наличии в U нейтрального элемента e), то пару $(U, \bullet)$ называют *полугруппой с единицей* (точнее было бы говорить о полугруппе с нейтральным элементом). В дальнейшем для краткости мы будем называть полугруппу с единицей просто полугруппой, а при невыполнении второй аксиомы это особо оговаривать.

Рассмотрим некоторые примеры групп и полугрупп.

1. Пусть задано $U = N$ – множество целых (положительных и отрицательных чисел, включая 0) и бинарная операция «обычного» сложения «+». Множество N замкнуто относительно операции сложения. Легко проверяется выполнимость всех трех аксиом: ассоциативности, наличия в множестве U нейтрального элемента и наличия вместе с любым элементом множества элемента, обратного к нему. Кроме того, легко проверяется четвертая (не обязательная для группы) аксиома коммутативности. Таким образом, множество N с бинарной операцией сложения является коммутативной (абелевой) группой.

2. Пусть задано $U = N$ – множество целых чисел (как в предыдущем примере) и бинарная операция умножения. Множество N замкнуто относительно операции умножения, так как произведение любых двух целых чисел есть число целое. Ассоциативность выполняется, так как она выполняется в более «широком» множестве действительных чисел. Нейтральным элементом по умножению является 1. А обратные элементы существуют не для всех элементов (только для 1 существует обратный элемент по умножению, равный 1). Следовательно, множество целых чисел с операцией умножения образует полугруппу.

3. Пусть заданы числа 0, 1, 2, 3, 4 и операция сложения этих чисел по модулю 5, что будем записывать так: N (0, 1, 2, 3, 4), $\oplus \mathrm{mod}5$. Пара $(N, \oplus \mathrm{mod}5)$ образует коммутативную группу. Действительно, складывая любые числа множества N и беря результат по модулю (т. е. находя наименьшее положительное число, не превосходящее 4), мы не выйдем за пределы множества N. Так, например, $2 \oplus 4 = 1 \mathrm{mod}5$; $2 \oplus 3 = 0 \mathrm{mod}5$ и т. п. Легко проверяется аксиома ассоциативности. Нейтральным элементом является 0, и для каждого элемента существует

обратный: $1^{-1} = 4$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 1$. Эта группа коммутативна и определена для любого множества чисел вида $(0, 1, 2, \ldots, n-1, \oplus \bmod n)$.

4. Исключим из множества N в предыдущем примере 0 и запишем это в виде $N/0 = (1, 2, 3, 4)$. Введем на полученном множестве $N/0$ операцию умножения по модулю 5. Так как 5 – простое число, то выполняются все аксиомы группы, что легко проверяется. Так, замкнутость следует из того, что произведение чисел, меньших простого модуля, не кратна ему. Ассоциативность легко доказывается при переходе от сравнения к равенствам. Нейтральным по умножению элементом является 1. Для каждого элемента можно найти обратный: $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$. Обобщая приведенный пример, можно утверждать, что для любого простого числа p пара $(U = 1, 2, 3, \ldots, p-1; \otimes \bmod p)$ образует коммутативную (абелеву) группу.

5. Пусть заданы три элемента a, b, c. Рассмотрим всевозможные перестановки h_i, $i = 0, 1, 2 \ldots 5$ из этих элементов и запишем их в виде

$$h_0 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix},\ h_1 = \begin{pmatrix} a & b & b \\ a & c & c \end{pmatrix},\ h_2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix},\ h_3 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix},$$

$$h_4 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix},\ h_5 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix},$$

где верхняя строка в каждой перестановке указывает порядок элементов до преобразования, а нижняя строка – после преобразования.

Множество этих перестановок образует некоммутативную группу. Бинарная операция в данном случае представляет собой операцию последовательного применения (умножения) перестановок, что записывается $h_i\, h_j$. Легко проверяется, что $h_i\, h_0 = h_0\, h_i = h_i$ для любых $i = 1, 2, 3 \ldots 5$. Обратный элемент может быть получен путем перестановки строк и упорядочивания столбцов так, чтобы восстановить исходный порядок элементов в верхней строке. Например:

$$h_3^{-1} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}^{-1} = \begin{pmatrix} b & c & a \\ a & b & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = h_4,\ h_3 h_4 = h_4 h_3 = h_0.$$

3.1.2. Группы преобразований

Рассмотрим группы, элементами которых являются некоторые преобразования. В последнем примере подподразд. 3.1.1 каждый элемент группы h_i выполнял некоторые перестановки точек a, b, c. Так, элемент h_3 переставляет (преобразует) пары: $a \to b$, $b \to c$, $c \to a$.

В общем случае *преобразованием g* множества U называют взаимно однозначное отображение этого множества на себя. В качестве приме-

ра возьмем круг, вырезанный из картона, и будем вращать его вокруг неподвижного центра O. Заметим положения некоторых точек до и после поворота. Каждый произвольный поворот меняет положение точек. Можно говорить, что поворот осуществляет преобразование на множестве точек круга, при этом такое преобразование является взаимно однозначным.

Пусть задано множество U с элементами $x \in U$. Рассмотрим некоторое преобразование g элементов множества U. Образ элемента x из U (результат преобразования) обозначим gx. Если совокупность преобразований $g \in U$ образует группу преобразований множества U, то каждому элементу g группы G ставится в соответствие преобразование, переводящее элемент x в gx, т. е. $x \to gx \in U$. Нейтральному элементу группы $e \in U$ ставится в соответствие преобразование $x \to ex = x$.

Для любых двух элементов g_1 и g_2 из G выполняется равенство (по определению)

$$(g_1 g_2)x = g_1(g_2 x). \tag{3.1}$$

Примерами групп преобразований могут служить:

– группа всех перестановок из n элементов;

– группа вращений плоскости вокруг неподвижного центра;

– группа движений плоскости (смещения вдоль координатных осей и вращение вокруг неподвижного центра);

– группы преобразований точек плоскости уравнениями Ли и т. п.

Во всех этих примерах бинарной операцией $\bullet$ является операция последовательного выполнения преобразований, т. е. в выражении (3.1) сначала над элементом x выполняется преобразование g_2, а затем над полученным результатом $g_2 x$ выполняется преобразование g_1.

3.1.3. Циклические группы

Пусть g – некоторый элемент группы G конечного порядка. Заметим, что порядком группы называют число ее элементов. Так, группа перестановок трех элементов a, b, c, рассмотренная в п. 5 подподразд. 3.1.1, имеет порядок 6. Группа вращений круга имеет бесконечный континуальный порядок. Группа вращений правильного n-угольника, при которых происходит самосовмещение вершин, имеет конечный порядок n.

Образуем произведения вида $gg = g^2 = g_1$, $ggg = g^3 = g_2$, $gggg = g^4 = g_3$. Поскольку число элементов группы конечно, найдется такое значение k, что $g^k = g^l$, где $l < k$, откуда $g^{k-l} = e$. Обозначим $k - l = n$, тогда $g^n = e$. Набор элементов e, g^1, g^2,..., g^{n-1} образует *циклическую* группу. Действительно, ассоциативность обеспечивается ассоциативностью исход-

ной группы, нейтральным элементом является $g^0 = e$, обратным к g^s элементом является элемент g^{n-s}, так как $g^s g^{n-s} = g^{n-s} g^s = g^n = e$. Эта группа коммутативна, поскольку коммутативна операция сложения целых чисел: $g^s g^l = g^{s+l} = g^{l+s} = g^l g^s$.

Рассмотрим примеры построения циклических групп.

Пример 1. Пусть имеется 5 различных элементов. Для простоты обозначим их целыми числами 1, 2, 3, 4, 5. Выпишем нейтральную h^0 и какую-либо h перестановку:

$$h^0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}.$$

Найдем степени перестановки h:

$$h^2 = hh = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix},$$

$$h^3 = h^2 h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix},$$

$$h^4 = h^3 h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix},$$

$$h^5 = h^4 h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix},$$

$$h^6 = h^5 h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = h^0.$$

Таким образом, степени некоторой перестановки h, а именно: $h^0 = e$, h^1, h^2, h^3, h^4, h^5 образуют циклическую группу. Легко проверить, что эта группа коммутативна.

Пример 2. Пусть задана матрица $\mathbf{A}$ с элементами $\{0, 1\}$ и определителем, равным 1, над полем $GF(2)$:

$$\mathbf{A} = \begin{pmatrix} 01101 \\ 10110 \\ 11010 \\ 01001 \\ 11000 \end{pmatrix}.$$

Будем возводить ее последовательно в степени 2, 3, 4, ... При возведении в 12-ю степень получим единичную матрицу

$$\mathbf{E} = \begin{pmatrix} 10000 \\ 01000 \\ 00100 \\ 00010 \\ 00001 \end{pmatrix}.$$

Множество матриц $\{\mathbf{E}, \mathbf{A}, \mathbf{A}^2, \mathbf{A}^3, \ldots, \mathbf{A}^{11}\}$ образует циклическую (коммутативную) группу.

3.1.4. Математические модели

Кольца

Пусть на множестве U заданы две операции: типа сложения и типа умножения. Запишем это так: $(U, «+», «\bullet»)$. Пусть $(U, «+»)$ – коммутативная группа с нейтральным элементом $e = 0$, а $(U/0, «\bullet»)$ образует полугруппу, где $U/0$ обозначает множество U с «выколотым» нулем. Тогда множество U с этими двумя операциями «+» и «•» есть *кольцо*.

Примеры.

1. Пусть N – множество целых чисел (положительных, отрицательных и 0). Множество N с операцией «обычного» сложения образует коммутативную группу с нейтральным элементом по сложению 0. То же множество N с «выколотым» (исключенным) нулем с операцией умножения образует полугруппу (так как не для всех элементов множества N существуют обратные элементы по умножению). Поэтому $(N, +, \times)$ – кольцо, которое называют кольцом целых чисел.

2. Возьмем множество U полиномов степени не выше n вида $R(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0$, $Q(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x^1 + b_0$, где a_i, b_j – произвольные действительные числа. Определим на множестве полиномов операцию сложения: $R(x) + Q(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \ldots + (a_1 + b_1)x^1 + (a_0 + b_0)$.

Легко убедиться, что при такой операции сложения множество полиномов образует коммутативную группу по сложению с нейтральным полиномом $e = 0$. Исключим нейтральный полином из множества U и введем на оставшемся множестве $U/0$ операцию умножения. Ее нельзя ввести «естественным» образом, т. е. в виде почленного произведения полиномов, так как в этом случае степень результирующего полинома может оказаться выше n. Для того чтобы этого не произошло, введем операцию умножения полиномов так, чтобы степени полиномов при

умножении складывались по модулю $n + 1$. В этом случае степень результирующего полинома не будет превосходить n. В общем виде это можно записать так: $R(x) \bullet Q(x) = \ldots a_l b_s x^{l \oplus s \bmod(n+1)} \ldots$, где l и s принимают все возможные значения от n до 0.

Например, пусть мы имеем полиномы степени не выше 4. Для конкретности возьмем произведение двух полиномов: $R(x) = 3x^4 + 2x^2 + 5$; $Q(x) = x^4 + 4x^3 + x$. Тогда произведение полиномов R и Q будет иметь вид $(3x^4 + 2x^4 + 5) \bullet (x^4 + 4x^3 + x) = 3x^{8 \bmod 5} + 2x^{6 \bmod 5} + 5x^{4 \bmod 5} + 12x^{7 \bmod 5} + 8x^{5 \bmod 5} + 20x^{3 \bmod 5} + 3x^{5 \bmod 5} + 2x^{3 \bmod 5} + 5x = 5x^4 + 25x^3 + 12x^2 + 17x + 11$ (т. е. степень результирующего полинома не превосходит 4).

При такой операции умножения полиномов свойство замкнутости множества относительно операции умножения будет выполнено. Легко проверяется аксиома ассоциативности. Нейтральный элемент по умножению $e = 1$ (точнее, нейтральный элемент равен полиному, у которого все коэффициенты кроме a_0 равны 0, а $a_0 = 1$). Однако не для всякого полинома существует обратный, т. е. аксиома об обратном элементе на множестве $U/0$ не выполняется. Таким образом, множество полиномов степени не выше n с введенными выше операциями сложения и умножения образует кольцо. Оно называется *кольцом полиномов степени не выше n*.

Поля

Пусть на множестве U задано две операции: типа сложения «+» и типа умножения «•». Множество U с операцией «+» пусть образует коммутативную группу с нейтральным элементом $e = 0$. А множество $U/0$ с операцией «•» также образует группу. Тогда (U, «+», «•») есть *поле*.

Примеры.

1. U – множество действительных чисел, на котором введены операции «обычного» сложения и умножения. (U, +) – коммутативная группа с нейтральным элементом $e = 0$. Множество ($U/0$, ×) – также коммутативная группа. Следовательно, (U, +, ×) есть поле. Это поле имеет бесконечное континуальное множество элементов и называется полем действительных чисел.

2. Возьмем в качестве U конечную совокупность чисел: $N = 0, 1, 2, 3, 4$ и зададим две операции: $\oplus \bmod 5$ и $\otimes \bmod 5$. Как было показано выше, пары (N, $\oplus \bmod 5$) и ($N/0$, $\otimes \bmod 5$) – коммутативные группы. Следовательно, (N, $\oplus \bmod 5$, $\otimes \bmod 5$) есть поле с конечным числом элементов. Обобщая полученный пример, можно утверждать, что для любого простого числа p существует поле с конечным числом элементов $p = 0, 1, 2, 3, \ldots, p-1$. Такие поля называются *полями Галуа* и обозначаются $GF(p)$ – поле Галуа с p элементами.

Определим теперь модели с двумя классами объектов.

Линейные векторные пространства

Пусть L – множество объектов, которые условно назовем векторами и обозначим $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$,... . Введем на множестве векторов операцию сложения так, чтобы $(L, +)$ была бы коммутативной группой. Введем операцию умножения скаляра на вектор так, чтобы результат был вектором того же множества L: $\alpha\mathbf{A} = \mathbf{B} \in L$. Множество скаляров $\alpha, \beta, \gamma,\ldots$ должно принадлежать числовому кольцу или полю. Если при этом выполняется набор аксиом дистрибутивности: $(\alpha+\beta)\mathbf{A} = \alpha\mathbf{A} + \beta\mathbf{A}$, $\alpha(\mathbf{A}+\mathbf{B}) = \alpha\mathbf{A}+\alpha\mathbf{B}$, кроме того, $0\mathbf{A} = 0$, $1\mathbf{A} = \mathbf{A}$ для всех векторов L, то L является *линейным векторным пространством*. Первым классом объектов является множество векторов. Вторым классом объектов является множество скаляров.

Примеры.

1. Возьмем плоскость с декартовой системой координат. Каждой точке плоскости можно сопоставить вектор, выходящий из начала координат и заканчивающийся в данной точке. Каждому вектору можно сопоставить пару чисел, соответствующих проекциям его на координатные оси, причем эти соответствия будут взаимно однозначными. Таким образом, задав пару чисел (a, b), мы можем считать, что задали вектор на плоскости, выходящий из начала координат. Обозначим множество таких двумерных векторов через L. Введем на множестве векторов операцию сложения: $(a, b)+(c, d) = (a+c, b+d)$. Легко убедиться в том, что множество векторов L с такой операцией сложения образует коммутативную группу. Введем операцию умножения скаляра на вектор: $\alpha(a, b) = (\alpha a, \alpha b)$. Аксиомы дистрибутивности выполняются, следовательно, множество таких векторов образует линейное двумерное векторное пространство.

Рассмотрим теперь тройки чисел вида (a, b, c) и назовем их векторами в трехмерном пространстве. Введем операцию сложения трехмерных векторов аналогично двумерным, т. е. компоненты трехмерного вектора будут равны сумме соответствующих компонентов слагаемых векторов. Введем операцию умножения скаляра на трехмерный вектор, при которой компоненты вектора умножаются на скаляр. В этом случае легко проверить, что все аксиомы дистрибутивности выполняются. Следовательно, мы построили трехмерное линейное векторное пространство.

Рассмотрим теперь объекты вида $(a_1, a_2, a_3, \ldots, a_n)$, где все a_i принадлежат полю действительных чисел, а сами объекты назовем n-мерными векторами. Аналогично рассмотренным случаям введем операции сложения n-мерных векторов и умножения скаляров на n-мерный вектор. Проверив, что такие векторы образуют коммутативную груп-

пу относительно операции сложения и выполняются аксиомы дистрибутивности, мы можем считать, что построили линейное n-мерное векторное пространство.

Если считать, что все компоненты n-мерного вектора (c_1, c_2, c_3,..., c_n) есть комплексные числа, то, введя аналогичным образом операции сложения векторов и умножения скаляра на вектор и проверив выполнимость всех аксиом, получим линейное n-мерное комплекснозначное векторное пространство.

2. Рассмотрим всевозможные непрерывные функции с интегрируемым квадратом, заданные на интервале $[a, b]$. Введем операцию сложения двух функций $F_1(x) + F_2(x) = F_3(x)$ так, что значение функции F_3 в каждой точке интервала равно сумме значений функций F_1 и F_2 в этой же точке. Каждую функцию условно можно назвать вектором, тогда относительно операции сложения множество непрерывных функций на интервале $[a, b]$ образует коммутативную группу. Введя операцию масштабирования функции (умножения скаляра на функцию), мы можем убедиться в том, что все аксиомы дистрибутивности будут выполняться. Таким образом, мы получили линейное векторное пространство функций с интегрируемым квадратом, заданных на интервале $[a, b]$. Это пространство будет бесконечномерным (континуальным).

Линейные алгебры

Возьмем линейное векторное пространство L и введем операцию умножения векторов друг на друга так, чтобы множество векторов образовывало относительно операции умножения полугруппу или группу. В первом случае мы получаем *алгебру без деления*, во втором – *алгебру с делением*.

Примеры.

1. Взяв множество действительных чисел и рассматривая их как совокупность одномерных векторов с операциями сложения векторов и умножения скаляра на вектор, мы получим одномерное линейное векторное пространство. Введя операцию умножения одномерных векторов друг на друга и убедившись в том, что относительно такой операции множество одномерных векторов образует коммутативную группу, можно считать, что мы построили линейную алгебру действительных чисел с делением.

2. Рассмотрим объекты вида $a_0 + ia_1$, где a_0 и a_1 принадлежат полю действительных чисел, $i^2 = -1$. Такие объекты называют комплексными числами. Введем операцию сложения комплексных чисел по правилу $(a_0 + ia_1) + (b_0 + ib_1) = (a_0 + b_0) + i(a_1 + b_1)$. То есть в результате сложения комплексных чисел получаем комплексное число (замкнутость). Легко проверяются аксиомы группы по сложению комплексных

чисел. Операция умножения скаляра на комплексное число $\alpha(a_0 + ia_1) = (\alpha a_0 + i\alpha a_1)$. Аксиомы дистрибутивности в этом случае выполняются. Введем операцию умножения комплексных чисел $(a_0 + ia_1) \bullet (b_0 + ib_1) = (a_0 b_0 - a_1 b_1) + i(a_1 b_0 + a_0 b_1)$. То есть в результате умножения двух комплексных чисел получаем комплексное число. Кроме того, для любых комплексных чисел кроме $0 + i0 = 0$ существует обратный элемент по умножению. Для того чтобы его найти, введем сопряженное комплексное число $\overline{a_0 + ia_1} = a_0 - ia_1$. Тогда обратный элемент по умножению равен $(a_0 + ia_1)^{-1} = \dfrac{a_0 - ia_1}{a_0^2 + a_1^2}$. Знаменатель дроби есть квадрат модуля комплексного числа.

Таким образом, множество комплексных чисел с введенными операциями сложения, умножения на скаляр и умножения комплексных чисел друг на друга образует линейную алгебру комплексных чисел с делением.

3. Рассмотрим объекты вида $a_0 + ia_1 + ja_2 + ka_3$, где a_0, a_1, a_2, a_3 принадлежат полю действительных чисел; $i^2 = j^2 = k^2 = -1$, при этом

$$ij = k,\ ji = -k;$$

$$jk = i,\ kj = -i;$$

$$ki = j,\ ik = -j.$$

Такие объекты называют *кватернионами*. Аналогично операциям сложения и умножения комплексных чисел вводятся операции сложения и умножения кватернионов. Обратный кватернион по умножению определяется аналогично обратному комплексному числу:

$$\left(a_0 + ia_1 + ja_2 + ka_3\right)^{-1} = \frac{a_0 - ia_1 - ja_2 - ka_3}{a_0^2 + a_1^2 + a_2^2 + a_3^2}.$$

В результате получаем линейную алгебру кватернионов с делением. В отличие от линейной алгебры комплексных чисел она является некоммутативной по умножению.

4. Ранее рассматривались объекты, названные полиномами степени не выше n, и на множестве таких полиномов вводились операции сложения и умножения. Можно ввести операцию умножения скаляра на полином в виде умножения скаляра на каждый член полинома, при этом, как легко убедиться, аксиомы дистрибутивности выполняются. Однако относительно операции умножения множество полиномов образует полугруппу. Следовательно, множество полиномов с такими операциями образует линейную алгебру полиномов без деления.

3.1.5. Задачи для контрольной

Группы и полугруппы

Определить, к какой математической модели (группе или полугруппе) относятся следующие множества с заданными операциями (либо не относятся ни к одной из перечисленных).

1. $U = R$ – множество действительных чисел; $\bullet$ – бинарная операция сложения.

2. $U = R$; $\bullet$ – бинарная операция умножения.

3. $U = R/0$ – множество действительных чисел с «выколотым» нулем, т. е. из множества действительных чисел исключено только число 0, а остальные числа, даже сколь угодно малые, остались; $\bullet$ – бинарная операция умножения.

4. $U = C$ – множество комплексных чисел; $\bullet$ – бинарная операция сложения.

5. $U = C$; $\bullet$ – бинарная операция умножения.

6. $U = C/0$; $\bullet$ – бинарная операция умножения.

7. $U = N_5$ – конечное множество, состоящее из элементов 0, 1, 2, 3, 4; $\bullet$ – бинарная операция сложения по модулю 5.

8. $U = N_5$; $\bullet$ – бинарная операция умножения по модулю 5.

9. $U = N_5/0$ – конечное множество с «выколотым» нулем, т. е. множество, состоящее из элементов 1, 2, 3, 4; $\bullet$ – бинарная операция умножения по модулю 5. Пояснение: операции сложения или умножения по модулю M выполняются следующим образом: сначала выполняется операция «обычного» сложения или умножения, а затем результат делится на M и берется наименьший положительный остаток от деления. Например, $2 + 4 = 6 \equiv 1 \bmod 5$; $3 \bullet 4 = 12 \equiv 2 \bmod 5$. Здесь использованы обозначения, принятые в теории чисел, а именно знак сравнения: $a \equiv b \bmod M$ означает, что a и b имеют одинаковые остатки при делении на M.

10. $U = N_M$ – конечное множество, состоящее из целых чисел от 0 до $M-1$; $\bullet$ – бинарная операция сложения по модулю M. Постройте группу (проверить все аксиомы, найти нейтральный элемент по сложению e и для каждого элемента – обратный к нему элемент по сложению) для следующих значений M: 3, 6, 7, 8, 9, 10, 11. Обобщите полученные результаты и постройте группу в общем виде.

11. $U = N_M/0$ – те же конечные множества, что и в примерах 10, но с исключенным 0; $\bullet$ – бинарная операция умножения по модулю M. Попытайтесь построить группы для M = 3, 4, 6, 7, 8, 9, 10, 11. Для каких значений модулей M будут существовать группы с операцией умножения по модулю? Проверьте выполнимость групповых аксиом и в случае существования группы найдите обратные элементы. Обобщите группу с операцией умножения по модулю.

12. U – множество кватернионов; $\bullet$ – бинарная операция сложения кватернионов. Образует ли эта пара группу и какую (коммутативную или некоммутативную)?

13. U – множество кватернионов; $\bullet$ – бинарная операция умножения кватернионов. Образует ли группу эта пара?

14. U – множество кватернионов с «выколотым» нулем (нулевым кватернионом); $\bullet$ – бинарная операция умножения кватернионов. Образует ли группу эта пара? Является ли группа (если она есть) коммутативной?

15. Пусть U – множество полиномов степени не выше n; $\bullet$ – бинарная операция сложения полиномов, указанная выше. Образует ли данное множество группу с такой операцией сложения и какую?

16. Пусть U – множество полиномов степени не выше n; $\bullet$ – бинарная операция умножения. Образует ли группу пара $(U, \bullet)$?

17. Пусть U – множество всех трехразрядных двоичных векторов, $\oplus$ – операция поразрядного сложения векторов по модулю 2. Образует ли это множество с данной операцией группу? Какую? Найдите нейтральный элемент и для каждого вектора элемент, обратный к нему.

18. Для операции сложения векторов в предыдущем примере рассмотрите множество n-разрядных векторов. В каком случае они образуют группу? Какую?

19. Пусть U – множество матриц размера 2×2; $+$ – бинарная операция сложения матриц. Образует ли множество матриц с такой операцией группу? Какую?

20. Пусть U – множество матриц размера 2×2; $\bullet$ – бинарная операция умножения. Образует ли пара $(U, \bullet)$ группу?

21. Из множества матриц U исключим матрицы с определителем, равным нулю. Полученное множество обозначим $U/0$. Образует ли полученная пара $(U/0, \bullet)$ группу с операцией умножения матриц? Какую?

22. Пусть U – множество матриц с определителем, равным единице. Образует ли это множество матриц группу с операцией умножения матриц?

23. Пусть U – множество матриц вида $\mathbf{K} = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$, где k – любое действительное число. Образует ли это множество группу с операцией умножения матриц?

24. Исключим из множества U предыдущего примера нулевую матрицу (т. е. матрицу, в которой $k = 0$). Образует ли множество $U/0$ группу с операцией умножения матриц?

25. Пусть U – множество матриц вида $\mathbf{K} = \begin{pmatrix} k_1 & 0 \\ 0 & k_2 \end{pmatrix}$, где k_1, k_2 – любые действительные числа. Образует ли это множество матриц группу с операцией умножения матриц?

26. Исключим из множества матриц предыдущего примера матрицу с определителем, равным нулю, и обозначим $U/0$. Образует ли это множество матриц группу?

27. Возьмем 4 точки a, b, c, d и рассмотрим всевозможные перестановки этих точек. Число перестановок n элементов равно $P_n = n!$. При $n = 4$ число перестановок $P_4 = 24$. Показать, что множество таких перестановок образует некоммутативную группу. Найти обратные элементы для некоторых перестановок и некоммутативную пару.

Другие математические модели

1. Постройте кольцо целых чисел, введя и проверив необходимые аксиомы.

2. Проверьте выполнимость аксиом кольца целых чисел из множества N_{11} с операциями сложения и умножения по модулю 11. Образует ли это множество с данными операциями поле?

3. Образует ли множество полиномов степени не выше n кольцо или поле?

4. Образует ли множество чисел 0, 1, 2, 3, 4, 5 с операциями сложения и умножения по модулю 6 кольцо или поле?

5. Образует ли множество чисел 0, 1, 2, 3, 4, 5, 6, 7 с операциями сложения и умножения по модулю 8 кольцо или поле?

6. Рассмотрите всевозможные полиномы степени не выше 10. Как определить операцию умножения полиномов, чтобы обеспечить замкнутость полиномов относительно такой операции умножения?

7. Рассмотрите всевозможные полиномы степени не выше 12. Как определить операцию умножения полиномов, чтобы обеспечить замкнутость полиномов относительно такой операции умножения?

8. Рассмотрите всевозможные полиномы степени не выше 4. Как определить операцию умножения полиномов, чтобы обеспечить замкнутость полиномов относительно такой операции умножения?

9. Рассмотрите всевозможные полиномы степени не выше 5. Как определить операцию умножения полиномов, чтобы обеспечить замкнутость полиномов относительно такой операции умножения?

10. Какие операции нужно ввести и какие аксиомы проверить, чтобы получить алгебру полиномов степени не выше n? Будет ли эта алгебра с делением или нет?

11. Рассмотрим непрерывные функции на интервале $[a, b]$. Введите необходимые операции, чтобы построить линейное векторное пространство функций на интервале $[a, b]$. Что нужно дополнительно определить, чтобы построить из этого линейного векторного пространства линейную алгебру?

12. Опишите алгебру кватернионов и сравните ее с алгеброй комплексных чисел.

13. Постройте кольцо полиномов с коэффициентами из поля действительных чисел без ограничения максимальной степени полиномов. Обратите внимание, как в этом случае вводится операция умножения полиномов.

14. Проверьте выполнимость аксиом кольца целых чисел из множества N_{17} с операциями сложения и умножения по модулю 17. Образует ли это множество с данными операциями поле?

15. Постройте алгебру матриц размера 2×2 с коэффициентами из поля действительных чисел.

16. Попытайтесь построить алгебру комплексных чисел с коэффициентами из кольца целых чисел. Будет ли она алгеброй с делением?

17. Постройте алгебру комплексных чисел с коэффициентами из поля Галуа $GF(11)$.

18. Постройте алгебру комплексных чисел с коэффициентами из поля Галуа $GF(13)$.

19. Постройте алгебру кватернионов с коэффициентами из кольца целых чисел.

20. Постройте алгебру кватернионов с коэффициентами из поля Галуа $GF(11)$.

21. Постройте алгебру кватернионов с коэффициентами из поля Галуа $GF(13)$.

22. Постройте алгебру полиномов степени не выше n с коэффициентами из кольца целых чисел. Будет ли эта алгебра алгеброй с делением или без?

23. Постройте алгебру полиномов степени не выше n с коэффициентами из некоторого поля Галуа. Будет ли эта алгебра алгеброй с делением или без?

24. Опишите алгебру комплексных чисел.

25. Постройте кольцо полиномов с коэффициентами из кольца целых чисел без ограничения максимальной степени полиномов. Обратите внимание, как в этом случае вводится операция умножения полиномов.

Приведем примеры ответов на вопросы подразд. 3.1.

1. U – множество кватернионов; $\bullet$ – бинарная операция умножения кватернионов. Образует ли группу эта пара?

Ответ: Кватернионом называют полином вида $a_0 + ia_1 + ja_2 + ka_3$, где a_0, a_1, a_2, a_3 принадлежат полю действительных чисел, при этом $i^2 = j^2 = k^2 = -1$. Кроме того, $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, $ik = -j$.

Введем операцию умножения кватернионов, для этого перемножим два кватерниона:

$$(a_0 + ia_1 + ja_2 + ka_3) \bullet (b_0 + ib_1 + jb_2 + kb_3) =$$
$$= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) + i(a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2) +$$
$$+ j(a_2b_0 + a_0b_2 + a_3b_1 - a_1b_3) + k(a_3b_0 + a_0b_3 + a_1b_2 - a_2b_1). \qquad (1)$$

Таким образом, в результате умножения двух кватернионов получен также кватернион (выполняется замкнутость множества кватернионов относительно такой операции умножения). Ассоциативность умножения кватернионов следует из того, что коэффициенты принадлежат полю действительных чисел. Нейтральным кватернионом по умножению будет кватернион вида $e = 1 + i0 + j0 + k0 = 1$. Для любого кватерниона (кроме нулевого) имеется обратный кватернион

$$\left(a_0 + ia_1 + ja_2 + ka_3\right)^{-1} = \frac{a_0 - ia_1 - ja_2 - ka_3}{a_0^2 + a_1^2 + a_2^2 + a_3^2}.$$

Проверим, выполняется ли аксиома коммутативности умножения кватернионов. Для этого перемножим кватернионы в обратном порядке:

$$(b_0 + ib_1 + jb_2 + kb_3) \bullet (a_0 + ia_1 + ja_2 + ka_3) =$$
$$= (b_0a_0 - b_1a_1 - b_2a_2 - b_3a_3) + i(b_1a_0 + b_0a_1 + b_2a_3 - b_3a_2) +$$
$$+ j(b_2a_0 + b_0a_2 + b_3a_1 - b_1a_3) + k(b_3a_0 + b_0a_3 + b_1a_2 - b_2a_1). \qquad (2)$$

Из сравнения (1) и (2) следует, что операция умножения кватернионов не коммутативна.

Таким образом, множество кватернионов K с операцией умножения не образует группу, так как для нулевого кватерниона не существует обратного по умножению. Однако то же множество K с исключенным нулевым кватернионом, т. е. $K/0$, образует некоммутативную группу.

2. Постройте кольцо полиномов с коэффициентами из поля действительных чисел без ограничения максимальной степени полиномов. Обратите внимание, как в этом случае вводится операция умножения полиномов.

Ответ: Полиномом произвольной (неограниченной) степени называют многочлен вида $R(X) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots$

Для таких полиномов операция сложения и умножения вводится «естественным» образом, т. е. путем почленного сложения и умножения коэффициентов при соответствующих степенях. При этом замкнутость по умножению выполняется, так как максимальная степень полинома не ограничивается. Нейтральным полиномом по сложению является нулевой полином, т. е. $e = 0 + 0x + 0x^2 + 0x^3 + \ldots = 0$. Нейтральным по умножению полиномом является единичный полином, т. е. $e = 1 + 0x + 0x^2 + 0x^3 + \ldots = 1$.

Однако не для каждого полинома существует обратный, поэтому множество таких полиномов с операциями сложения и умножения образует кольцо.

3.2. Группы преобразований и линейные представления

3.2.1. Однородные пространства. Классы транзитивности

Часто множество U с элементами $x \in U$ называют *пространством* U, не наделяя его никакими свойствами. В этом случае элементы x называют точками пространства U.

Пусть в пространстве U действует некоторая группа G. Если для любых двух точек x и y пространства U в группе G найдется элемент такой, что $y = gx$, то U называют *однородным пространством* с группой преобразований G. Группу G в этом случае называют *транзитивной группой* в пространстве U. Так, например, группа вращений плоскости вокруг неподвижного центра O не является транзитивной на плоскости, поскольку можно выбрать такие точки x и y на плоскости, которые никаким вращением вокруг центра O совместить нельзя (x и y находятся на разных расстояниях от центра вращения O).

Если взять любую окружность с центром в точке O, то ее точки образуют однородное пространство (подпространство точек всей плоскости) с группой вращения вокруг этого центра. Группа вращений является транзитивной на такой окружности. Группа движений плоскости является транзитивной на плоскости, поскольку для любых двух точек x и y всегда найдется такое движение g, которое совместит x и y, т. е. $y = gx$.

Если группа G не является транзитивной в пространстве U, то пространство U распадается на непересекающиеся классы точек (подпространства) такие, что две любые точки одного подпространства можно перевести друг в друга преобразованием некоторым элементом группы G, а точки разных подпространств не переводятся друг в друга никакими преобразованиями из группы G. Такие классы точек (подпространства пространства U) называют *классами транзитивности*. Таким образом, каждый класс транзитивности является однородным подпространством с группой преобразований G.

Например, пусть U – трехмерное евклидово пространство; G – группа вращений пространства вокруг центра O. Группа не является транзитивной во всем пространстве U, поскольку, если в качестве x и y взять точки, находящиеся на разном расстоянии от центра O, то никаким вращением их нельзя совместить. Все пространство группой G разбивается на непересекающиеся классы транзитивности (сферы разных радиусов с центром в точке O). Каждая сфера является однород-

ным пространством с группой G, поскольку любые две точки сферы совмещаются некоторым вращением. Группа G будет транзитивна на каждой сфере.

3.2.2. Подгруппы. Стационарные подгруппы

Часть элементов G_1 группы G, удовлетворяющая аксиомам группы, называется *подгруппой* G_1 группы G.

Пример 1. Группа всех действительных чисел R с операцией сложения $(R, +)$ содержит подгруппу всех целых чисел Z с той же операцией $(Z, +)$.

Пример 2. Группа всех комплексных чисел с исключенным 0 и операцией умножения, т. е. $(C/0, \bullet)$, содержит в качестве подгруппы группу $(R/0, \bullet)$.

Пример 3. Группа всех движений плоскости с координатными осями содержит подгруппы смещений вдоль одной и другой оси и подгруппу вращения плоскости вокруг некоторого неподвижного центра.

Пусть G – транзитивная группа преобразований пространства U, a – некоторая фиксированная точка этого пространства. Рассмотрим все элементы h группы G, оставляющие точку a на месте, т. е. такие, что $ha = a$. Одним из таких элементов является нейтральный элемент, так как $ea = a$. Множество таких элементов $\{h\}$ обозначим через H. Покажем, что H – группа, причем H является подгруппой группы G.

Действительно, ассоциативность обеспечивается тем, что элементы h являются также и элементами G. Нейтральный элемент e входит в выбранное множество $\{h\}$. Остается показать, что для любого элемента $h \in H$ обратный элемент h^{-1} также принадлежит H, т. е. оставляет точку a на месте. Это следует из соотношений $ha = a$; $h^{-1}ha = h^{-1}a = a$.

Таким образом, множество элементов $\{h\}$ образует подгруппу H группы G, которая называется *стационарной подгруппой* группы G точки a и обозначается H_a.

Если преобразование $g \in G$ переводит точку a в некоторую точку x, т. е. $x = ga$, то все остальные преобразования g_1, переводящие a в x, имеют вид $g_1 = gh$, где $h \in H$. Множество таких преобразований gh, $h \in H$, $g \in G$ называется *левым смежным классом* gH группы G по подгруппе H. Поскольку группа G транзитивна в пространстве U, то этим устанавливается взаимно однозначное соответствие между точками x пространства U и левыми смежными классами по H. Преобразование $x \to gx$ при этом соответствии переходит в умножение слева на g: если точке x соответствует смежный класс g_1H, то точке gx соответствует смежный класс gg_1H. Заметим, что стационарная подгруппа H не определяется однозначно заданием однородного пространства U, а зависит еще и от выбора точки a.

Выясним, как связаны между собой стационарные подгруппы различных точек. Пусть H – стационарная подгруппа точки a в пространстве U и пусть преобразование g переводит точку a в точку b, т. е. $b = ga$. Преобразование вида ghg^{-1} оставляет точку b на месте. Таким образом, стационарной подгруппой точки b является подгруппа gHg^{-1}, которая называется *сопряженной стационарной подгруппе* H точки a. Поскольку группа G транзитивна в U, все стационарные подгруппы точек U сопряжены между собой. Таким образом, каждому однородному пространству U с группой преобразований G соответствует класс сопряженных подгрупп в G (стационарных подгрупп точек пространства U).

3.2.3. Делители группы. Нормальные делители

Любая подгруппа G_1 группы G называется *делителем группы* G, поскольку при конечном числе элементов в G порядок (число элементов) группы G делится без остатка на порядок группы G_1.

Пусть G_1 – делитель группы G и пусть g – элемент группы G, не входящий в G_1. Будем называть gg_1g^{-1} элементом, преобразованным из g_1 при помощи g. Совокупность элементов gg_1g^{-1}, где g_1 пробегает всю группу G_1, будем обозначать gG_1g^{-1}. Эта совокупность также образует группу. Можно показать, что группа gG_1g^{-1} изоморфна группе G_1. Такие группы называются *сопряженными*.

Если всякая группа gG_1g^{-1} при любом $g \in G$ совпадает с G_1, то G_1 называют *нормальным делителем группы* G.

Пример. Пусть G – группа матриц размера $n \times n$ с действительными элементами, а G_1 – группа унимодулярных матриц, т. е. матриц с определителем, равным 1. Тогда G_1 есть нормальный делитель G. Действительно, так как $g_1 \in G_1$, то $|g_1| = 1$. В то же время при любом $g \in G$ и $g_1 \in G_1$ $|gg_1g^{-1}| = |g|\,|g_1|\,|g^{-1}| = 1$. Таким образом, группа gG_1g^{-1} тоже унимодулярна.

Можно вывести и более простой способ проверки, является ли G_1 нормальным делителем G. Из условия $gG_1g^{-1} = G_1$ следует, что $gG_1 = G_1g$.

3.2.4. Фактор-группа

Пусть G – произвольная группа; G_1 – нормальный делитель. Образуем множество смежных классов группы G по подгруппе G_1 вида gG_1, где $g \in G$. Введем операцию умножения на множестве смежных классов $(g'G_1) \bullet (g''G_1) = g'g''G_1$, где g', $g'' \in G$. Так как подгруппа G_1 является нормальным делителем группы G, то произведение $g'G_1g''G_1$ не зависит от выбора представителей g' и g'' в перемножаемых классах. Покажем, что множество смежных классов образует группу.

Ассоциативность умножения классов вытекает из ассоциативности умножения в группе G. Единичным элементом группы классов служит сама подгруппа G_1. Действительно: $G_1(gG_1) = (eG_1)(gG_1) = egG_1 = gG_1$; $(gG_1)G_1 = (gG_1)(eG_1) = geG_1 = gG_1$.

Обратным элементом к классу gG_1 будет класс $g^{-1}G_1$, так как $gG_1g^{-1}G_1 = gg^{-1}G_1 = eG_1 = G_1$, $g^{-1}G_1gG_1 = g^{-1}gG_1 = eG_1 = G_1$.

Полученная группа обозначается G/G_1 и называется *фактор-группой* (группой классов) группы G по нормальному делителю G_1.

Пример 1. На числовой оси выделим все целые числа, кратные, например, числу 3. Их количество бесконечно и счетно. Обозначим класс этих чисел через A_0. Образуем теперь два класса чисел вида $A_1 = a + A_0$ и $A_2 = b + A_0$, где $a = 1 \bmod 3$, $b = 2 \bmod 3$. Классы A_1 и A_2 не зависят от выбора конкретных представителей a и b и определяют все целые числа, сравнимые соответственно с 1 и 2 по модулю 3. Классы A_0, A_1 и A_2 образуют группу, что легко проверяется. Эта группа и есть фактор-группа группы целых чисел с операцией сложения по нормальному делителю – группе целых чисел, кратных 3.

Пример 2. Возьмем множество $N_7/0 = (1, 2, 3, 4, 5, 6)$ и операцию $\bullet \bmod 7$. Эта пара образует коммутативную группу G. Подмножество множества $N_7/0$, состоящее из 2-х элементов (1, 6), также образует группу с этой операцией, т. е. является подгруппой G_1 исходной группы G.

Покажем, что пара (1, 6; $\bullet \bmod 7$) является нормальным делителем в группе G. Выпишем для каждого элемента группы G соответствующие обратные элементы: $1^{-1} = 1$; $2^{-1} = 4$; $3^{-1} = 5$; $4^{-1} = 2$, $5^{-1} = 3$, $6^{-1} = 6$ и левые смежные классы: $2G = (2, 5)$; $3G = (3, 4)$; $4G = (4, 3)$; $5G = (5, 2)$. Условие $gGg^{-1} = G$ проверяется тривиально.

Таким образом, имеется три различных смежных класса, которые образуют фактор-группу с операцией умножения по модулю 7: (1, 6), (2, 5), (3, 4).

3.2.5. Прямое произведение нормальных делителей

Пусть G – некоторая группа, имеющая два взаимно простых нормальных делителя H и K. Две группы называются *взаимно простыми*, если не содержат общих элементов, кроме e.

Докажем несколько полезных свойств, которыми обладает такая модель.

Произведения из элементов групп H и K перестановочны. Действительно, рассмотрим выражение $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$. С одной стороны, $hkh^{-1} \in K$ и $(hkh^{-1})k \in K$, с другой стороны, $kh^{-1}k^{-1} \in H$ и $h(kh^{-1}k^{-1}) \in H$. Следовательно, $hkh^{-1}k^{-1} = e$, откуда $hk = kh$.

Совокупность произведений hk, где h пробегает всю группу H, а k – всю группу K, образует группу, так как, если $hh' = h''$ и $kk' = k''$, то

$(hk')(h'k) = hh'kk' = h''k''$ – замкнутость. Нейтральный элемент $ee = e$. Кроме того, $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1}$. Эта группа называется *прямым произведением групп* H и K и обозначается $H \times K$.

Отметим важное свойство такой группы. Всякий элемент прямого произведения разлагается в произведение множителей одним единственным образом. Действительно, если бы имело место $hk = h'k'$, то $hkk^{-1} = h'k'k^{-1} = h$, $k'k^{-1} = (h')^{-1}h$. Однако, поскольку эти группы взаимно просты, следовательно, $k'k^{-1} = e \to k' = k$ и $(h')^{-1}h = e \to h = h'$.

3.2.6. Группы Ли на плоскости

В работах Ли эти группы названы непрерывными.

Пусть задано n-мерное пространство; $(x_1, x_2, x_3,\ldots, x_n)$ – координаты некоторой точки в этом пространстве. Пусть в пространстве действует преобразование f, которое меняет положение точек по некоторому правилу:

$$x_1 \to f_1(x_1, x_2, x_3,\ldots, x_n, a_1, a_2,\ldots, a_r);$$

$$x_2 \to f_2(x_1, x_2, x_3,\ldots, x_n, a_1, a_2,\ldots, a_r);$$

$$\ldots$$

$$x_n \to f_n(x_1, x_2, x_3,\ldots, x_n, a_1, a_2,\ldots, a_r),$$

где $f_1, f_2,\ldots, f_n$ – непрерывные функции, аналитические или дифференцируемые столько раз, сколько это требуется. Переменные $a_1, a_2,\ldots, a_r$ называются параметрами преобразования. Придавая этим параметрам различные значения, получим разные элементы группы преобразований n-мерного пространства. Непрерывность группы определяется непрерывностью изменения ее параметров. При цифровой обработке как само пространство, так и параметры группы меняются дискретно.

Рассмотрим двумерное пространство (плоскость). Группы Ли на плоскости делятся на два класса: примитивные и импримитивные.

Примитивные группы.

а. *Проективная группа* задается системой уравнений

$$\begin{cases} x' = \dfrac{a_1x + a_2y + a_3}{a_4x + a_5y + 1}; \\ y' = \dfrac{a_6x + a_7y + a_8}{a_4x + a_5y + 1}. \end{cases}$$

Проективная группа часто называется дробно-линейной. При таком преобразовании непрерывная линия на плоскости остается непрерывной, прямая переходит в прямую, однако параллельность линий не сохраняется.

b. *Аффинная группа* задается системой уравнений

$$\begin{cases} x' = a_1 x + a_2 y + a_3; \\ y' = a_4 x + a_5 y + a_6. \end{cases}$$

При преобразовании аффинной группой сохраняется параллельность прямых.

c. *Аффинная унимодулярная группа*.

Эта группа описывается уравнениями аффинной группы, однако параметры связаны условием $a_1 a_5 - a_2 a_4 = 1$.

При преобразованиях аффинной унимодулярной группой сохраняется площадь фигуры.

Импримитивные группы.

Число таких групп на плоскости равно 14. Основной особенностью импримитивных групп является то, что одна координата меняется по линейному закону, а вторая – по нелинейному, например:

$$\begin{cases} x' = a_1 x + a_2; \\ y' = a_3 x + a_4 x^2 + a_5 y. \end{cases}$$

Кроме перечисленных основных групп G на плоскости могут действовать также группы, сопряженные с перечисленными, т. е. группы вида sGs^{-1}, где s – некоторое непрерывное невырожденное (имеющее обратное) преобразование.

Группы Ли являются очень эффективным математическим аппаратом при решении различных задач распознавания объектов по их изображениям, полученным с помощью различных датчиков: TV-камер, радиолокационных и ультразвуковых систем, лазерных дальномерных систем, спектранов, лидаров и т. п. Рассмотрим некоторые свойства аффинных преобразований на плоскости.

Пусть задано центрированное точечное изображение, состоящее из k точек. Тогда $\sum_{i=1}^{k} x_i = 0;\ \sum_{i=1}^{k} y_i = 0$. Кроме того, пусть на плоскости действует аффинная группа преобразований

$$\begin{cases} x' = a_1 x + a_2 y + a_3; \\ y' = a_4 x + a_5 y + a_6. \end{cases}$$

Вычислим центр формы изображения после преобразования некоторым элементом аффинной группы:

$$x'_c = \frac{\sum_{i=1}^{k} x'_i}{k} = \frac{\sum_{i=1}^{k} \left(a_1 x_i + a_2 y_i + a_3\right)}{k} = a_3;$$

$$y'_c = \frac{\sum_{i=1}^{k} y'_i}{k} = \frac{\sum_{i=1}^{k} \left(a_4 x_i + a_5 y_i + a_6\right)}{k} = a_6.$$

Таким образом, параметры a_3 и a_6 определяют сдвиг центра формы изображения, если оно было предварительно центрировано. На этом основана процедура упрощения искажения изображения, состоящая в том, что все эталоны предварительно центрируются, на искаженном изображении находятся координаты центра формы и в него переносится начало координат. Тем самым исключается действие параметров сдвига, и оставшаяся группа имеет вид

$$\begin{cases} x' = a_1 x + a_2 y; \\ y' = a_4 x + a_5 y. \end{cases}$$

Эта группа является подгруппой аффинной группы и называется аффинной группой без сдвига.

3.2.7. Матричная запись групповых преобразований

Аффинное преобразование без сдвига удобно представить в матричной форме

$$\begin{pmatrix} a_1 & a_2 \\ a_4 & a_5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' = a_1 x + a_2 y \\ y' = a_4 x + a_5 y \end{pmatrix}.$$

При таком представлении легко находится результат последовательного преобразования различными элементами в виде произведения соответствующих матриц. Определитель матрицы

$$\left| \begin{pmatrix} a_1 & a_2 \\ a_4 & a_5 \end{pmatrix} \right| = a_1 a_5 - a_2 a_4$$

равен коэффициенту изменения площади фигуры при таком преобразовании.

Легко находятся подгруппы такой группы, например:

a) $\begin{pmatrix} \cos(l) & -\sin(l) \\ \sin(l) & \cos(l) \end{pmatrix}$ – подгруппа вращений против часовой стрелки на угол l;

b) $\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$ – подгруппа равномерных по осям масштабных преобразований;

с) $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ – подгруппа симметричных отражений плоскости вокруг оси Y.

Полная аффинная группа также может быть представлена в матричном виде:

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} x' = a_1x + a_2y + a_3 \\ y' = a_4x + a_5y + a_6 \\ 1 \end{pmatrix}.$$

Для записи в матричном виде проективного преобразования используется однородная система координат:

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ a_6 & a_7 & a_8 \\ a_4 & a_5 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} x' = a_1x + a_2y + a_3 \\ y' = a_6x + a_7y + a_8 \\ a_4x + a_5y + 1 \end{pmatrix}.$$

Результат преобразования записан также в однородной системе координат. Для перевода в обычную систему необходимо первую и вторую строки результирующей матрицы разделить на третью строку.

Матричное представление преобразований позволяет легко определить, является ли некоторая подгруппа G_1 нормальным делителем в группе G. Для примера возьмем

$$G_1 := \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix},\ G := \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}.$$

Поскольку

$$\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix},$$

то группа равномерного масштабного преобразования является нормальным делителем в аффинной группе без сдвига.

3.2.8. Гомоморфизм групп. Линейные представления групп

Будем говорить, что группа G' *гомоморфна* группе G или что имеется гомоморфное отображение f группы G на группу G', если каждому элементу g группы G поставлен в соответствие определенный элемент $f(g)$ группы G' (причем каждый элемент группы G поставлен в соответствие хотя бы одному элементу группы G') так, что для всех элементов $g_1, g_2 \in G$ выполняется $f(g_1g_2) = f(g_1)f(g_2)$. Таким образом гомоморфизм «сохраняет групповую операцию».

Частным случаем гомоморфизма является *изоморфизм* групп, который обеспечивает взаимно однозначное соответствие элементов групп

G и G', сохраняя также групповую операцию. С точки зрения теории групп, все изоморфные группы считаются неразличимыми, так как все имеют одинаковые свойства и для исследования можно брать любого представителя из множества изоморфных групп.

Пример 1. Циклическая группа G_6 шестого порядка с элементами $(e, a^1, a^2, a^3, a^4, a^5)$ гомоморфна циклической группе G_2 второго порядка с элементами (E, A). Гомоморфизм f можно задать следующим образом: $f(e) = f(a^2) = f(a^4) = E$; $f(a) = f(a^3) = f(a^5) = A$.

Пример 2. Циклическая группа C_5 пятого порядка с элементами (e, a^1, a^2, a^3, a^4) изоморфна группе дискретных вращений правильного пятиугольника. Изоморфизм можно задать следующим образом:

$f(e) = E$ – отсутствие вращения;

$f(a) = g$ – вращение на угол $2\pi/5$ против часовой стрелки;

$f(a^2) = g^2$ – вращение на угол $(2\pi/5) \cdot 2$;

$f(a^3) = g^3$ – вращение на угол $(2\pi/5) \cdot 3$;

$f(a^4) = g^4$ – вращение на угол $(2\pi/5) \cdot 4$.

Каждая группа изоморфна самой себе (можно положить $f(g) = g$ для всех элементов $g \in G$) и гомоморфна единичной группе (состоящей из одной единицы). В этом случае $f(g) = 1$ для всех $g \in G$.

Можно показать, что каждая группа гомоморфна любой своей фактор-группе. Более того, фактор-группы группы G – это все (с точностью до изоморфизма) группы, которым гомоморфна данная группа G.

Гомоморфная группа G' «устроена» так же, как и фактор-группа группы G, и «проще», чем сама группа G. В связи с этим говорят, что гомоморфная группа представляет исходную группу неточно, а изоморфная – точно. Известна теорема Кели, в силу которой каждая группа конечного порядка может быть точно представлена некоторой группой подстановок.

Пример. Группа вращений правильного n-угольника может быть точно представлена группой подстановок. Положим $n = 5$ и перенумеруем вершины цифрами 1, 2, 3, 4, 5 по часовой стрелке. Тогда:

$$f(e) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}, \quad f(g) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}, \quad f(g^2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix},$$

$$f(g^3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, \quad f(g^4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}.$$

Однако в практических приложениях чаще всего используются представления групп не в форме групп подстановок, а так называемые *линейные представления*.

Пусть дано некоторое (комплекснозначное) n-мерное векторное пространство R, в котором действуют невырожденные (имеющие обрат-

ные) линейные операторы. Эти операторы образуют группу G', которая может быть гомоморфной исходной группе G.

Если в пространстве R выбрать базис, то каждому линейному оператору будет соответствовать квадратная невырожденная матрица порядка n. Если обозначить $T(g)$ матричное представление элемента $g \in G$, то $T(g_1 g_2) = T(G_1)T(G_2)$, $g_1, g_2 \in G$.

Если пространство R одномерно, то $T(g)$ – комплексное число. Нейтральному элементу группы соответствует число 1. Заметим, что если T – одномерное представление группы G и элементы g_1 и g_2 сопряжены в G, т. е. $g_2 = g^{-1}g_1 g$, где $g_1, g_2 \in G$, то $T(g_2) = T(g^{-1}g_1 g) = T(g^{-1})T(g_1)T(g) = [T(g)]^{-1}T(g_1)T(g) = T(g_1)$.

Если группа матричных преобразований G' в пространстве R гомоморфна группе G, то говорят, что G' является линейным представлением G.

3.2.9. Представление группы вращений правильного n-угольника

Рассмотрим правильный n-угольник. Пусть число его вершин n для определенности равно 5. Нас будут интересовать только такие вращения многоугольника вокруг центра O, которые обеспечивают самосовмещение всех вершин. Для $n = 5$ это будут вращения на углы $\alpha = 0$, $2\pi/5$, $2(2\pi/5)$, $3(2\pi/5)$, $4(2\pi/5)$. В общем случае при произвольном n эти вращения будут определяться углами $a = l(2\pi/n)$, где $l = 0, 1, 2, 3, \ldots, n-1$. Матрица вращения плоскости вокруг центра O на угол α может быть задана в виде

$$\mathbf{g} = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}.$$

Таким образом, мы можем найти линейные представления группы вращений правильного многоугольника в виде набора линейных операторов (матриц поворота плоскости). Однако ранее было показано, что группа вращений правильного n-угольника изоморфна циклической группе порядка n, т. е. группе вида $(e, g, g^2, g^3, \ldots, g^{n-1})$, где g эквивалентен повороту на угол $2\pi/n$.

Известно, что линейные представления циклической группы (и всякой коммутативной группы) одномерны. Тогда линейные представления группы вращений правильного многоугольника можно найти из следующих соотношений: $T(e) = 1$; $T(g) = \gamma$, где γ – некоторое комплексное число. Тогда $T(g^n) = (T(g))^n = \gamma^n$, но, так как $g = e$, то $T(g^n) = T^n(e) = 1$, поэтому $\gamma^n = 1$, откуда $\gamma = \exp[j(2\pi/n)\alpha]$, где $\alpha = 0, 1, 2, \ldots, n-1$, $j = \sqrt{-1}$.

Придавая α различные значения, мы можем получить набор линейных представлений. Так, для $n = 5$ получим:

$T(\alpha)$	e	g	g^2	g^3	g^4
$T(0)$	1	1	1	1	1
$T(1)$	1	e_1	e_2	e_3	e_4
$T(2)$	1	e_2	e_4	e_1	e_3
$T(3)$	1	e_3	e_1	e_4	e_2
$T(4)$	1	e_4	e_3	e_2	e_1

где обозначено $e_s = \exp[j(2\pi/5)s]$.

Для $n = 4$ получаем следующую таблицу представлений:

$T(\alpha)$	e	g	g^2	g^3
$T(0)$	1	1	1	1
$T(1)$	1	j	-1	$-j$
$T(2)$	1	-1	1	-1
$T(3)$	1	$-j$	-1	j

Для $n = 2$ (вырожденный многоугольник – 2-угольник) получаем таблицу представлений:

$T(\alpha)$	e	g
$T(0)$	1	1
$T(1)$	1	-1

Среди представлений при $n = 5$ только одно $T(0)$ является неточным. Остальные представления точные (взаимно однозначные). При $n = 4$ неточными являются представления $T(0)$ и $T(2)$. Можно показать, что если n – простое число, то все представления, кроме $T(0)$, являются точными. При $n = 2$ мы получили матрицу, которая является базовой для построения *матриц Адамара* (матрицы получаются кронекеровскими степенями представления при $n = 2$). Количество точных представлений при любом значении n равно функции Эйлера $\Psi(n)$.

3.2.10. Представление диэдральной группы

Представим теперь многоугольник в виде объемной фигуры (его можно вырезать из картона). Рассмотрим пространственные вращения такого многоугольника, при которых производится самосовмещение всех его вершин. Легко видеть, что к вращениям многоугольника в плоскости e, g^1, g^2, g^3,..., g^{n-1} следует добавить повороты на 180° вокруг

оси, проходящей, например, через центр вращения и одну из вершин. Такой поворот обозначим через s, тогда множество различных элементов так называемой диэдральной группы преобразований будет $\{e, g^1, g^2, g^3,\ldots, g^{n-1}, s, sg, sg^2, sg^3,\ldots, sg^{n-1}\}$. Так, при $n = 5$ число различных элементов диэдральной группы преобразований равно 10. Таким образом, диэдральная группа преобразований порождается двумя «образующими» элементами g и s. Очевидными соотношениями между элементами группы являются следующие:

$$g^n = e;\ s^2 = e,\ sgs = g^{n-1}. \qquad (3.1)$$

Справедливость третьего соотношения легко проверить, представив диэдральную группу изоморфной группой подстановок. Так, для $n = 5$, обозначив вершины многоугольника цифрами 1, 2, 3, 4, 5, получим

$$e \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix},\ g \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix},\ s \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}.$$

Тогда

$$sgs \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \to g^{n-1}.$$

Из последнего соотношения можно получить $sg^2s = g^{n-2}$; $sg^3s = g^{n-3}$; …; $sg^{n-1}s = g$.

Построим линейные представления диэдральной группы.

1. Соотношениям (3.1) удовлетворяет следующий набор значений: $T_0(e) = 1$, $T_0(g) = 1$, $T_0(s) = 1$. Получили единичное, т. е. неточное представление.

2. $T_1(e) = 1$, $T_1(g) = 1$, $T_1(s) = -1$. Это представление также является неточным.

3. $T_2(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $T_2(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. $T_2(g) \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$. Это представление является изоморфным, т. е. точным.

3.2.11. Скалярное произведение функций, заданных на группе

В пространстве функций, заданных на группе G порядка n, определим скалярное произведение следующим образом:

$$(\varphi, \psi) = \frac{1}{n} \sum_{g \in G} \varphi_{(g)} \overline{\psi_{(g)}},$$

где $\overline{\Psi_{(g)}}$ – комплексно сопряженное значение функции $\Psi_{(g)}$. В этом выражении суммирование распространяется на все элементы группы G.

Пример. Пусть D_3 – группа диэдральных преобразований правильного треугольника с элементами e, r, r^2, s, sr, sr^2, где r – вращение на угол $2\pi/3$, s – симметричное отражение (поворот на 180° в пространстве) вокруг вертикальной оси. Одномерные представления такой группы приведены далее:

$T(g)$	e	r	r^2	s	sr	sr^2
T_0	1	1	1	1	1	1
T_1	1	1	1	−1	−1	−1

Двумерное представление может быть построено, если положить:

$$T_2(e)=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ T_2(r)=\begin{pmatrix}\cos(2\pi/3) & -\sin(2\pi/3)\\ \sin(2\pi/3) & \cos(2\pi/3)\end{pmatrix}=\begin{pmatrix}-\frac{1}{2} & -\frac{1}{2}\sqrt{3}\\ \frac{1}{2}\sqrt{3} & -\frac{1}{2}\end{pmatrix},$$

$$T_2(s)=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$

Тогда

$$T_2\left(r^2\right)=\begin{pmatrix}-\frac{1}{2} & \frac{1}{2}\sqrt{3}\\ -\frac{1}{2}\sqrt{3} & -\frac{1}{2}\end{pmatrix},\ T_2(sr)=\begin{pmatrix}-\frac{1}{2} & -\frac{1}{2}\sqrt{3}\\ -\frac{1}{2}\sqrt{3} & \frac{1}{2}\end{pmatrix},$$

$$T_2\left(sr^2\right)=\begin{pmatrix}-\frac{1}{2} & \frac{1}{2}\sqrt{3}\\ \frac{1}{2}\sqrt{3} & \frac{1}{2}\end{pmatrix}.$$

Рассмотрим шесть функций, определенных на элементах группы T_0, T_1 и g_{11}, g_{12}, g_{21}, g_{22}. Последние четыре функции представляют собой элементы матричного (точного) представления:

$$T_2(g)=\begin{pmatrix}\gamma_{11} & \gamma_{12}\\ \gamma_{21} & \gamma_{22}\end{pmatrix}.$$

Запишем все эти функции в виде таблицы:

$T(g)$	e	r	r^2	s	sr	sr^2
T_0	1	1	1	1	1	1
T_1	1	1	1	−1	−1	−1
γ_{11}	1	$-\frac{1}{2}$	$-\frac{1}{2}$	1	$-\frac{1}{2}$	$-\frac{1}{2}$
γ_{12}	0	$-\frac{1}{2}\sqrt{3}$	$\frac{1}{2}\sqrt{3}$	0	$-\frac{1}{2}\sqrt{3}$	$\frac{1}{2}\sqrt{3}$
γ_{21}	0	$\frac{1}{2}\sqrt{3}$	$-\frac{1}{2}\sqrt{3}$	0	$-\frac{1}{2}\sqrt{3}$	$\frac{1}{2}\sqrt{3}$
γ_{22}	1	$-\frac{1}{2}$	$-\frac{1}{2}$	−1	$\frac{1}{2}$	$\frac{1}{2}$

Вычислим попарные скалярные произведения этих функций: $(T_0, T_1) = \frac{1}{6}(1\cdot1 + 1\cdot1 + 1\cdot1 + 1\cdot(-1) + 1\cdot(-1) + 1\cdot(-1)) = 0$. Аналогично получаем: $(T_0, g_{11}) = 0$, $(T_0, g_{12}) = 0$, $(T_{0,} g_{21}) = 0$, $(T_0, g_{22}) = 0$. Далее $(g_{11}, g_{12}) = 0$, $(g_{11}, g_{21}) = 0$, $(g_{11,} g_{22}) = 0$, $(g_{12}, g_{21}) = 0$, $(g_{12}, g_{22}) = 0$, $(g_{21}, g_{22}) = 0$.

Таким образом, все функции, приведенные в таблице, попарно ортогональны. Скалярные квадраты этих функций $(T_0, T_0) = 1$, $(T_1, T_1) = 1$, $(g_{ij}, g_{ij}) = \frac{1}{2}$. Следовательно, функции, заданные на элементах группы в виде матричных элементов линейных представлений, могут служить *ортогональным базисом*.

3.2.12. Задачи для контрольной

1. U – плоскость; G – группа смещений плоскости вдоль оси X. На какие классы транзитивности группа G разбивает плоскость?

2. U – плоскость; G – группа смещений плоскости вдоль оси Y. На какие классы транзитивности группа G разбивает плоскость?

3. U – плоскость; G – группа масштабных преобразований плоскости с центром в O, т. е. в зависимости от коэффициента масштаба точки плоскости удаляются или приближаются к O. На какие классы транзитивности группа масштабных преобразований разбивает плоскость?

4. U – трехмерное евклидово пространство; G – группа масштабных преобразований этого пространства с центром в O. На какие классы транзитивности разбивает трехмерное пространство группа масштабных преобразований?

5. U – трехмерное евклидово пространство; G – группа движений пространства параллельных некоторой плоскости P. На какие классы транзитивности разбивает эта группа трехмерное пространство?

6. U – плоскость; G – группа смещений плоскости вдоль линии L, проходящей на плоскости, и симметричных отражений плоскости вокруг этой линии. На какие классы транзитивности разбивает плоскость эта группа?

7. Пусть на бесконечной плоскости U действует группа вращений плоскости G вокруг неподвижного центра O. Является ли группа G транзитивной на плоскости? На какие классы транзитивности распадается плоскость при действии на ней группы G?

8. Пусть G – группа невырожденных матриц с действительными коэффициентами размера 2×2 с операцией умножения матриц, а G_1 – группа матриц масштабных преобразований вида $\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$, где k не равно 0. Является ли G_1 подгруппой группы G?

9. Пусть на плоскости U действует группа G – вращений плоскости вокруг неподвижного центра O. Какой вид имеет сфера, проходящая через точку Y, если Y не совпадает с точкой O?

10. Рассмотрим множество перестановок четырех элементов a, b, c, d. Число таких перестановок равно $4! = 24$. Выпишем некоторые из них:

$$h_0 = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix},\ h_1 = \begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix},\ h_2 \begin{pmatrix} a & b & c & d \\ d & c & a & b \end{pmatrix}.$$

Определите порядок циклической группы, порождаемой элементами h_0, h_1 и h_2.

Покажем, как это сделать, на примере элемента h_1:

$$h_1^2 = \begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix}\begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix},$$

$$h_1^3 = \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}\begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix},$$

$$h_1^4 = \begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix},\begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix} = h_0.$$

Таким образом, совокупность перестановок h_0, h_1, ${h_1}^2$, ${h_1}^3$ образует циклическую коммутативную группу. Проверьте коммутативность и покажите, что вместе с любым элементом это множество содержит и обратный к нему элемент.

11. Используя методику решения предыдущего примера, определите порядок циклических групп, порождаемых степенями некоторых перестановок пяти элементов:

$$h_0 = \begin{pmatrix} a & b & c & d & e \\ a & b & c & d & e \end{pmatrix},\ h_1 = \begin{pmatrix} a & b & c & d & e \\ c & d & e & a & b \end{pmatrix},\ h_2 = \begin{pmatrix} a & b & c & d & e \\ e & c & a & d & b \end{pmatrix},$$

$$h_3 = \begin{pmatrix} a & b & c & d & e \\ b & a & e & c & d \end{pmatrix},\ h_4 = \begin{pmatrix} a & b & c & d & e \\ d & e & c & b & a \end{pmatrix}.$$

12. В чем состоит отличие групп преобразований от числовых групп? Дайте краткий ответ.

13. Является ли группа всевозможных перестановок n элементов группой преобразований? Дайте краткий письменный ответ.

14. Образует ли совокупность степеней некоторого элемента некоммутативной группы коммутативную группу? Дайте краткий письменный ответ.

15. Пусть на бесконечной плоскости U действует группа вращений плоскости G вокруг неподвижного центра O. Является ли группа G транзитивной группой на U? На какие классы транзитивности распадается плоскость при действии на ней группы G?

16. Пусть на бесконечной плоскости U действует группа масштабных преобразований G с центром масштаба в точке O. Является ли группа G транзитивной на U? На какие классы транзитивности распадается U при действии группы G?

17. Пусть G – группа невырожденных матриц размера 2×2 с действительными коэффициентами, а G_1 – группа матриц вида $\begin{pmatrix} k_1 & 0 \\ 0 & k_2 \end{pmatrix}$, где k_1 может быть не равен k_2. Является ли G_1 нормальным делителем в G?

18. Является ли группа матриц G_1 с элементами вида $\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}$ нормальным делителем в G?

19. На числовой оси отметим все целые (положительные и отрицательные) числа, кратные 3, и обозначим множество этих чисел через A_0. Тогда множество всех чисел, которые при делении на 3 дают в остатке 1, можно получить следующим образом: $a + A_0$, где a – любое целое, сравнимое с 1 по модулю 3. Обозначим это множество A_1. Тогда $A_2 = b + A_0$, где b – любое целое, сравнимое с 2 по модулю 3, есть множество всех чисел, сравнимых с 2 по модулю 3. Совокупность трех множеств A_0, A_1 и A_2 образует группу, у которой каждый элемент есть бесконечное множество чисел. Эта группа называется *фактор-группой* группы G целых чисел с операцией сложения по модулю 3 по нормаль-

ному делителю H – группы чисел, кратных 3 по сложению. Постройте фактор-группу, в которой H – группа чисел, кратных 5. Обобщите на произвольный модуль m.

20. Пусть некоторая многоугольная фигура задана набором координат угловых точек:

N точки	1	2	3	4	5
x	1	1	−1	−1	0
y	1	−1	−1	1	3

Найдите координаты точек этой фигуры после аффинного преобразования элементом вида $\begin{cases} x' = 2x - y + 3; \\ y' = -x + 3y - 2 \end{cases}$ и вычислите площадь фигуры до и после преобразования.

21. Пусть некоторая многоугольная фигура задана набором координат угловых точек:

N точки	1	2	3	4	5
x	2	0	−2	−2	2
y	3	1	3	−2	−2

Найдите координаты точек этой фигуры после аффинного преобразования элементом вида $\begin{cases} x' = 2x - 3y; \\ y' = -x - y - 2 \end{cases}$ и вычислить площадь фигуры до и после преобразования.

22. Пусть некоторая многоугольная фигура задана набором координат угловых точек:

N точки	1	2	3	4	5
x	1	2	−2	−1	−2
y	0	2	2	0	−2

Найдите координаты точек этой фигуры после аффинного преобразования элементом вида $\begin{cases} x' = 2x - y + 3; \\ y' = -x + 3y - 2 \end{cases}$ и вычислите площадь фигуры до и после преобразования.

23. Пусть некоторая многоугольная фигура задана набором координат угловых точек:

N точки	1	2	3	4	5
x	1	1	−1	−1	0
y	1	−1	−1	1	3

Найдите координаты точек этой фигуры после аффинного преобразования элементом вида $\begin{cases} x' = -x - 3y - 2; \\ y' = -x - y + 3 \end{cases}$ и вычислите площадь фигуры до и после преобразования.

Приложение. Вычисление площади произвольного n-угольника.

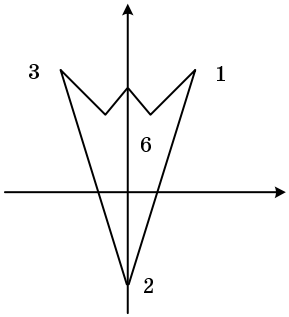
Пусть многоугольник задан списком координат вершин: (x_1, y_1), (x_2, y_2), ..., (x_n, y_n), где n – число вершин многоугольника. Тогда его площадь

$$S = \begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \end{pmatrix} \begin{pmatrix} y_n - y_2 \\ y_1 - y_3 \\ y_2 - y_4 \\ \dots \\ y_{n-1} - y_1 \end{pmatrix}.$$

Пусть, например, многоугольник задан следующими координатами вершин:

x	3	0	−3	−1	0	1
y	5	−5	5	2	4	2

Его изображение на плоскости до преобразования аффинной группой имеет вид



Возьмем некоторое аффинное преобразование

$$x' = -3x - 2y - 1;$$
$$y' = 2x + 2y + 2.$$

Найдем координаты фигуры после преобразования с помощью матричного умножения:

$$\begin{pmatrix} -3 & -2 & -1 \\ 2 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 3 & 0 & -3 & -1 & 0 & 1 \\ 5 & -5 & 5 & 2 & 4 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}=\begin{pmatrix} -20 & 9 & -2 & -2 & -9 & -8 \\ 18 & -8 & 6 & 4 & 10 & 8 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Площадь фигуры до преобразования будет равна

$$S_0=\frac{1}{2}\begin{pmatrix} 3 & 0 & -3 & -1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 7 \\ 0 \\ -7 \\ 1 \\ 0 \\ -1 \end{pmatrix}=\frac{1}{2}(21+21-1-1)=20.$$

Площадь фигуры после преобразования будет равна

$$S_0=\frac{1}{2}\begin{pmatrix} -20 & 9 & -2 & -2 & -9 & -8 \end{pmatrix}\begin{pmatrix} 16 \\ 12 \\ -12 \\ -4 \\ -4 \\ -8 \end{pmatrix}=$$

$$=\frac{1}{2}(-320+108+24+8+36+64)=-40.$$

Коэффициент изменения площади фигуры при аффинном преобразовании равен определителю матрицы: $\begin{pmatrix} a_1 a_2 \\ a_3 a_4 \end{pmatrix}$. Для выбранного преобразования $a_1=-3$, $a_2=-2$, $a_3=2$, $a_4=2$. Следовательно, определитель равен -2. Площадь фигуры увеличится в 2 раза, при этом фигура перевернется на противоположную сторону (об этом свидетельствует знак «$-$«). Если вершины многоугольника были обозначены возрастающими числами по часовой стрелке, то после такого преобразования порядок вершин будет идти против часовой стрелки.

24. Постройте линейные представления группы вращений правильного 6-угольника. Убедитесь, что векторы-строки представлений попарно ортогональны.

25. Постройте линейные представления группы вращений правильного 8-угольника. Убедитесь, что векторы-строки представлений попарно ортогональны.

26. Постройте линейные представления диэдральной группы преобразований правильного 5-угольника.

27. Для матриц линейных представлений диэдральной группы преобразований правильного 5-угольника убедитесь в том, что строки этих матриц попарно ортогональны.

Приведем пример ответа на вопросы подразд. 3.2.

Является ли группа матриц G_1 с элементами вида $\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}$ нормальным делителем в G?

Ответ: Если исключить случай $k = 0$, то проверка факта, является ли подгруппа G_1 нормальным делителем в G, сведется к проверке коммутативности умножения матриц: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, где a, b, c, d, k принадлежат полю действительных чисел. Легко убедиться, что в общем случае это равенство не выполняется. Следовательно, G_1 не является нормальным делителем в G.

Литература

1. *Головина*, *Л. И.* Линейная алгебра и некоторые ее приложения / Л. И. Головина. М.: Наука, 1975.

2. *Ерош*, *И. Л.* Адаптивные робототехнические системы: учеб. пособие для вузов / И. Л. Ерош, М. Б. Игнатьев, Э. С. Москалев; ЛИАП. Л., 1985. 144 с.

3. *Ерош И. Л.* Элементы теории дискретных групп: учеб. пособие / И. Л. Ерош. СПбГУАП. СПб., 1998. 36 с.

4. ЭЛЕМЕНТЫ КОМБИНАТОРИКИ

Комбинаторика является разделом дискретной математики, ориентированным на решение задач выбора и расположения элементов некоторого множества в соответствии с заданными правилами и ограничениями. Каждое такое правило определяет способ построения некоторой комбинаторной конфигурации, поэтому комбинаторный анализ (комбинаторика) занимается изучением свойств комбинаторных конфигураций, условиями их существования, алгоритмами построения и оптимизацией этих алгоритмов.

Этот раздел математики тесно связан с рядом других разделов дискретной математики: теорией вероятностей, теорией графов, теорией чисел, теорией групп и т. д.

Первые подразделы посвящены элементам классической комбинаторики: размещениям, перестановкам, сочетаниям. Далее рассматриваются некоторые классы наиболее часто встречающихся задач: комбинаторные задачи с ограничениями, комбинаторные задачи раскладок и разбиений; комбинаторные задачи, решаемые с помощью рекуррентных соотношений.

Порядок изложения материала и многие примеры заимствованы из книг известного российского математика и прекрасного популяризатора математических идей Н. Я. Виленкина.

4.1. Основные понятия и теоремы комбинаторики

Рассмотрим сначала основные понятия комбинаторики: размещения, перестановки и сочетания, главная теорема,– что часто называют классическим разделом комбинаторики. Затем рассмотрим несколько классов комбинаторных задач.

4.1.1. Размещения с повторениями

Рассмотрим следующую задачу: сколько различных пятиразрядных чисел можно составить с помощью 10 цифр?

Пронумеруем разряды:

1	2	3	4	5

В первый разряд можно поставить одну из 10 цифр. Независимо от того, какая цифра поставлена, во второй разряд можно также поставить одну из 10 цифр и т. д. Всего получается 10^5 различных чисел.

Для двоичной системы счисления (в которой используются только две цифры: 0 или 1) получаем 2^5 различных чисел. Для системы с основанием k и числом разрядов n соответственно получаем

$$\overline{A} = k^n. \tag{4.1}$$

Формула (4.1) определяет количество конфигураций $\overline{A}$ – размещений с повторениями.

В общем виде задача размещений с повторениями ставится следующим образом. Имеется k типов предметов (количество предметов каждого типа неограничено) и n позиций (ящиков, сумок, кучек, разрядов). Требуется определить, сколько разных комбинаций можно составить, если в позициях предметы могут повторяться? Ответ дается формулой (4.1).

Сколько разных десятиразрядных чисел можно записать в троичной системе счисления? Получаем 3^{10}.

Упражнения.

1. Кодовый замок имеет 5 одинаковых ячеек, каждая ячейка может быть установлена в одно из 6 устойчивых положений. Какое максимальное число комбинаций нужно перебрать, чтобы открыть кодовый замок?

2. Пятеро студентов сдают экзамен. Каким количеством способов могут быть поставлены им оценки, если известно, что никто из студентов не получил неудовлетворительной оценки?

3. Частично определенная булева функция в таблице истинности (диаграмме Вейча) кроме 1 и 0 содержит 30 прочерков. На месте каждого прочерка при доопределении может быть поставлена либо 1, либо 0. Сколько существует разных способов доопределения этой булевой функции? Оцените число способов доопределения в десятичной системе, используя очевидное неравенство: $2^{10} > 10^3$.

В некоторых случаях кроме числа позиций дополнительно указывается ограничение на количество предметов, которые могут быть помещены на каждую позицию. Пусть, например, имеется n позиций и на каждую i-ю можно поставить n_i предметов. Сколько существует разных расстановок предметов по позициям?

Легко обосновывается формула

$$\overline{A} = k_1 k_2 k_3 \ldots k_n = \prod_{i=1}^{n} k_i. \tag{4.2}$$

Пример. В эстафете 100 + 200 + 400 + 800 метров на первую позицию тренер может поставить одного из 3-х бегунов, на вторую – одного из 5,

на третью – одного из 6, на четвертую – единственного бегуна (на каждую позицию выставляются разные бегуны). Сколько вариантов расстановки участников эстафетного забега может составить тренер?

В соответствии с формулой (4.2) получаем: $3 \cdot 5 \cdot 6 \cdot 1 = 90$.

Упражнения.

1. Сколько существует автомобильных номеров, содержащих 3 буквы и 5 цифр, если используется 20 букв русского алфавита и все 10 цифр?

2. Сколько существует 7-разрядных чисел, в первых трех разрядах которых нет цифр 0, 8, 9?

3. Время работы агрегата в течение суток задается часами, минутами и секундами. Сколько разных временных интервалов может быть задано для работы агрегата?

4.1.2. Размещения без повторений

Рассмотрим задачу: сколько разных 5-разрядных чисел можно записать с использованием всех 10 цифр при условии, что в числах не используются одинаковые цифры?

Перенумеруем разряды:

1	2	3	4	5

В первый разряд можно поставить одну из 10 цифр. Независимо от того, какая цифра помещена в первый разряд, во второй разряд можно поставить одну из 9 цифр, в третий – одну из 8 цифр и т. д. Всего существует $10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 = 30\,240$ различных 5-разрядных чисел, в каждом из которых нет двух одинаковых цифр.

В общем случае, если имеется k позиций и n разных предметов, причем каждый представлен в единственном экземпляре, то количество разных расстановок равно

$$A_n^k = n(n-1)(n-2)\ldots(n-k+1) = \frac{n!}{(n-k)!}. \qquad (4.3)$$

В формуле (4.3) $n!$ означает факториал числа n, т. е. произведение всех чисел от 1 до n.

Пример. Из группы в 25 человек требуется выбрать старосту, заместителя старосты и профорга. Сколько существует вариантов выбора руководящего состава группы?

Старосту можно выбрать 25 способами. Поскольку староста не может быть своим заместителем, то выбор заместителя выполняется 24 способами. Выбор профорга – 23 способами. Всего получается $25 \cdot 24 \cdot 23 = 25!/22! = 13\,800$.

Упражнения.

1. Из коллектива работников кооператива в 20 человек нужно выбрать председателя, заместителя председателя, бухгалтера и казначея. Каким количеством способов это можно сделать?

2. В парламент нового независимого государства нужно представить для рассмотрения варианты флагов (для определенности – три горизонтальные полосы). Сколько вариантов флагов можно представить, если каждый флаг должен содержать три разных цвета, а количество цветов имеющегося материала равно 12?

3. На дискотеку пришли 12 девушек и 15 юношей. Объявлен «белый» танец. Все девушки выбрали для танцев юношей (и никто из них не отказался). Сколько могло образоваться разных танцующих пар?

4.1.3. Перестановки без повторений

В рассмотренных ранее случаях комбинации отличались как составом предметов, так и их расположением. Однако, если бы в последней задаче юношей было 12, то все комбинации отличались бы только порядком. Рассмотрим, сколько разных расстановок можно получить, переставляя n предметов. В (4.3) положим $n = k$, тогда:

$$A_n^n = P_n = n!. \qquad (4.4)$$

Пример. К кассе кинотеатра подошли 6 человек. Сколько существует вариантов установки их в очередь друг за другом? Расставим 6 человек произвольным образом и начнем их переставлять всеми возможными способами. Получим $P_6 = 6! = 720$.

Упражнения.

1. Сколько различных слов (пусть и не имеющих смысла) можно получить, переставляя буквы слова ДУБЛЕНКА?

2. В заезде на ипподроме участвуют 12 рысаков. Играющие в тотализатор заполняют карточки, в которых указывают порядок, в котором, по их мнению, рысаки придут к финишу. Будем считать, что к финишу одновременно не могут прийти два и более рысака. Сколько вариантов заполнения карточек существует?

3. На заседании Думы 14 депутатов записались на выступления. Сколько вариантов списков выступающих может быть составлено, если списки отличаются только порядком?

4. Подсчитайте количество расстановок в списках выступающих для предыдущего примера, если известно, что некоторые депутаты, например Ж, З и Я, пользуясь своим влиянием в секретариате, уже обеспечили себе места в списках, соответственно 3, 6 и 7.

4.1.4. Перестановки с повторениями

Иногда требуется переставлять предметы, некоторые из которых неотличимы друг от друга. Такой вариант перестановок называется перестановками с повторениями.

Пусть имеется n_1 предметов 1-го типа, n_2 предметов 2-го типа, n_k предметов k-го типа и при этом $n_1 + n_2 + ... + n_k = n$.

Количество различных перестановок предметов определится формулой

$$P(n_1, n_2, n_3, \dots, n_k) = \frac{n!}{(n_1! n_2! \dots n_k!)}. \qquad (4.5)$$

Для обоснования (4.5) сначала будем переставлять все n предметов в предположении, что они все различные. Число таких перестановок равно $n!$. Затем заметим, что в любой выбранной расстановке перестановка n_1 одинаковых предметов не меняет комбинации, аналогично перестановка n_2 одинаковых предметов также не меняет комбинации и т. д. Поэтому получаем формулу (4.5).

Пример. Найдем количество разных перестановок букв слова КОМБИНАТОРИКА.

Это слово содержит 2 буквы К, 2 буквы О, 1 букву М, 1 букву Б, 2 буквы И, 1 букву Н, 2 буквы А, 1 букву Т и 1 букву Р.

Таким образом, число разных слов, получаемых перестановкой букв слова КОМБИНАТОРИКА, равно $P(2, 2, 1, 1, 2, 1, 2, 1, 1) = 13!/(2!\ 2!\ 2!\ 2!) = 13!/16$.

Упражнения.

1. У школьника 2 авторучки, 4 карандаша и 1 резинка. Он раскладывает эти предметы на парте в ряд. Сколько вариантов раскладки?

2. Рыбаки поймали 5 подлещиков, 4 красноперки и 2 уклейки, посолили и вывесили на солнце сушиться. Сколько вариантов развешивания рыбы на нитке?

3. На узком участке трассы в линию движутся гонщики. Из них 5 – на российских автомобилях, 6 – на американских и 3 – на итальянских. Сколько существует разных комбинаций машин на трассе, если нас интересует только принадлежность автомобиля конкретной стране?

4. Выходной алфавит абстрактного автомата содержит 4 буквы: y_0, y_1, y_2 и y_3. Сколько разных выходных слов может выработать автомат при условии, что в выходном слове 2 раза встречается буква y_0, 4 раза буква y_1, 3 раза буква y_2 и 1 раз буква y_3?

4.1.5. Основные правила комбинаторики

При вычислении количества различных комбинаций используются правила сложения и умножения. Сложение двух множеств комбинаций используется тогда, когда множества не совместны. Умножение – когда для каждой комбинации первого множества существуют все комбинации (или одинаковое число комбинаций) второго множества.

Пример. Из 28 костей домино берутся 2 кости. В каком числе комбинаций вторая кость окажется приложимой к первой?

На первом шаге имеется две возможности: выбрать дубль (7 вариантов) или не дубль (21 вариант). В первом случае независимо от того, какой конкретно дубль будет выбран, имеется 6 вариантов продолжения, во втором 12.

Общее число благоприятных комбинаций: $7 \cdot 6 + 21 \cdot 12 = 294$.

Упражнения.

1. Пароль состоит из 2-х букв, за которыми следуют 4 цифры, или из 4-х букв, за которыми следуют 2 цифры. Сколько можно составить разных паролей, если из 33-х букв русского алфавита используются только буквы: а, б, в, г, д, е, ж, и, к, л, м, н, п, р, с, т и все 10 цифр? А сколько можно получить разных паролей, если из множества букв исключить дополнительно буквы а, е и с, а к десяти цифрам добавить символ *?

2. У перевозчика через реку в лодке имеется 6 мест для пассажиров. Подходит веселая компания из 7 мужчин и 4-х женщин и просит перевезти хотя бы часть людей на другой берег. Перевозчик ставит условие, чтобы в лодку село не менее 2-х женщин (женщины выполняют функцию стабилизатора в веселой компании). Сколько вариантов у перевозчика посадить в лодку часть компании так, чтобы в лодке было не менее 2-х женщин?

4.1.6. Главная теорема комбинаторики (теорема о включениях и исключениях)

Рассмотрим *пример*. На предприятии работают 67 человек. Из них 48 знают английский язык, 35 – немецкий и 27 – оба языка. Сколько человек не знают ни английского, ни немецкого?

Построим диаграмму, аналогичную приведенной на рис. 1.1, на которой изобразим прямоугольник, соответствующий общему числу работающих U, и две пересекающиеся области А и Н по 48 и 35 человек. Пересечение областей $\text{А} \cap \text{Н} = 27$. Требуется найти число человек, не вошедших в области А и Н. Тогда решением будет $|U \setminus (\text{А} \cap \text{Н})| = 67 - 48 - 35 + 27 = 11$.

Теорема.

Пусть имеется множество из N объектов произвольной природы и пусть задано n произвольных свойств так, что объекты могут обладать или не обладать некоторыми из этих свойств. Сами свойства обозначим α_1, α_2, ..., α_n. Кроме того, будем обозначать $N(\alpha_i)$ – количество объектов, точно обладающих свойством α_i и, может быть, какими-то другими, а $N(\bar{\alpha}_i, \bar{\alpha}_j)$ – число объектов, не обладающих ни свойством α_i, ни свойством a_j. Тогда число объектов, не обладающих ни одним из перечисленных свойств, будет равно

$$N(\bar{\alpha}_1, \bar{\alpha}_2, ..., \bar{\alpha}_n) = N - N(\alpha_1) - N(\alpha_2) - ... N(\alpha_n) +$$
$$+N(\alpha_1, \alpha_2) + N(\alpha_1, \alpha_3) + ... N(\alpha_1, \alpha_n) + N(\alpha_2, \alpha_3) + ... N(\alpha_{n-1}, \alpha_n) -$$
$$- N(\alpha_1, \alpha_2, \alpha_3) - ... N(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n). \qquad (4.6)$$

Продолжим рассмотрение примера. Дополнительное тестирование на предприятии показало, что 20 человек знают французский, 12 – английский и французский, 11 – немецкий и французский и 5 – все три языка.

Тогда в соответствии с теоремой количество человек, не знающих ни английского, ни немецкого, ни французского языков, равно $N = 67 - 48 - 35 - 20 + 27 + 12 + 11 - 5 = 9$.

Задача "Решето Эратосфена".

Выпишем все числа от 1 до N. Сколько чисел из них делятся на k нацело? Очевидно, что $[N/k]$, где $[x]$ обозначает целую часть числа x. Тогда легко подсчитать количество чисел, которые не делятся на конкретные числа $k_1, k_2, ..., k_s$.

Пример. Сколько чисел в диапазоне от 1 до 100 не делятся ни на 5, ни на 7?

Воспользуемся теоремой о включениях и исключениях. Под первым свойством числа будем понимать делимость на 5, под вторым – делимость на 7. Тогда количество чисел, которые не делятся ни на 5, ни на 7, будет равно: $100 - 20 - 14 + 2 = 68$.

Упражнение.

1. В механической мастерской работают 12 человек, из них 6 человек имеют дипломы слесаря, 4 – дипломы оператора станков с ЧПУ, 7 человек – дипломы фрезеровщика, 3 человека владеют двумя из перечисленных дипломов и 2 человека – всеми тремя. Начальство решило уволить работников, не имеющих дипломов хотя бы по одной из этих специальностей. Имеется ли такая возможность?

2. Найти количество чисел, не делящихся на 3, 5 и 7, в диапазоне от 200 до 500.

4.1.7. Сочетания без повторений

Если требуется выбрать k предметов из n и порядок выбора безразличен, то имеем

$$C_n^k = \frac{n!}{k!(n-k)!}. \qquad (4.7)$$

Формула (4.7) может быть получена следующим образом. Выберем по очереди k предметов из n. Число вариантов выбора будет определяться формулой (4.3). Однако порядок выбранных предметов нас не интересует, поэтому, разделив это выражение на $k!$, получим формулу (4.7).

Пример 1. Из группы в 25 человек нужно выбрать троих для работы в колхозе. Если выбирать их, присваивая номера, то получим 25·24·23 варианта. Но порядок выбора нам не важен, поэтому решение нужно разделить на $3! = 6$.

Пример 2. В середине 60-х годов в Советском Союзе появились две лотереи, которые по недоразумению были названы «Спортлото», а именно, лотерея выбора 5 из 36 и лотерея выбора 6 из 49. Рассмотрим одну из них, например 6/49. Играющий покупает билет, на котором имеется 49 клеточек. Каждая клеточка соответствует какому-либо виду спорта. Нужно выделить (зачеркнуть) 6 из этих клеточек и отправить организаторам лотереи. После розыгрыша лотереи объявляются 6 выигравших номеров. Награждаются угадавшие все 6 номеров, 5 номеров, 4 номера и даже угадавшие 3 номера. Соответственно, чем меньше угадано номеров (видов спорта), тем меньше выигрыш.

Подсчитаем, сколько существует разных способов заполнения карточек «Спортлото». Казалось бы, заполняя последовательно номер за номером, должны получить: $49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44$. Но ведь порядок заполнения карточек не важен, поэтому используется формула числа сочетаний

$$C_{49}^6 = \frac{49!}{6!43!} = 13\,983\,816.$$

Эту же задачу можно решить и другим способом. Выпишем все номера подряд и под выбираемыми номерами поставим 1, а под остальными – 0. Тогда различные варианты заполнения карточек будут отличаться перестановками 1 и 0. При этом переставляется 6 единиц, соответствующих выбираемым клеточкам, и 43 нуля, соответствующих невыбираемым клеточкам, т. е. получаем

$$P(6,\ 43) = \frac{49!}{6!43!} = 13\,983\,816.$$

Если все участники заполнят карточки по-разному, то в среднем один из 14 миллионов участников выиграет 6 номеров. А сколько человек в среднем из 14 миллионов участников угадают 5 номеров?

Для решения этого вопроса возьмем один из угаданных номеров (число выборов $C_6^1 = 6$ и заменим его на один из не угаданных $\left(C_{43}^1 = 43\right)$. Всего вариантов замены будет: 6·43 = 256. Такое количество в среднем угадает 5 номеров из 14 миллионов участников. А сколько человек в среднем угадают 4 номера? Выберем из 6 угаданных номеров 2 номера и еще из 43 не угаданных 2 номера и произведем замену. Тогда получим: $C_6^2 \cdot C_{43}^2 = 13\,545$.

Аналогично найдем, что 3 номера угадают в среднем 246 820 человек, т. е. примерно 1,77% от всех играющих. Казалось бы, если взять 60 билетов и их «хорошо» заполнить, то можно надеяться на выигрыш хотя бы одной тройки номеров, при этом можно угадать и 4, и 5, и даже 6 номеров. Однако не все так просто. Чтобы гарантировать надежное угадывание 3-х номеров, число билетов должно быть существенно больше. Кроме того, нужно обосновать алгоритм «хорошего» заполнения билетов.

О целесообразности игры в «Спортлото» можно рассуждать с различных точек зрения. Прагматики понимают, что, купив *все* выпущенные билеты и как-то их заполнив, вы всегда проиграете, так как из выручки за проданные билеты сразу же производятся отчисления организаторам, изготовителям и распространителям билетов любой лотереи и, может быть, на какие-то благотворительные цели (например, на развитие спорта). Остатки идут на премии угадавшим 6, 5, 4 и 3 номера. Люди, верящие в свою счастливую судьбу, рассуждают примерно так: если не купить ни одного билета, то даже теоретической возможности выиграть не будет. Поэтому надо играть. Мне казалось, что компромисс между этими позициями состоит в том, чтобы, если уж очень хочется испытать судьбу, купить один билет. Однако лет 30 назад мое мнение об этом было поколеблено. В одном из крымских санаториев я познакомился с тренером по теренкуру, который при каждом заезде отдыхающих уговаривал их в складчину сыграть в «Спортлото», обещая честно разделить выигрыш. Меня же он попросил разработать алгоритм беспроигрышной игры в «Спортлото». Я ему честно сказал, что такого алгоритма не существует, и предложил алгоритм, который позволял при минимальном числе билетов гарантировать угадывание хотя бы одной комбинации из 3-х номеров. Он собрал деньги, купил билеты, и мы заполнили их по моему алгоритму. Объявлены выигравшие номера были накануне отъезда. Мы угадали несколько комбинаций из 3-х номеров и даже 2 комбинации из 4-х. Конечно, выигрыш был меньше затрат, что я и обещал ранее всем участникам. Однако, поскольку все участники эксперимента разъехались, то выигрыш полностью достался тренеру. Тогда я понял, что играть в лоте-

рею все-таки можно и *можно даже выигрывать*, но только в том случае, когда *играешь на чужие деньги*, а не на свои! Этот мой вывод уже в недавнее время подтвердили и продолжают подтверждать организаторы различных современных лотерей типа МММ.

Кстати, попробуйте обосновать алгоритм заполнения минимального числа билетов лотереи «Спортлото», при котором гарантируется угадывание хотя бы одной комбинации из 3-х номеров. А может быть, попробовать то же с 4 номерами?

4.1.8. Сочетания с повторениями

Пример. Требуется купить 7 пирожных. В магазине имеются пирожные следующих 4-х видов: эклеры, песочные, слоеные и наполеоны. Сколько вариантов покупки 7 пирожных 4-х видов?

Решим задачу следующим образом. Построим код из 7 единиц, к которому припишем справа три нуля: 1111111000. Будем переставлять теперь элементы этого кода всеми возможными способами. Можем получить, например, такой код: 1101111001. В соответствии с этим кодом сделаем такую покупку: купим эклеров столько, сколько единиц стоит перед первым нулем, песочных купим столько, сколько единиц стоит между первым и вторым нулем, слоеных купим столько, сколько единиц стоит между вторым и третьим нулем, наполеонов купим столько, сколько единиц стоит после третьего нуля. Таким образом, покупка будет выглядеть так: 2 эклера, 4 песочных, ни одного слоеного и 1 наполеон. Каждому коду можно сопоставить одну покупку и каждой покупке 7 пирожных 4-х видов однозначно можно сопоставить перестановку из 7 единиц и 3-х нулей. Таким образом, количество вариантов покупки равно

$$P(7,3)=\frac{10!}{7!3!}=120.$$

Обобщим полученное решение. Если имеются предметы n разных типов (без ограничений числа предметов каждого типа) и требуется определить, сколько комбинаций можно составить из них так, чтобы в каждую комбинацию входило k предметов. Каждую комбинацию будем шифровать с помощью 1 и 0, причем 1 будет соответствовать предметам, а нули будут выполнять функцию разделителей. Тогда, записав k единиц и добавив $n-1$ нуль, получим комбинацию, при которой выбираются k предметов первого типа и ни одного предмета остальных типов. Переставляя всеми способами эти k единиц и $n-1$ нуль, мы будем каждый раз получать некоторую расстановку, содержащую k предметов. Тогда

$$P(k, n-1) = \frac{(k+n-1)!}{k!(n-1)!} = C_{n+k-1}^{k}. \qquad (4.8)$$

Упражнения.

1. Входной алфавит абстрактного конечного автомата содержит 5 символов, например a, b, c, d, e. Входные слова имеют длину в 11 символов. Сколько разных слов может быть подано на вход конечного автомата, если слова, имеющие одинаковый состав букв и различающиеся только порядком, считать одинаковыми? Например, слова *baabce* и *eabcba* считаются одинаковыми. При решении задачи нужно учесть, что формула (4.8) определяет только количество вариантов выбора букв, но не их порядок в слове.

2. Граф-схема алгоритма микропрограммного автомата содержит операторные и условные вершины. Операторные вершины «начало» и «конец» являются обязательными. Сколько существует различных граф-схем алгоритмов, содержащих 6 вершин, если нас интересует только количественный состав, а не связи между вершинами?

3. У человека, спустившегося с гор, есть 5 баранов, которых он хочет раздать своим 8 сыновьям. Ему нужно найти число способов раздачи целых баранов, если:

a) каждый сын может получить либо одного барана, либо ничего;

b) число баранов, которые получают сыновья, неограничено (но, естественно, не превышает 5).

4. Некоторый банк имеет 3 «свободных» миллиона и готов раздать их 5 клиентам. Правление банка принимает решение о выдаче ссуды, кратной 0,25 миллиона. Сколько существует способов выдачи ссуд?

4.1.9. Свойства чисел сочетаний

Приведем некоторые свойства чисел сочетаний, которые часто используются при преобразованиях формул комбинаторики.

1. $C_n^k = C_n^{n-k}$.

2. $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$.

3. $C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^n = 2^n$.

Первое свойство совершенно очевидно. Второе легко доказывается, если оба члена правой части представить по формуле (4.7). Третье свойство можно доказать методом математической индукции. Для примера, при $n = 2$ получаем $C_2^0 + C_2^1 + C_2^2 = 1 + 2 + 1 = 2^2$. При $n = 3$ получаем $C_3^0 + C_3^1 + C_3^2 + C_3^3 = 1 + 3 + 3 + 1 = 2^3$.

Упражнения.

1. Полный дешифратор имеет n входов и 2^n выходов. Сколько выходов будет иметь дешифратор на 5 входов, если исключить все выходы, соответствующие равновесным входным наборам из 2-х и 4-х единиц?

2. В некотором государстве не было двух жителей с одинаковым набором зубов. Сколько жителей могло быть в этом государстве, если во рту человека не может быть больше 32-х зубов? Для оценки используйте очевидное неравенство: $2^{10} > 10^3$.

4.1.10. Основные формулы классической комбинаторики

Нами рассмотрены следующие основные случаи, которые обычно относят к классической комбинаторике.

1. *Размещения с повторениями*: $\overline{A}_n^k = n^k$.

Здесь n – число типов объектов, k – число позиций.

Примеры:

– количество k-разрядных чисел в системе с основанием n;

– максимальное число попыток вскрытия замка, состоящего из n ячеек с k – числом позиций (устойчивых положений) каждой ячейки.

2. *Размещения без повторений*: $A_n^k = \dfrac{n!}{(n-k)!}$.

Здесь n – число различных объектов, k – число позиций. Каждый объект представлен в единственном экземпляре.

Примеры:

– выборы из n человек k человек с назначением их на должности;

– выборы из n предметов k предметов с присваиванием им номеров.

3. *Перестановки без повторений*: $P_n = n!$.

Примеры:

– различные списки выступающих;

– перестановка букв в слове в случае, когда ни одна буква не повторяется.

4. *Перестановки с повторениями*: $P(n_1, n_2, \ldots, n_k) = (n_1 + n_2 + \ldots + n_k)! / (n_1! n_2! \ldots n_k!)$.

Здесь $n_1, n_2, \ldots, n_k$ – количество объектов каждого типа.

Примеры:

– количество различных слов, получаемых перестановкой букв в словах, в которых одинаковые буквы могут повторяться несколько раз;

– равновесные коды.

5. *Сочетания без повторений*: $C_n^k = \dfrac{n!}{k!(n-k)!}$.

Формула сочетаний используется тогда, когда порядок выбора k предметов из n не учитывается.

Примеры:

– выбор нескольких человек из группы для выполнения каких-либо работ;

– выбор нескольких букв алфавита для использования в автомобильных номерах.

6. *Сочетания с повторениями*: $P(k, n-1) = \dfrac{(k+n-1)!}{k!(n-1)!} = C_{n+k-1}^{k}$.

Формула используется тогда, когда требуется набрать k предметов n типов.

Примеры:

– выдача n клиентам банка ссуды с использованием k квот;

– покупка k пирожных n типов.

4.2. Комбинаторные задачи с ограничениями

Рассмотрим несколько классов задач, в которых на комбинации накладываются определенные ограничения. Следует заметить, что таких классов задач встречается очень много.

4.2.1. Простые задачи с ограничениями

а) *«Задача о львах и тиграх»*. Имеется 5 львов и 4 тигра. Необходимо их расставить в ряд, но при этом дрессировщик знает, что тигр не может спокойно идти за тигром.

Для решения задачи сначала расставим львов с промежутками (получим 6 промежутков), выберем из них 4 и на них поставим тигров, а лишние промежутки уберем. В этом случае ни один тигр не будет идти за тигром. Таким образом, если львы и тигры обезличенные, то $C_6^4 = 15$. В общем случае при n львах и k тиграх получаем: C_{n+1}^{k}.

b) *«Задача о книжной полке»*. Из n книг, стоящих на полке, нужно выбрать k таких, которые не стояли рядом на книжной полке.

Отберем сразу k книг, останется $n-k$ книг. Расставим их с промежутками, получим $n-k+1$ промежуток. Выберем из этих промежутков k и на них вернем выбранные книги. Остальные промежутки уберем. Решение:

$$C_{n+k-1}^{k}. \qquad (4.9)$$

c) *«Рыцари короля Артура»*. 12 рыцарей сидят за круглым столом, едят, пьют вино и, естественно, ссорятся. Причем ссорятся сидящие рядом. Неожиданно приходит известие о том, что любимая дочь короля украдена. Нужно послать команду для спасения доче-

ри короля из 5 рыцарей, причем таких, которые не сидели рядом за круглым столом.

Множество всех рыцарей разбиваем на два подмножества в зависимости от того, входит ли в команду спасателей конкретный рыцарь, например Ланселот. Ответ: 15 + 21 = 36. При n рыцарях и составе команды спасателей из k рыцарей решение имеет вид

$$C_{n-k-1}^{k-1} + C_{n-k}^{k}. \qquad (4.10)$$

Упражнения.

1. Определите соотношение между n и k, при которых задачи a), b) и c) имеют решения.

2. Найдите все восьмиразрядные двоичные коды, содержащие по 5 единиц, в которых не встречаются подряд два нуля.

4.2.2. «Задачи о смещениях (о беспорядках)»

Рассмотрим задачу. Имеется 5 различных предметов, например букв A, B, C, D, E. Сколько существует различных перестановок этих предметов, в которых ни один предмет не находится на своем месте? Эту задачу можно решить с помощью теоремы о включениях и исключениях. Под объектами теоремы будем понимать различные перестановки предметов (их число равно 5! = 120). Будем считать, что перестановка обладает первым свойством, если первый предмет находится на своем месте, а остальные – на любых. Будем считать, что перестановка обладает вторым свойством, если второй предмет находится на своем месте, а остальные – на любых и т. д. Всего имеем пять свойств. Решение имеет вид

$$N\left(\overline{5}\right) = 5! - C_5^1 4! + C_5^2 3! - C_5^3 1! - C_5^5 0! = 44.$$

В некоторых случаях количество объектов, обладающих определенным набором свойств, зависит только от количества свойств, а не от самого набора. Тогда формула для подсчета числа объектов, не обладающих ни одним из выделенных свойств, упрощается. Так, при решении только что приведенной задачи количество перестановок, в которых некоторый предмет оказывался на своем месте, не зависело от того, какой конкретно предмет или предметы находились на своем месте, а зависело только от числа этих предметов. При произвольном n имеем

$$N\left(\overline{n}\right) = n! - C_n^1 (n-1)! + C_n^2 (n-2)! - \ldots + (-1)^n C_n^n 0! = D_n. \qquad (4.11)$$

Полученное значение D_n иногда называют формулой полного беспорядка или субфакториалом. Субфакториал можно представить и так:

$$D_n = n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + \frac{(-1)^n}{n!}\right], \qquad (4.12)$$

где выражение в [...] стремится к e^{-1} при неограниченном возрастании n.

Субфакториал имеет свойства, похожие на свойства обычного факториала, например $n! = (n-1)[(n-1)! + (n-2)!]$ – для обычного факториала, $D_n = (n-1)[D_{n-1} + D_{n-2}]$ – для субфакториала.

Субфкториалы легко вычисляются по рекуррентной формуле

$$D_n = n\,D_{n-1} + (-1)^n. \qquad (4.13)$$

Вычислим по формуле (4.13) значения некоторых субфакториалов. Для этого определим, что субфакториал $D_1 = 0$. Остальные значения субфакториала находятся по формуле (4.13):

n	1	2	3	4	5	6	7	8	9	10
D_n	0	1	2	9	44	265	1854	14833	133496	1334961

Упражнения.

1. Вычислите значения субфакториалов для $n = 11, 12, 13, 14$.

2. Имеется 7 различных предметов. В каком числе перестановок этих предметов ровно 3 предмета находятся на своих местах, а остальные – на чужих?

3. Электромонтажник забыл дома схему и монтирует 12-контактный разъем наугад. В каком числе комбинаций правильно будут припаяны ровно 4 провода, а остальные – неверно? Если считать, что вероятность некоторого дискретного события P может быть определена отношением числа благоприятных комбинаций к общему числу комбинаций, тогда можно оценить вероятность этого события. Определите эту вероятность, если общее число комбинаций в данном случае равно 12!.

4.2.3. «Задача о караване»

Рассмотрим еще одну задачу, решение которой может быть получено с использованием главной теоремы комбинаторики.

По пустыне много дней движется караван из 9 верблюдов. И верблюдам, и погонщикам надоело видеть перед собой хвост одного и того же верблюда. Сколько существует перестановок верблюдов таких, при которых ни один верблюд не идет за тем, за кем шел раньше? Выделим запрещенные пары верблюдов: (1 2), (2 3), (3 4), (4 5), (5 6), (6 7), (7 8), (8 9). Если под объектами теоремы понимать перестановки верблюдов, а под свойствами – наличие одной из запрещенных пар, тогда

количество перестановок, не обладающих ни одним из восьми свойств, будет равно

$$N\left(\overline{8}\right) = 9! - C_8^1 8! + C_8^2 7! - C_8^3 6! + \ldots C_8^8 1! = 148\,329.$$

В общем случае при n верблюдах получаем

$$N\left(\overline{n}\right) = n! - C_{n-1}^1 (n-1)! + C_{n-1}^2 (n-2)! -$$
$$-C_{n-1}^3 (-3)! + \ldots (-1)^n C_{n-1}^{n-1} 1! = D_n + D_{n-1}. \qquad (4.14)$$

Упражнения.

1. Пусть имеется последовательность некоторых чисел $a_1, a_2, a_3, \ldots, a_n$. В каком количестве перестановок не встречается ни одной подряд стоявшей пары?

2. В каком количестве перестановок чисел предыдущего примера встречается ровно 5 пар чисел, которые находились рядом в исходной расстановке?

4.3. Комбинаторные задачи на раскладки и разбиения

Этот класс задач часто используется для оптимизации стратегий в различных играх.

4.3.1. Раскладки с указанием числа предметов

При анализе стратегий различных игр часто требуется подсчитывать количество комбинаций при раскладке определенных предметов (карт, костей, спичек и т. п.). Наиболее распространенная карточная игра – преферанс. В классическом варианте этой игры 32 карты раздаются на руки трем игрокам по 10 карт каждому и 2 карты кладутся в «прикуп». Определим количество вариантов расклада при игре в преферанс:

$$N = \frac{32!}{(10!)^3 2!}.$$

Для обоснования полученной формулы выложим все карты подряд и переставим их 32! способами. При каждой перестановке первые 10 карт будем отдавать первому игроку, следующие 10 карт – второму, следующие 10 карт – третьему и последние 2 карты будем класть в «прикуп». После этого заметим, что перестановка 10 карт в руках каждого игрока не меняет варианта расклада, как и положения двух карт в «прикупе». Поэтому 32! разделим три раза на 10! и один раз на 2!.

При игре в древнюю китайскую игру НИМ раскладывается n спичек на 3 кучки. Подсчитаем число вариантов расклада при игре в НИМ.

Для определения числа вариантов расклада выпишем n единиц и справа добавим два нуля. После этого начнем переставлять эти объекты всеми возможными способами. Их число будет равно

$$P(n, 2) = \frac{(n+2)!}{n!2!}.$$

При $n = 10$

$$P(10, 2) = \frac{12!}{10!2!} = \frac{12 \cdot 11}{2} = 66.$$

Каждой перестановке из n единиц и 2-х нулей однозначно будет соответствовать вариант расклада n спичек на 3 кучки и наоборот, каждому раскладу n спичек на 3 кучки однозначно будет соответствовать одна перестановка из n единиц и 2-х нулей.

В общем случае, если раскладываются n предметов по k ящикам так, чтобы в 1-й ящик (кучку, в руки игроку) попал n_1 предмет, во второй ящик – n_2 предмета, в k-й – n_k предметов, при этом $n_1 + n_2 + n_3 + ... + n_k = n$, то число вариантов расклада равно

$$P(n_1, n_2, n_3, ..., n_k) = \frac{n!}{n_1!n_2!...n_k!} \qquad (4.15)$$

Упражнения.

1. Один из трех игроков в преферанс хочет сыграть «мизер». Для этого ему нужно, чтобы в прикупе находилась либо бубновая семерка, либо семерка треф, либо они вместе. Найдите количества вариантов такого расклада. Определите вероятность этого события.

2. Определите количество вариантов расклада при игре в НИМ, когда в любой кучке есть хотя бы одна (две, три) спички.

3. Командир взвода охраны расставляет солдат у трех объектов: 2-х солдат у первого, 4-х у второго и 1 у третьего. Сколько вариантов расстановки солдат?

4.3.2. Раскладка предметов на 2 кучки (в 2 ящика, кармана)

Рассмотрим простую задачу. Сколько существует вариантов расклада пяти одинаковых рублей в два кармана? Выпишем разные варианты расклада:

1-й карман: 5 р.; 4 р.; 3 р.; 2 р.; 1 р.; 0 р.;
2-й карман: 0 р.; 1 р.; 2 р.; 3 р.; 4 р.; 5 р.

Итого, существует 6 вариантов расклада пяти рублей по двум карманам. Если раскладываются n рублей, то число вариантов расклада равно $n+1$.

Если раскладываются предметы нескольких типов на 2 кучки (ящики, корзины, множества), то такой расклад можно выполнять независимо для каждого типа предметов.

Например. Два студента, гуляя по лесу, набрали 10 васильков, 15 незабудок и 12 ромашек. При раскладке на два букета они решили, что васильки можно разложить 11 различными способами, незабудки 16 и ромашки 13. Всего будет $11 \cdot 16 \cdot 13 = 2\,288$ различных способов. Среди этих способов встретятся и «несправедливые», когда в одном из букетов вообще не будет васильков, или ромашек, или незабудок, и даже учитывается расклад, при котором один из букетов будет пустым. Однако алгоритм более справедливого расклада мы обсудим позже.

Обобщим полученный результат. Если имеется n_1 предмет 1-го типа, n_2 предмета 2-го, ..., n_k предметов k-го типа и требуется разложить эти предметы на 2 кучки, то число вариантов расклада будет равно $(n_1+1)(n_2+1)...(n_k+1)$.

А теперь, используя полученное решение, найдем количество делителей любого целого числа N. Известно, что любое целое число однозначно может быть представлено в так называемой канонической форме, т. е. в виде произведения простых чисел в соответствующих степенях: $N = p_1^{n_1} \; p_2^{n_2} \; ... \; p_k^{n_k}$. Простым числом называется такое целое число, которое не имеет никаких делителей, кроме 1 и самого себя. Примерами простых чисел являются числа: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ... Задача о нахождении количества делителей любого целого числа N сводится к раскладке этого числа на два сомножителя. В этом случае степени простых сомножителей раскладываются так же, как цветы в вышеприведенной задаче. Таким образом, число делителей D некоторого числа N равно

$$D(N) = (n_1+1)(n_2+1)(n_3+1)...(n_k+1). \qquad (4.16)$$

Пример. Найти число делителей $N = 720$. В канонической форме $760 = 2^3 \cdot 5^1 \cdot 19^1$. Следовательно, число делителей равно $D(760) = (3+1)(1+1)(1+1) = 16$.

Для нахождения количества делителей N, кратных некоторому числу R, можно $\frac{N}{R}$ представить в канонической форме и найти количество делителей этого числа.

Например, найти количество делителей числа 600, кратных 15. Находим $\frac{600}{15} = 40 = 2^3 \cdot 5^1$. Количество делителей числа 600, кратных 15, равно $D(40) = (3+1)(1+1) = 8$.

Упражнения.

1. Сколько разных делителей имеют числа: 1350, 1617, 8280, 10013?

2. Сколько разных делителей, кратных 102, имеют число 62424?

При решении комбинаторных задач для нахождения числа благоприятных комбинаций иногда удобнее вычислять число неблагоприятных комбинаций и вычитать его из общего числа комбинаций.

Пример 1. Из n различных чисел требуется отобрать k таких, чтобы в выбранное множество не входили s конкретных чисел. Общее число выборов из n по k определяется формулой

$$C_n^k = \frac{n!}{k!(n-k)!}.$$

Возьмем s конкретных чисел и остальные доберем C_{n-s}^{k-s} способами. Это будет число неблагоприятных комбинаций. Число благоприятных комбинаций определится разностью $C_n^k - C_{n-s}^{k-s}$.

Пример 2. Из группы в 15 человек нужно отобрать бригаду, в которую должно входить не менее 5 человек. Сколько имеется вариантов выбора?

Подсчитаем число неблагоприятных комбинаций: $C_{15}^1 + C_{15}^2 + C_{15}^3 + C_{15}^4 = 15 + 105 + 455 + 1365 = 1940$. Общее число комбинаций равно $2^{15} - 1 = 32767$. Тогда число благоприятных комбинаций равно $32767 - 1940 = 30827$.

Упражнение.

Обобщите решение последней задачи, если выбор выполняется из n человек, а в бригаду должно войти не менее k человек.

4.3.3. Раскладка предметов по k ящикам

Рассмотрим следующую задачу. Трое мальчиков собрали 40 яблок. Сколько существует вариантов раздела яблок между ними?

Запишем 40 единиц и добавим к ним два нуля. Будем переставлять полученную комбинацию всеми возможными способами. Каждой перестановке взаимно однозначно будет соответствовать способ раздела 40 яблок на три кучки. Следовательно, число способов раздела равно

$$P(40, 2) = \frac{42!}{40!2!} = \frac{42 \cdot 41}{2} = 861.$$

Если требуется разложить n предметов по k ящикам, то число способов раскладки будет равно $P(n, k-1) = \frac{(n+k-1)!}{n!(k-1)!}$. Если же требуется

разложить n_1 предмет 1-го типа, n_2 предмета 2-го типа, ..., n_k предметов k-го типа по s ящикам, то число способов расклада будет равно $P(n_1, s-1)P(n_2, s-1)...P(n_k, s-1)$.

Рассмотренный способ раздела содержит комбинации, при которых в какой-либо кучке вообще может не оказаться ни одного предмета, поэтому его можно назвать несправедливым. Для обеспечения более справедливого раздела можно заранее разложить часть предметов по кучкам (ящикам, корзинам), а затем оставшиеся предметы раскладывать описанным несправедливым способом.

Упражнение.

Четверо грибников, гуляя по лесу, собрали 12 подберезовиков, 8 белых, 11 волнушек и 15 сыроежек. При разделе грибов решили, что каждый должен получить не менее чем по 2 подберезовика, по 1 белому, 2 волнушки и 3 сыроежки. Сколько вариантов раздела грибов?

4.3.4. «Флаги на мачтах»

На корабле имеется n флагов, которые в праздники развешивают по k мачтам. Сколько разных сигналов можно передать, по-разному развешивая флаги на мачтах?

Сначала будем считать, что все флаги одинаковые, и рассмотрим задачу развешивания n одинаковых флагов по k мачтам. Объяснить это можно неожиданным туманом. Тогда

$$P(n, k-1) = \frac{(n+k-1)!}{n!(k-1)!}.$$

Когда туман рассеется, получим окончательное решение, умножив $P(n, k-1)$ на $n!$, т. е.

$$\frac{(n+k-1)!}{n!(k-1)!}n!. \qquad (4.16)$$

Количество разных сигналов, получаемых путем развешивания флагов на мачтах, можно еще увеличить, если учитывать варианты, при которых вывешиваются не все флаги, а, например, только s флагов из n имеющихся. Тогда общее число расстановок будет равно

$$\sum_{i=1}^{n} C_n^s s! P(s, k-1). \qquad (4.17)$$

Упражнения.

1. Имеется 8 флагов и 4 мачты. Подсчитайте количество разных сигналов, которые можно передать, по-разному развешивая флаги на мачтах.

2. Определите, во сколько раз увеличится количество сигналов, если учесть способы развешивания не всех флагов.

4.3.5. «Покупка билетов»

Перед кассой кинотеатра стоит очередь из n владельцев рублей и k владельцев полтинников. Билет в кинотеатр стоит полтинник (было же такое время!). В каком количестве комбинаций очередь пройдет без задержки?

Для решения задачи уточним условия. Если к кассе подходит человек с полтинником, он отдает его и получает билет. Если подходит человек с рублем, он отдает рубль, получает на сдачу полтинник и билет. У кассирши нет запаса полтинников, т. е. вообще говоря, она не готова к работе, но в России этим никого не удивишь. Ясно, что задача имеет смысл, если число рублей меньше или равно числу полтинников, т. е. $n \le k$.

Возьмем комбинацию, при которой очередь застрянет, и запишем ее следующим образом: (s рублей + s полтинников) Р... Очередь, конечно, застрянет на рубле, перед которым было одинаковое число рублей и полтинников. Добавим впереди полтинник (их тогда станет $k+1$, и теперь уже число рублей будет строго меньше числа полтинников), а затем проинвертируем всю комбинацию до рубля включительно, на котором очередь застрянет (заменим полтинники на рубли и рубли на полтинники). Мы придем к комбинации из n рублей и $k+1$ полтинника, которая начинается с рубля: Р (s рублей + s полтинников) П... Если теперь взять n рублей и $k+1$ полтинник и начать комбинацию с рубля, то обратным преобразованием мы придем к комбинации, при которой очередь застрянет. Таким образом, число комбинаций из n рублей и k полтинников, при которой очередь в кассу застрянет, равно $P(n-1, k+1)$. Число же благоприятных комбинаций, при которых очередь пройдет без задержки, будет равно $P(n, k) - P(n-1, k+1)$. Например, при $n = 4$, $k = 5$ число благоприятных комбинаций равно $P(4, 5)-P(3, 6) = 126-84 = 42$.

4.4. Рекуррентные соотношения в комбинаторике

В ряде случаев комбинаторная задача не может быть решена с использованием описанных методов и приемов, но легко решается с помощью упорядоченного перебора вариантов. Часто это решение может быть получено с использованием так называемых рекуррентных соотношений. Рассмотрим несколько примеров.

4.4.1. «Задача о наклейке марок»

На почте имеются марки достоинством 4, 6 и 10 копеек. Для отправки заказного письма требуется наклеить марки так, чтобы сумма составляла 18 копеек. Сколько существует разных вариантов наклейки марок?

Будем считать, что порядок наклейки марок важен, т. е. способы наклейки марок достоинством в 4, 10, 4 копейки и 10, 4, 4 копейки – разные способы. Тогда можно написать следующее рекуррентное соотношение:

$$F(N) = F(N - 4) + F(N - 6) + F(N - 10), \qquad (4.18)$$

где под $F(N)$ понимается число способов наклейки марок в сумме, равной N копейкам. Формула (4.18) показывает, что все множество решений распадается на три несовместных подмножества в зависимости от того, какой наклеена последняя марка. Подсчитаем значения $F(N)$ для некоторых начальных значений N. Так, $F(N<0) = 0$, $F(0) = 1$ (не используется ни одна марка), $F(1) = F(2) = F(3) = 0$, $F(4) = 1$, $F(5) = 0$, $F(6) = 1$, $F(7) = 0$, $F(8) = 1$, $F(9) = 0$, $F(10) = 3$. Тогда для $n = 18$ получим $F(18) = F(14) + F(12) + F(8)$.

Используя соотношение (4.18) для каждого нового члена, далее получаем $F(18) = F(10) + F(8) + F(4) + F(8) + F(6) + F(2) + F(8) = F(10) + 3 \cdot F(8) + F(4) + F(6) + F(2) = 3 + 3 + 1 + 1 + 0 = 8$.

4.4.2. «Задача об уплате долга»

В кошельке имеются монеты достоинством в 1, 2, 3, 5, 10, 15, 20 и 50 копеек. Требуется уплатить долг в 73 копейки. Каким количеством способов это можно сделать?

Запишем рекуррентное соотношение в общем случае, когда монеты имеют достоинство в $k_1, k_2, k_3, \ldots, k_m$ копеек и требуется набрать суму в N копеек, при этом произведем ранжирование монет по возрастанию:

$$F(k_1, k_2, k_3, \ldots, k_m; N) =$$

$$= F(k_1, k_2, k_3, \ldots, k_{m-1}; N - k_m) + F(k_1, k_2, k_3, \ldots, k_{m-1}; N). \qquad (4.19)$$

Первый член правой части (4.19) учитывает количество комбинаций, в которых монета старшего достоинства использована, второй член – в которых монета старшего достоинства не использована. Для рассматриваемого примера $F(1, 2, 3, 5, 10, 15, 20, 50; 73) = F(1, 2, 3, 5, 10, 15, 20; 73) + F(1, 2, 3, 5, 10, 15, 20; 23)$.

Первый член полученного выражения равен 0, так как сумма оставшихся монет меньше набираемой суммы. Применим ту же рекуррент-

ную формулу ко второму члену. В результате получим $F(1, 2, 3, 5, 10, 15, 20; 23) = F(1, 2, 3, 5, 10, 15; 3) + F(1, 2, 3, 5, 10, 15; 23)$.

В первом члене правой части монеты достоинством в 5, 10 и 15 копеек можно не учитывать, так как достоинство каждой из этих монет больше набираемой суммы, т. е. можно правую часть переписать так: $F(1, 2, 3; 3) + F(1, 2, 3, 5, 10, 15; 23) = F(1, 2; 0) + F(1, 2; 3) + F(1, 2, 3, 5, 10; 8) + F(1, 2, 3, 5, 10; 23) = 1 + F(1;1) + F(1; 3) + F(1, 2, 3, 5; 8) + F(1, 2, 3, 5, 10; 23)$.

Очевидно, что $F(1, 2; 0) = 1$, $F(1, 2; 3) = F(1; 1) = 1$, $F(1; 3) = 0$, $F(1, 2, 3, 5, 10; 23) = 0$. Поэтому правая часть перепишется в виде $1+1+0+F(1, 2, 3, 5; 8) + 0 = 2 + F(1, 2, 3; 3) + F(1, 2, 3; 8) = 2+2+0 = 4$. Таким образом, задача имеет 4 различных решения.

Еще раз подчеркнем, что в последней задаче порядок монет не важен.

4.4.3. «Задача о размене гривенника»

Рассмотрим задачу, в которой сняты ограничения как на порядок предметов, так и на их количество: размен гривенника (10 копеек) монетами достоинством в 1, 2, 3 и 5 копеек. Для этого случая рекуррентное соотношение можно представить в следующем виде: $S(1, 2, 3, 5; 10) = S(1, 2, 3; 10) + S(1, 2, 3; 5) + S(1, 2, 3; 0)$.

Все множество решений разбивается на подмножества в зависимости от числа монет старшего достоинства, использованных для размена.

Найдем все 20 способов размена:

$5\cdot2$	$5 + 1\cdot5$	$3 + 2\cdot3 + 1$	$2\cdot4 + 1\cdot2$
$5 + 3 + 2$	$3\cdot3 + 1$	$3 + 2\cdot2 + 1\cdot3$	$2\cdot3 + 1\cdot4$
$5 + 3 + 1\cdot2$	$3\cdot2 + 2\cdot2$	$3 + 2 + 1\cdot5$	$2\cdot2 + 1\cdot6$
$5 + 2\cdot2 + 1$	$3\cdot2 + 2 + 1\cdot2$	$3 + 1\cdot7$	$2 + 1\cdot8$
$5 + 2 + 1\cdot3$	$3\cdot2 + 1\cdot4$	$2\cdot5$	$1\cdot10$

В приведенных выше задачах использовались копейки, однако все рассуждения справедливы и для рублей и сотен рублей, для долларов и сотен долларов, т. е. метод решения не зависит от достоинства или стоимости предметов. Все разменные автоматы и банкоматы, выдающие набор купюр определенных достоинств, должны решать подобные задачи.

4.5. Задачи для контрольной работы

1. В спортивном клубе 25 человек. Требуется составить команду из 4-х человек для участия в беге на 100 м. Сколькими способами это можно сделать? А если требуется составить команду из 4-х человек для участия в эстафете 100 + 200 + 400 + 800 м?

2. В скольких 7-разрядных числах все цифры различны?

3. Сколько чисел от 1 до 900 не делится ни на 3, ни на 7, ни на 11?

4. На загородную прогулку выехали 92 человека. Бутерброды с колбасой взяли 48 человек, с сыром – 38, с ветчиной – 42, с сыром и колбасой – 28, с колбасой и ветчиной – 31, с сыром и ветчиной – 26. 25 человек взяли с собой все три вида бутербродов. Сколько человек взяли пирожки?

5. Сколько разных делителей, кратных 10, имеет число 3350?

6. Четыре числа сложили всеми возможными способами по 2 и получили 6 сумм: 2, 4, 9, 9, 14, 16. Найдите эти числа.

7. На прямой взяты p точек, а на параллельной ей прямой еще g точек. Сколько существует треугольников, вершинами которых являются эти точки?

8. В каком числе перестановок из 33 букв русского алфавита не встречаются слова СТУДЕНТ, ДЕКАН, ИНСТИТУТ?

9. 4 волчка с 3, 5, 11 и 4 гранями соответственно запускаются и останавливаются в некоторых положениях. Сколькими различными способами они могут упасть? А если известно, что, по крайней мере, 3 из них остановились на цифре 2?

10. У мамы 3 яблока, 4 груши и 4 апельсина. Каждый день в течение 11 дней подряд она выдает дочери по одному фрукту. Сколькими способами она это может сделать?

11. Найдите число способов наклейки марок достоинством в 3, 5 и 10 копеек так, чтобы общая сумма была равна 16 копейкам.

12. Имеется 4 утки, 3 курицы и 2 гуся. Сколькими способами можно выбрать из них несколько птиц так, чтобы среди выбранных были и утки, и куры, и гуси?

13. Найдите и выпишите все перестановки их букв X, Y, Z, при которых ни одна буква не остается на своем месте. А сколько существует перестановок из букв a, b, c, d, e, при которых ровно одна из них на своем месте?

14. Из колоды в 52 карты двое игроков выбирают по 4 карты каждый. Сколько существует различных вариантов выбора? В скольких случаях один из игроков получает 4 туза, а другой – 4 короля?

15. Сколько 6-разрядных чисел содержат ровно 3 различные цифры? Сколько n-разрядных чисел содержат ровно k различных цифр?

16. Сколько чисел, меньших миллиона, можно записать с помощью цифр 9, 8, 7. А с помощью цифр 9, 8, 0, если число не может начинаться с 0?

17. Сколькими способами можно переставить буквы слова ЮПИТЕР так, чтобы гласные шли в алфавитном порядке?

18. На собрании должны выступить 5 человек A, B, C, D, E. Сколькими способами можно составить списки выступающих при условии, что B не должен выступать до тех пор, пока не выступит A? Решите ту же задачу при условии, что A должен выступить непосредственно перед B.

19. Сколькими способами можно переставить буквы слова КАРАКУЛИ так, чтобы никакие две гласные не стояли рядом?

20. Сколько разных делителей, кратных 21, имеет число 525?

21. Сколько разных списков для выступлений можно составить из 20 депутатов, если депутаты З, Ж и Я уже обеспечили себе места соответственно 7, 11 и 13 ?

22. Сколько разных делителей имеет число 6350?

23. В каком числе перестановок из 33 букв русского алфавита встречаются слова СПОРТ, ПРОФЕССОР, КАЧЕЛИ?

24. Директор школы отобрал 7 учеников для награждения, но денег хватило только на 3 книги «Гарри Поттер и философский камень». Сколько вариантов награждения?

25. Имеется 11 тетрадей, 7 авторучек и 5 комплектов контурных карт. Сколькими способами можно выбрать из них несколько предметов так, чтобы среди выбранных были все имеющиеся виды предметов?

26. Сколько существует комбинаций из 8 рублей и 9 полтинников, при которых очередь в кассу застрянет?

27. Сколько 8-разрядных чисел содержат ровно 3 различные цифры? Сколько n-разрядных чисел содержат ровно k различных цифр?

28. Сколькими способами можно переставить буквы слова САЛАМАНДРА так, чтобы никакие две гласные не стояли рядом?

29. В каком числе перестановок из 26 букв английского алфавита не встречаются слова BOOK, HELP, INDEPENDENT?

30. В компании 7 мужчин и 5 женщин. Сколько вариантов выбора группы, в которой было бы не менее 3-х женщин?

31. На корабле имеется 30 флагов и 5 мачт. Сколько различных сигналов можно передать, развешивая флаги на мачтах?

32. Сколько разных ожерелий можно составить из 5 изумрудов, 3 рубинов и 7 сапфиров?

33. В скольких 7-разрядных числах все цифры различны?

34. Сколько существует способов уплаты 18 копеек, если имеется по одной монете каждого достоинства в 1, 2, 3, 5, 10, 15 копеек?

35. Из 25 человек, работающих в отделе, 14 имеют диплом инженера, 8 – диплом техника, 7 – диплом экономиста, 5 – одновременно диплом инженера и техника, 4 – диплом инженера и экономиста, 6 – диплом техника и экономиста, 2 имеют все три вида дипломов. Руководство решило уволить сотрудников без дипломов. Сколько может быть уволено сотрудников?

36. В каком числе перестановок из 33 букв русского алфавита встречаются слова АБИТУРИЕНТ, КОКОС, АМБРОЗИЯ?

37. На книжной полке 15 книг. Сколько существует способов взять с полки 7 книг, которые не стояли рядом? А 12 книг?

38. Найдите число способов наклейки марок достоинством в 3, 5, 6 и 10 копеек так, чтобы общая сумма была равна 18 копейкам.

39.Сколько существует способов раздачи 7 авторучек 8 ученикам без ограничения числа авторучек, передаваемых каждому?

40. Сколько существует перестановок из букв a, b, c, d, e, f, при которых ровно 2 буквы остаются на месте, а остальные – на чужих?

41. В отчете профкома написано: в отделе 7 человек имеют сыновей, 8 – дочерей, 4 – человека и сыновей и дочерей, 1 не имеет детей. Число работающих в отделе не было указано. Сколько человек работает в отделе?

42. Сколькими способами можно переставить буквы слова САТУРН так, чтобы гласные шли в алфавитном порядке?

43. За круглым столом короля Артура сидят 15 рыцарей. Сколько существует способов выбрать из них 6 таких, которые не сидели рядом за столом?

44. Сколько слов можно составить из трех букв a, двух букв b и одной буквы c?

45. Имеется 9 предметов. В скольких перестановках точно 2 предмета остаются на месте?

46. Сколько четных делителей имеет число 1520?

47. На карусели имеется 8 мест. Сколько существует разных способов рассадки детей, если все места будут заняты?

48. Найдите число способов наклейки марок достоинством в 2, 3, 5 и 10 копеек так, чтобы общая сумма была равна 14 копейкам.

49. Сколько чисел от 1 до 1678 не делится ни на 3, ни на 5, ни на 13?

50. На полке 20 книг. Сколькими способами можно выбрать из них 9 книг, которые не стояли рядом? А сколько вариантов для выбора 11 книг?

51. Сколько существует способов разложить 12 роз, 8 пионов и 9 флоксов на 3 букета так, чтобы в каждом букете было бы не менее чем по 3 розы, 2 пиона и 1 флоксу?

52. Сколькими способами можно переставить буквы слова БАКАЛАВР так, чтобы никакие две гласные не стояли рядом?

53. В каком числе перестановок из 26 букв английского алфавита не встречаются слова MAELSTROM, NOTICE, REDOUND?

54. В каком числе перестановок из 26 букв английского алфавита встречаются слова HELP, COMMAND, SPACE?

55. При игре в преферанс одному из игроков, чтобы сыграть «мизер», нужно, чтобы в прикупе оказалась бубновая семерка. В каком количестве случаев это может быть?

56. На прямой взяты 9 точек, а на параллельной ей прямой еще 5 точек. Сколько существует треугольников, вершинами которых являются эти точки?

Литература

1. *Виленкин*, *Н. Я.* Популярная комбинаторика / Н. Я. Виленкин. М.: Наука, 1975. 208 с.

2. *Риордан*, *Дж.* Введение в комбинаторный анализ: [пер. с англ.] / Дж. Риордан. М.: Изд-во иностр. лит., 1963. 287 с.

3. *Холл*, *М.* Комбинаторика: [пер. с англ.] / М. Холл. М.: Мир, 1970. 424 с.

4. *Ерош*, *И. Л.* Дискретная математика. Комбинаторика: учеб. пособие / И. Л. Ерош. СПбГУАП. СПб., 2001. 36 с.

5. ТЕОРИЯ ГРАФОВ

Язык графов используется в ряде математических разделов, таких, например, как теория управляющих автоматов, теория алгоритмов, теория цепей Маркова. Широко применяется язык теории графов при описании моделей в экономике, биологии и других областях.

5.1. «Задача о кёнигсбергских мостах»

Первой работой, в которой использовалось название «граф» и давалось его точное определение, была работа Л. Эйлера, которая появилась в 1736 году в трудах Петербургской академии наук. В ней Эйлер предлагает читателю головоломку «Задача о кёнигсбергских мостах». Город Кёнигсберг (ныне Калининград) расположен на двух берегах реки Прегель и двух островах. Районы города соединены мостами (рис. 5.1, *a*).

Вопрос состоит в том, можно ли, выйдя из одного района города, по одному разу пройти по каждому из мостов и вернуться в исходный район?

Л. Эйлер каждому району сопоставляет вершину, каждому мосту – ребро и уже на языке графов (рис. 5.1, *b*) формулирует задачу: существует ли циклический маршрут из последовательности ребер, выходящий из любой вершины графа и проходящий по каждому ребру в точности по одному разу?

Попытки найти такой маршрут к успеху не приводят, и тогда Л. Эйлер формулирует и доказывает свою теорему: *Для того чтобы существовал циклический маршрут в графе G, необходимо и достаточно, чтобы граф был связным и степени всех его вершин были четными.*

Теперь мы можем сформулировать определение графа. Графом называется пара (V, E), где V – множество вершин, E – множество инцидентных им ребер. Под степенью вершины графа понимается число ребер, инцидентных этой вершине (связанных с ней).

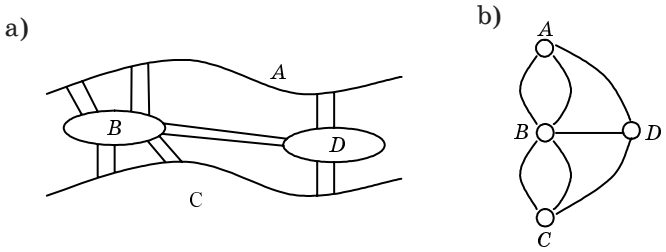


Рис 5.1. Граф переходов по мостам г. Калининграда

5.2. Виды графов

В различных технических приложениях встречаются графы, которые существенно отличаются внешним видом, а следовательно, и своими свойствами.

Основные виды графов показаны на рис. 5.2.

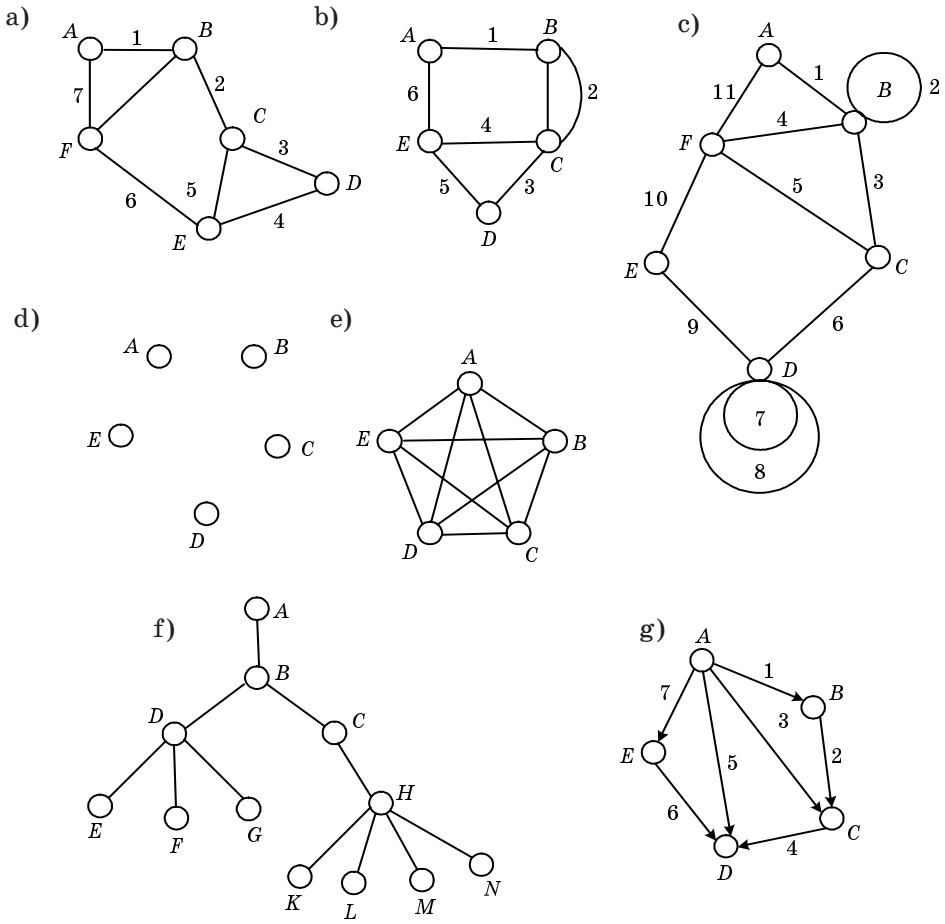


Рис. 5.2. Основные виды графов: *a* – обычный граф; *b* – граф с кратными ребрами; *c* – граф с петлями и вложенными петлями; *d* – «нуль-граф» – граф, не имеющий ребер, но имеющий вершины); *e* – «полный граф» – граф, у которого все вершины связаны со всеми остальными; *f* – граф типа «дерево», т. е. граф, у которого нет внутренних циклов; *g* – направленный граф, у которого переходы из вершины в вершину имеют направления

Встречаются и различные комбинации приведенных графов, например графы с кратными ребрами и петлями, графы с направленными и ненаправленными переходами (ребрами) и т. п.

5.3. Способы задания графов

Для того чтобы использовать задания в виде графов при решении разнообразных оптимизационных задач, применяют различные эквивалентные способы задания. Основным требованием является взаимная однозначность графического изображения и выбранного способа задания. Чаще всего используются следующие виды задания графа:

– матрица инциденции;

– список ребер;

– матрица смежности.

Рассмотрим эти виды задания.

1. Матрица инциденции. Нумеруются все ребра графа (например, арабскими цифрами) и все вершины (например, буквами). Строится матрица, каждой строке которой сопоставляется ребро, а каждому столбцу – вершина. Символами (например, единицами), отмечаются вершины, связанные ребрами. Так, для графов типа *a*, *b* (см. рис. 5.2) матрицы инциденции имеют вид (табл. 5.1, 5.2).

В табл. 5.2 два кратных ребра, связывающие вершины *B* и *C*, заменены одним ребром с двойной связью (обозначены цифрой 2).

В графе *c* (см. рис. 5.2) имеются петли. Для их указания можно использовать любые символы, отличные от 1. Мы использовали символ *. В вершине *D* имеются две петли. Их можно указывать отдельно (табл. 5.3) либо объединить две петли в одну и отметить каким-либо новым символом, например **.

При построении матрицы инциденции для направленного графа *d* (см. рис. 5.2) необходимо было указать направление перехода. Для этого в столбце, соответствующем вершине, из которой выходит стрелка,

Таблица 5.1

a)

Ребро	*A*	*B*	*C*	*D*	*E*	*F*
1	1	1				
2		1	1			
3			1	1		
4				1	1	
5			1		1	
6					1	1
7	1					1
8		1				1

Таблица 5.2

b)

Ребро	*A*	*B*	*C*	*D*	*E*
1	1	1			
2		2	2		
3			1	1	
4			1		1
5				1	1
6	1				1

Таблица 5.3

c)

Ребро	*A*	*B*	*C*	*D*	*E*	*F*
1	1	1				
2		*				
3		1	1			
4		1				1
5			1			1
6			1	1		
7				*		
8				*		
9				1	1	
10					1	1
11	1					1

Таблица 5.4

d)

Ребро	*A*	*B*	*C*	*D*	*E*
1	−1	1			
2		−1	1		
3	−1		1		
4			−1	1	
5	1			−1	
6				1	−1
7	−1				1

мы писали −1 (источник), а в столбце, соответствующем вершине, в которую входит стрелка, 1 (сток) (табл. 5.4).

Для остальных графов читателю предлагается самостоятельно нарисовать матрицы инциденции.

2. Список ребер. Этот список является сокращением матрицы инциденции. Число строк, как и ранее, равно числу ребер графа, а столбцов только два. В первом указываются вершины, из которых выходят ребра, а во втором – в которые входят. Приведем списки ребер для графов типа *a*, *b*, *c*, *d* (см. рис. 5.2) (табл. 5.5–5.8).

3. Матрица смежности. Матрица строится следующим образом. Каждой строке и каждому столбцу соответствует вершина графа. На пересечении строки и столбца ставятся символы, например 1, если эти вершины связаны одним ребром, 2 – если двумя и т. д. Для первых трех видов графов *a*, *b*, *c* (см. рис. 5.2) матрицы смежности имеют вид (табл. 5.9–5.11).

Таблица 5.5

a)

Ребро	Вершина	
1	*A*	*B*
2	*B*	*C*
3	*C*	*D*
4	*D*	*E*
5	*C*	*E*
6	*E*	*F*
7	*A*	*F*
8	*B*	*F*

Таблица 5.6

b)

Ребро	Вершина	
1	*A*	*B*
2	*B2*	*C2*
3	*C*	*D*
4	*E*	*C*
5	*D*	*E*
6	*A*	*E*

Таблица 5.7

c)

Ребро	Вершина	
1	*A*	*B*
2	*B*	*B*
3	*B*	*C*
4	*B*	*F*
5	*C*	*F*
6	*C*	*D*
7	*D*	*D*
8	*D*	*D*
9	*D*	*E*
10	*E*	*F*
11	*F*	*A*

Таблица 5.8

d)

Ребро	Источник	Сток
1	*A*	*B*
2	*B*	*C*
3	*A*	*C*
4	*C*	*D*
5	*D*	*A*
6	*E*	*D*
7	*A*	*E*

Очевидно, что для ненаправленных графов без петель *a*, *b* (см. рис. 5.2) матрица смежности симметрична относительно главной диагонали (табл. 5.9, 5.10). Если исключить избыточную информацию (главную диагональ и верхнюю правую половину матрицы), то получим треугольную таблицу.

Таблица 5.9

a)

	A	*B*	*C*	*D*	*E*	*F*
A		1				1
B	1		1			1
C		1		1	1	
D			1		1	
E			1	1		1
F	1	1			1	

Таблица 5.10

b)

	A	*B*	*C*	*D*	*E*
A		1			1
B	1		3		
C		3		1	1
D			1		1
E	1		1	1	

Таблица 5.11

c)

	A	*B*	*C*	*D*	*E*	*F*
A		1				1
B	1	1	1			1
C		1		1		1
D			1	2	1	
E				1		1
F	1	1	1		1	

Таблица 5.12

d)

	A	*B*	*C*	*D*	*E*
A		1	1		1
B			1		
C				1	
D	1				
E				1	

При построении матрицы смежности для направленного графа d (см. рис. 5.2) каждой строке сопоставляется вершина, из которой выходит стрелка, а каждому столбцу – вершина, в которую входит стрелка (табл. 5.12). Матрицы смежности для направленного графа не являются симметричными относительно главной диагонали, и поэтому они не сжимаются до треугольных таблиц.

5.4. Понятие о плоских графах – «Задача о трех домах и трех колодцах»

Рассмотрим простую головоломку, которая называется «Задача о трех домах и трех колодцах». Три друга получили садовые участки и начали строить дома. Сначала выкопали три колодца и ходили к любому из них. Когда же дома были построены, приехали домочадцы и, как часто бывает, перессорились. И потребовали, чтобы хозяева сделали дорожки так, чтобы от любого дома можно было бы дойти до любого колодца, но дорожки не должны были пересекаться, чтобы домочадцы не встречались на пути к колодцам. Можно ли удовлетворить требования домочадцев?

Все попытки удовлетворить требования домочадцев заканчиваются неудачно (рис. 5.3). Почему? Потому, что этот граф невозможно на плоскости изобразить так, чтобы его ребра не пересекались. Этот граф не является плоским.

Вопрос о том, является ли граф плоским или нет – исключительно важен для технологии интегральных микросхем. Ведь каждая микросхема представляет собой некоторый граф, в котором имеются контактные площадки (вершины) и связи (ребра).

Задача может ставиться так: имеется новая схема (например, процессора). На какое минимальное число фрагментов ее нужно разбить, чтобы каждый фрагмент мог быть представлен плоским графом?

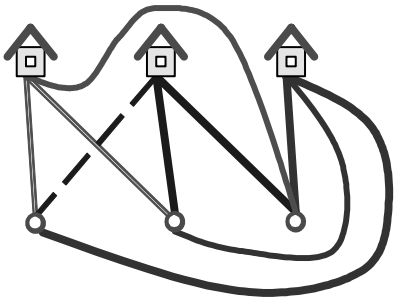


Рис. 5.3. «Задача о трех домах и трех колодцах»

5.5. Теорема Жордана о плоских графах

Вопрос о том, является ли граф плоским или нет и какие существуют необходимые и достаточные условия для того, чтобы граф был плоским, волновали математиков давно. Первые работы на эту тему принадлежат Жордану. Им была доказана теорема, существо которой сводится к следующему. Пусть на плоскости имеется некоторая непрерывная замкнутая линия L. Эта линия делит всю плоскость на две части: внутреннюю и внешнюю (рис. 5.4). Пусть на линии L имеются три пары точек, которые нужно соединить так: a с b, c с d, e с f. Соединить a с b можно, например, по внутренней области линией L_1, c с d – по внешней области линией L_2, тогда линия L_3, соединяющая e с f, обязательно пересечет либо L_1, либо L_2.

5.6. Определение числа ребер в графе

Число ребер графа можно определять различными способами. Наиболее простой способ – прямой пересчет ребер. Другой способ использует понятие степеней вершин графа. Рассмотрим граф типа a (см. рис. 5.2) и подсчитаем степени ρ его вершин. Получим: $\rho(A) = 2$; $\rho(B) = 3$; $\rho(C) = 3$; $\rho(D) = 2$; $\rho(E) = 3$; $\rho(F) = 3$. Если просуммировать степени всех вершин и разделить это число пополам, получим количество ребер графа. Так, для графа типа a имеем $\mathrm{P} = \dfrac{2+3+3+2+3+3}{2} = 8.$

В общем случае, пусть вершины графа обозначены $A_i (i = 1 \div n)$, тогда число ребер графа

$$\mathrm{P} = \frac{\sum_{i=1}^{n} \rho(A_i)}{2}. \qquad (5.1)$$

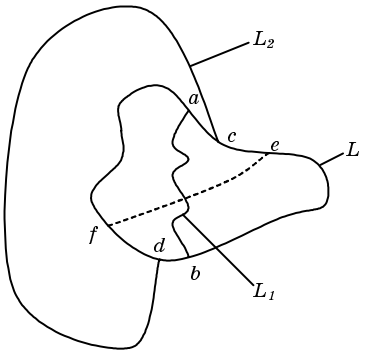


Рис. 5.4. Пояснение к теореме Жордана

Формула (5.1) для определения числа ребер графа применима как для графов с кратными ребрами, так и для графов с петлями. Следует только правильно подсчитывать степени вершин. Для этого нужно вокруг вершины провести маленькую окружность так, чтобы в нее не попала полностью петля. После чего подсчитать количество ребер, проходящих в этой окружности к вершине. Так, для вершины B графа c (см. рис. 5.2) получаем $\rho(B) = 5$, а для вершины D того же графа $\rho(D) = 6$. Число ребер этого графа $P = \frac{2+5+3+6+2+4}{2} = 11$, что соответствует значению, полученному прямым пересчетом.

5.7. Теорема о количестве вершин нечетной степени

Приведенные рассуждения позволяют сформулировать очевидную теорему о степенях вершин в графе: *В любом графе количество вершин нечетной степени четно*.

Во всех примерах графов это действительно так. Если бы был найден граф, у которого количество вершин нечетной степени было бы нечетным, то из формулы (5.1) следовало бы, что число ребер этого графа было бы нецелым!

5.8. Графы типа «дерево» – основные соотношения

В задачах сортировки используется особый вид графов – графы типа «дерево» (см. рис. 5.2, *f*) . Особенностью этих графов является то, что в них нет внутренних циклов.

Подсчитаем число ребер и вершин графа *f*: P = 11, B = 12. Легко показать, что в любом графе типа «дерево» число вершин на единицу больше числа ребер. Действительно, возьмем самый простой граф типа «дерево». Он будет содержать 2 вершины и одно ребро. Будем теперь произвольно наращивать этот граф, добавляя ребра и вершины. Число добавленных ребер будет равно числу добавленных вершин. Следовательно, в графе типа «дерево»

$$B - P = 1. \qquad (5.2)$$

5.9. Цикломатическое число графа

Рассмотрим произвольный граф, например граф *c* на рис. 5.2. В этом графе P = 11, B = 6. Для того чтобы превратить этот граф в граф типа «дерево», необходимо вычеркнуть 6 ребер. В этом случае будет справедливо соотношение (5.2).

Количество ребер графа, которые необходимо убрать, чтобы превратить его в граф типа «дерево», называется цикломатическим числом графа, т. е.

$$\gamma = P - B + 1. \qquad (5.3)$$

Для графа типа «дерево» $\gamma = 0$.

5.10. «Задача о наименованиях и переименованиях»

Справедливо утверждается*, что в любом городе мира наименование и переименование улиц и площадей является любимым занятием специального отдела мэрии. Особенно активно проводились переименования в период с 17-го по 90-е годы XX века в Советском Союзе. Может показаться странным, но переименования российских городов начались не с имен Ленина и Сталина, а с Троцкого. Российский город Гатчина получил новое имя Троцк. Следующий город получил имя Зиновьевск. И только затем небольшому поселку присвоили имя Сталино. Зато потом каждый член Политбюро получал по городу своего имени. Не повезло Рыбинску, который побывал и Андроповым, и Щербаковым, а затем опять стал Рыбинском. В атласе конца XX века 36 крупных городов мира носили имена, связанные с Лениным: Ленинград, Ленинабад, Ленинакан, Ленинварош и т. д.

Самым, пожалуй, курьезным случаем можно считать переименование старинного русского города Тверь, ровесника Москвы, в город Калинин. Указ об этом переименовании подписал «всесоюзный староста» М. И. Калинин в день своего рождения (своеобразный подарок себе ко дню рождения). В начале перестройки многим городам, улицам и площадям справедливо начали возвращать их прежние имена.

Мы тоже займемся присвоением улицам и площадям имен великих современников.

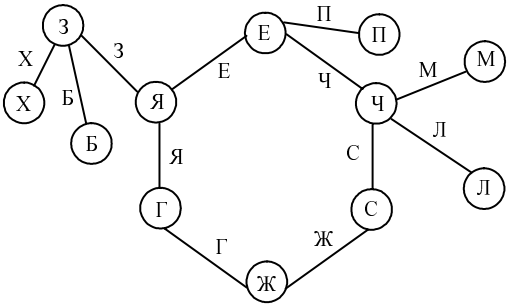


Рис. 5.5. План города демократов – цикл с ветвями в виде деревьев, вырастающих из вершин

* Оре О. Графы и их применение. М.: Мир, 1965. 174 с.

Пусть, например, бывшие пролетарии, а ныне демократы первой волны решили построить город и увековечить свои красивые фамилии. Пусть также принято условие, что каждый получает по улице и по площади, причем, улица Ельцина должна заканчиваться площадью Ельцина, улица Чубайса должна заканчиваться площадью Чубайса и т. д. План города демократов будет иметь такой вид (рис. 5.5).

Поскольку в этом городе число улиц (ребер) равно числу площадей (вершин), то цикломатическое число графа, соответствующего плану города демократов первой волны, равно $\gamma = 1$.

5.11. «Задача коммивояжера» и «Задача о минимальной сети дорог»

Во все времена математики пытались заработать на своих уникальных знаниях. Однако, похоже, что это удалось только венгерскому математику Рубику.

В 1859 году ирландский математик сэр Уильям Роуэн Гамильтон изготовил и пытался продавать новую головоломку. Он взял один из правильных многогранников (додекаэдр), в каждую вершину вбил маленькие гвоздики, а к одному гвоздю привязал веревку. Задача состояла в том, чтобы, наматывая веревку на гвоздики, образовать цикл такой, чтобы веревка (путь) прошла бы через все вершины в точности по одному разу. К сожалению, обыватели не заинтересовались головоломкой сэра Гамильтона, зато ее запомнили математики. Со временем, после некоторого изменения условий, эта головоломка превратилась в классическую теперь «Задачу коммивояжера», которая формулируется так. Имеется n городов и задана таблица попарных расстояний между ними. Найти циклический путь обхода по одному разу всех городов, при этом путь должен иметь минимально возможную длину. В более общих постановках на паре вершин задается значение некоторой функции и требуется найти цикл, при котором общее значение функции минимизируется или максимизируется.

В принципе, «Задача коммивояжера» была известна и российским коробейникам. Они обходили деревни и, как правило (если верить Некрасову), никогда не заходили в одну и ту же деревню дважды. А минимизировали они либо время обхода всех деревень, либо путь, либо количество стоптанных лаптей.

«Задача коммивояжера» очень похожа по постановке на задачу Эйлера о цикле в графе. Однако задача Эйлера была поставлена и блестяще решена Эйлером в его первой работе. Аналитическое решение «Задачи коммивояжера» до сих пор не найдено, хотя имеются достаточно хорошие решения, основанные на упорядоченном переборе (например,

метод Кенига). Для крупных городов США перебором найден цикл облета этих городов с минимизацией времени облета.

Известна еще одна задача, очень похожая по постановке на две предыдущие. Эта задача больше подходит к проблемам российской действительности. Называется она «Задача о минимальной сети дорог».

Путешествуя со студенческими строительными отрядами по Ленинградской области, авторы встречали некоторые населенные пункты в принципе недоступные большую часть года. Так, между городами Тихвином и Будогощью имеется некая деревушка, в которую можно пробраться по тропинкам через болота летом, если месяц не было дождей, или зимой, если долго стояли морозы. Да и то только на гусеничном тракторе. В остальное время деревню можно посетить только пешком, пробираясь с кочки на кочку через болота. Однако на большинстве карт дорога между Будогощью и Тихвином показана как дорога республиканского значения. Говорят, что эта ошибка сыграла хорошую службу во время Великой Отечественной войны. Немцы отступали от Тихвина в сторону Будогощи. Увидев на карте дорогу республиканского значения, решили, что это дорога с хорошим покрытием, и взяли всю тяжелую технику с собой. Между двумя городами вся эта техника навечно завязла в болотах.

Изложенные соображения приводят к новой постановке задачи для российской действительности. Имеется n городов и заданы попарные расстояния между ними. Построить граф типа «дерево» минимальной суммарной длины (рис. 5.6). В отличие от предыдущих двух задач алгоритм построения минимальной сети дорог прост и всегда приводит к решению. Для этого нужно из таблицы попарных расстояний выбрать минимальное расстояние и провести эту дорогу. Затем перейти к рассмотрению следующего минимального расстояния. Если имеются два или более минимальных расстояния, можно брать любое. На каждом

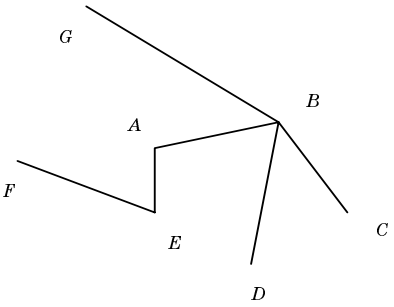


Рис 5.6. Минимальная сеть дорог

шаге необходимо следить, чтобы не образовался цикл. Как только все вершины будут задействованы, алгоритм завершен. Минимальный общий путь равен сумме всех выбранных путей.

Пусть, например, имеется 7 (*A, B, C, D, E, F, G*) городов и таблица минимальных расстояний.

Таблица 5.13

B	**18**					
C	24	**19**				
D	36	**25**	24			
E	**15**	21	33	18		
F	22	31	55	27	**19**	
G	28	**17**	41	19	29	22
	A	***B***	*C*	*D*	*E*	*F*

Из табл. 5.13 минимальное расстояние равно 15 (*A*–*E*). Соединим эти вершины. Следующее минимальное расстояние 17 (*B*–*G*). Соединим эти вершины. Следующее минимальное расстояние 18 (*A*–*B* и *E*–*G*). Мы можем выбрать только одно (любое) соединение, иначе образуется цикл. Возьмем, например, *A*–*B*, а *E*–*G* исключим из рассмотрения. Следующим минимальным расстоянием будет 19 (*E*–*F* и *C*–*B*). В данном случае мы можем соединить обе пары вершин. Очередное минимальное расстояние 21 (*B*–*E*) проводить нельзя, так как образуется цикл. Следующее минимальное расстояние 22 (*A*–*F F*–*G*) также следует пропустить (любая из этих пар образует цикл. Расстояние 24 (*A*–*C*) также неприемлемо, расстояние 25 (*B*–*D*) завершает построение минимальной сети дорог. Суммарная длина всех построенных дорог равна $L = 15+17+18+19+19+25 = 113$. Решения меньшей длины не существует.

5.12. Построение турнирной таблицы

Для проведения соревнований используются турнирные таблицы. В этих таблицах отмечается, какое количество туров нужно сыграть в турнире и какие команды или игроки должны играть в каждом туре. При этом количество туров должно быть минимально возможным, а в каждом туре должны быть заняты все или почти все игроки.

Приведем метод построения турнирной таблицы при условии, что число команд четное. Если число команд нечетное, то вводится фиктивный игрок, который не играет ни в одном туре и вместе с ним отдыхает его соперник по туру. Пусть число игроков равно N, при этом бу-

Таблица 5.14

1	2	3	4	5	6	.	.	.	.	N
2	2/1	N	$N-1$	$N-2$	$N-3$	.	.	.	4	3
3	4	3/1	2	N	$N-1$	.	.	.	6	5
4	6	5	4/1	3	2	N	.	.	8	7
.	.	.	.	.	.	.	.	.	.	.
$1/2N+1$	N	$N-1$	$N-2$	.	.	.	.	.	3	2
$1/2N+2$	3	2	N	$N-1$						
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
N	$N-1$	$N-2$	.	.	.	.	.	.	2	$N/1$

Таблица 5.15

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
2	1	8	7	6	5	4	3
3	4	1	2	8	7	6	5
4	6	5	1	3	2	8	7
5	8	7	6	1	4	3	2
6	3	2	8	7	1	5	4
7	5	4	3	2	8	1	6
8	7	6	5	4	3	2	1

дем считать, что N – четное. Перенумеруем игроков от 1 до N и выпишем их номера так, как указано в табл. 5.14. Затем зачеркнем номера на диагонали и заменим их на 1. В таблице это показано так: 2/1, 3/1, ..., $N/1$.

Из построенной таблицы видно, что в первом туре играют 1-й и 2-й игроки, 3-й и N-й и т. д. Число туров равно $N-1$ (минимально возможное), при этом в каждом туре заняты все участники.

Построим, например, турнирную таблицу для 7 игроков. Добавим фиктивного игрока для того, чтобы число участников стало четным. Таблица для 8 участников будет выглядеть так (табл. 5.15)

В первой строке построенной таблицы перечислены номера всех участников. В первом туре играют пары из 1-й и 2-й строк. Во втором туре играют пары из 1-й и 3-й строк и т. д. Один из игроков, например с номером 8, является фиктивным.

5.13. Теорема Куратовского о плоских графах

Плоским графам посвящено очень большое число работ. Попытки сформулировать необходимые и достаточные условия для того, чтобы граф был плоским, неоднократно предпринимались. Наиболее сильным результатом является теорема польского математика Куратовского. Прежде чем сформулировать его теорему, сделаем несколько предварительных замечаний.

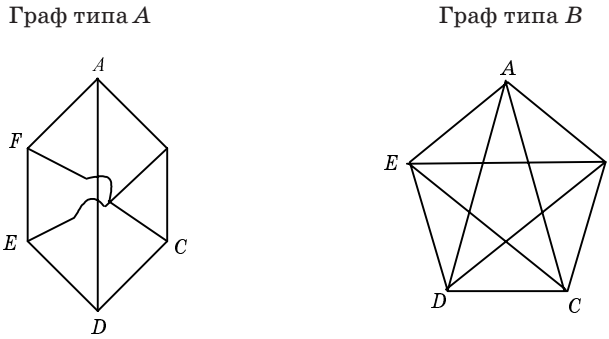


Рис. 5.7. Примеры неплоских графов с минимальным числом вершин

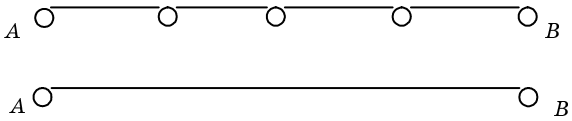


Рис. 5.8. Сжатие графа

На рис. 5.7 приведены два графа, которые не являются плоскими. Назовем их графами типа A и типа B.

Для произвольных графов введем операцию сжатия на графе. Пусть между двумя вершинами графа имеется путь, проходящий только через вершины степени 2 (рис. 5.8)

Заменим этот путь одним ребром, соединяющим A с B. Такая процедура называется сжатием на графе. Куратовский показал, что процедура сжатия на графе не меняет свойство графа быть плоским, то есть: если граф был плоским, то после сжатия он останется плоским, а если был не плоским, то останется не плоским.

Теорема Куратовского. *Для того чтобы граф G был плоским, необходимо и достаточно, чтобы после всех операций сжатия на графе внутри графа G не было бы графов типа A или типа B.*

5.14. Проецирование графа на сферу

Для плоских графов сформулировано несколько очень интересных теорем, например такая.

Теорема о прямых ребрах плоского графа. *Любой плоский граф может быть расположен на плоскости так, чтобы все его ребра были прямыми.*

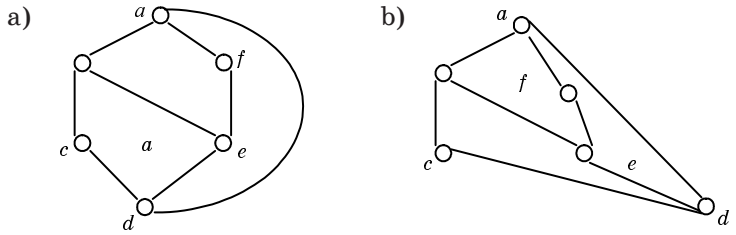


Рис. 5.9. Пояснение к теореме о прямых ребрах плоского графа

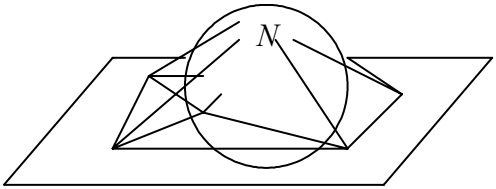


Рис. 5.10. Проецирование плоского графа на сферу

Возьмем какой-нибудь плоский граф. Например, если взять неплоский граф типа A и исключить из него одно ребро, он станет плоским (рис. 5.9, *a*).

Не меняя обозначений вершин и связей между ними, можно добиться того, чтобы все ребра стали прямыми (рис. 5.9, *b*).

Любой плоский граф может быть спроецирован на сферу.

Для проецирования плоского графа на сферу возьмем плоскость и на ней изобразим плоский граф G. Примерно в центре этого графа установим сферу и соединим все вершины плоского графа G с северным полюсом сферы N (рис. 5.10).

Отметим точки пересечения этих линий со сферой и соединим их между собой. Получим граф на сфере. Если через выделенные точки провести плоскости, мы получим некоторую объемную фигуру, вписанную в сферу. Таким образом, каждому плоскому графу будет соответствовать некоторый многогранник. Обратным проецированием мы каждому многограннику, вписанному в сферу, можем сопоставить некоторый плоский граф. Последняя процедура используется в картографии.

5.15. Теорема Эйлера о соотношении числа вершин, ребер и граней плоского графа

Рассмотрим некоторый плоский граф (рис. 5.11).

Назовем замкнутую область плоского графа, ограниченную ребрами и не имеющую внутри себя никаких фрагментов графа, *гранью*. Гра-

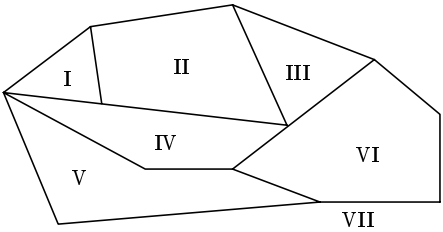


Рис. 5.11. Плоский граф с отмеченными гранями

ни плоского графа будет соответствовать грань многогранника, построенного путем проецирования плоского графа на сферу.

Подсчитаем число ребер, вершин и граней плоского графа: $Р = 17$, $В = 12$, $Г = 7$.

Эйлер доказал, что в любом плоском графе (так же, как и в любом многограннике) число вершин минус число ребер, плюс число граней равняется 2, т. е.

$$В - Р + Г = 2. \qquad (5.3)$$

Для плоского графа, изображенного на рис. 5.11, имеем $12 - 17 + 7 = 2$.

Интересно, что формула (5.3) справедлива и для графов с кратными ребрами, с петлями и с вложенными петлями (рис. 5.12). В этом графе имеются грани степени 1, т. е. ограниченные только одним ребром.

Таким образом, теорема Эйлера о плоских графах справедлива для любых плоских графов.

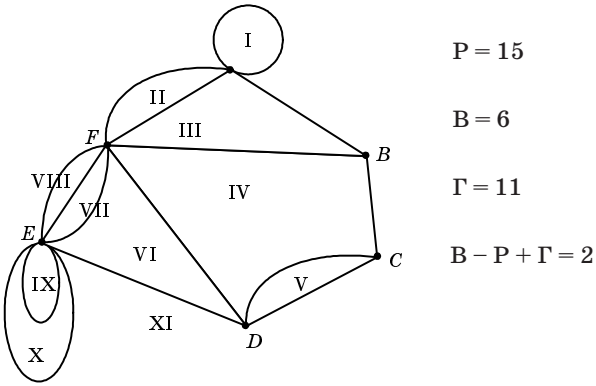


Рис. 5.12. Произвольный граф

5.16. Правильные многогранники

Для любого плоского графа число ребер можно сосчитать третьим способом – учитывая число ребер, ограничивающих каждую грань.

Пусть $\varphi(k)$ – количество граней степени k. Под гранью степени k будем понимать грань, ограниченную ровно k ребрами. Тогда число ребер графа можно определить по формуле

$$P = 1/2(\varphi(2)\cdot 2 + \varphi(3)\cdot 3 + \varphi(4)\cdot 4 + \varphi(5)\cdot 5 + \ldots). \qquad (5.4)$$

Так, для графа рис. 5.11 $\varphi(3) = 2$; $\varphi(4) = 2$; $\varphi(5) = 2$; $\varphi(6) = 0$; $\varphi(7) = 0$; $\varphi(8) = 1$; $\varphi(9) = 0$;... Поэтому $P = 1/2(2\cdot 3+2\cdot 4+2\cdot 5+1\cdot 8) = 16$. Прямой пересчет дает это же значение.

Формула (5.4) пригодна и для графов с кратными ребрами и вложенными петлями. Так, для графа рис. 5.12 получаем: $\varphi(1) = 2$; $\varphi(2) = 5$; $\varphi(3) = 2$; $\varphi(4) = 1$; $\varphi(8) = 1$. Тогда $P = 1/2(2\cdot 1+5\cdot 2+2\cdot 3+1\cdot 4+1\cdot 8) = 15$.

Возьмем произвольный плоский граф G и будем строить двойственный ему граф G^* по следующему правилу. В центре каждой грани плоского графа G выберем точку и назовем ее вершиной двойственного графа G^*. Соединим все новые вершины ребрами так, чтобы каждое ребро двойственного графа G^* пересекало в точности одно ребро (общее для двух граней) исходного графа G.

Результаты сравнения характеристик исходного графа G и двойственного ему графа G^* поместим в табл. 5.16.

Определение 1. *Граф G, у которого все степени вершин равны ρ, называется однородным.*

Таблица 5.16

Параметры графа	Исходный граф G	Двойственный граф G^*
Число вершин	В	$В^* = Г$
Число ребер	Р	$Р^* = Р$
Число граней	Г	$Г^* = В$

Определение 2. *Однородный граф G, у которого двойственный ему граф G^* тоже однороден, называется правильным графом. Правильным графам соответствуют правильные многогранники.*

Рассмотрение свойств правильных графов и, соответственно, правильных многогранников приводит к табл. 5.17.

Таблица 5.17

ρ	ρ^*	В	Р	Г	Тип правильного многогранника
3	3	4	6	4	Тетраэдр
3	4	8	12	6	Куб
3	5	20	30	12	Додекаэдр
4	3	6	12	8	Октаэдр
5	3	12	30	20	Икосаэдр

Поскольку каждому многограннику соответствует плоский граф и каждый плоский граф может быть нарисован на плоскости так, чтобы все его ребра были прямыми, приведем

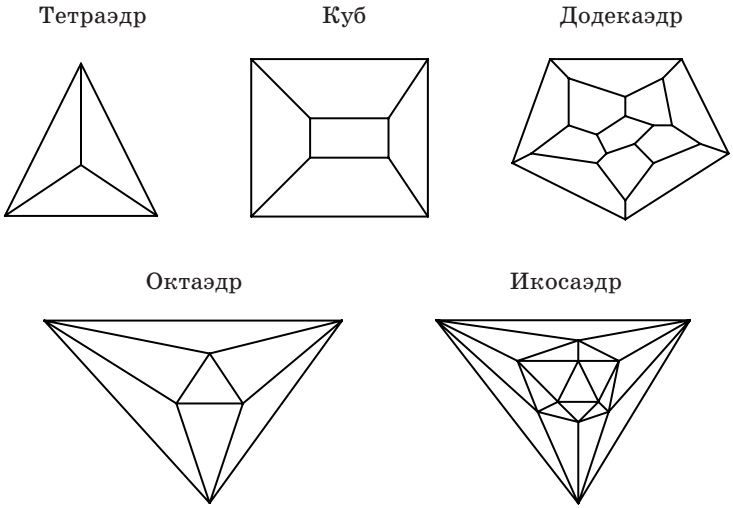


Рис. 5.13. Правильные графы (многогранники)

плоские изображения правильных графов, которым соответствуют правильные многогранники (рис. 5.13).

5.17. Мозаики

Мозаикой называют правильные бесконечные графы. Можно показать, что существует только три вида мозаик (рис. 5.14), других мозаик нет.

Двойственным бесконечным графом к мозаике на основе треугольников является мозаика на основе шестиугольников и наоборот. Двойственным бесконечным графом к мозаике на основе прямоугольников является сама эта мозаика.

Рис 5.14. Мозаики

5.18. «Задача о четырех красках»

Каждой политической или административной карте можно сопоставить некоторый многоугольный граф. Обычно такие карты раскрашиваются так, чтобы граничащие друг с другом два государства были раскрашены в разные цвета. Поскольку форма ребра значения не имеет, то плоские графы, соответствующих фрагментам таких карт, можно представить как графы с прямыми ребрами. Так, например, граф, изображенный на рис. 5.11, мог бы соответствовать некоторому фрагменту политической карты региона.

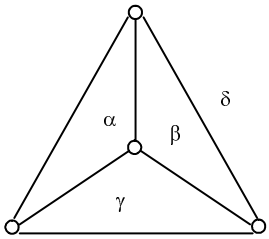


Рис. 5.15. Рисунок, поясняющий необходимость 4-х красок для раскрашивания карт

Существует мнение, что любую политическую карту, так же, как и любой плоский граф, можно раскрасить с использованием 4-х красок, при этом никакие две соседние страны (или никакие две соседние грани) не будут окрашены в один цвет. Эта задача называется «Задача о четырех красках». Достаточно просто показать, что четыре краски необходимы для раскрашивания произвольного графа. Пусть, например, имеется фрагмент графа (рис 5.15).

Пусть некоторая область раскрашена в цвет α, тогда соседняя с ней область должна будет раскрашиваться в другой цвет, например β, третья область, соседняя и с первой и со второй, должна будет раскрашиваться в третий цвет γ. Однако есть еще четвертая область, которая граничит со всеми тремя областями, и ее нужно раскрасить в четвертый цвет δ. Таким образом, четыре краски необходимы для раскрашивания произвольной карты. Но достаточно ли их? Несложно доказывается, что пяти красок достаточно для раскрашивания любой карты, однако не найдено ни одного графа, для раскрашивания которого потребовалось бы использовать пять красок. Похоже, что четыре краски и необходимы, и достаточны для раскрашивания любого графа, а следовательно, и любой политической карты.

5.19. Теорема о направленных графах

Результаты турнира, в котором отсутствуют ничьи, можно представить в виде направленного графа, в котором каждой вершине соответствует команда, а направление стрелки показывает, какая команда выиграла. Пусть, например, в турнире участвуют 7 команд, а результаты игр выглядят так, как это показано на рис. 5.16.

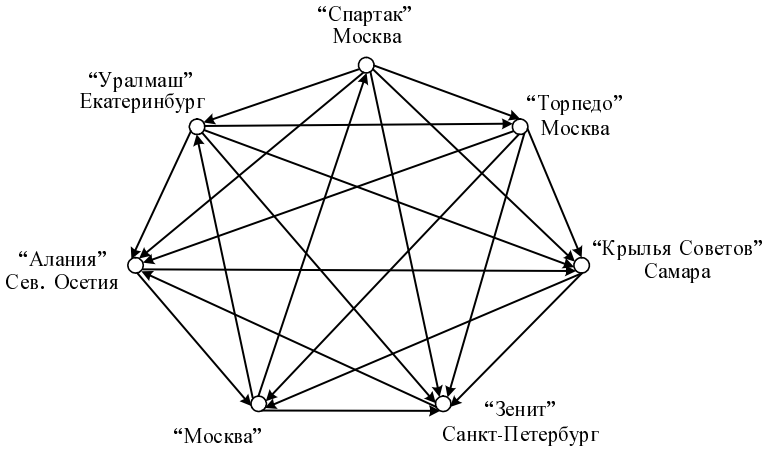


Рис. 5.16. Результаты футбольного турнира

Перепишем результаты в виде табл. 5.19.

После окончания турнира подводятся итоги, в результате любимая команда («Зенит» Санкт-Петербург) оказывается на последнем месте, и ее следует исключить из дальнейших соревнований. Однако находится корреспондент, который утверждает, что итоги подведены неверно, и в доказательство приводит такую цепочку побед: **«Зенит»** > **«Алания»** > **«Москва»** > **«Спартак»** > **«Уралмаш»** > **«Торпедо»** > **»Крылья Советов»**.

Эта цепочка предназначена доказать, что любимая команда – самая лучшая. Из этой цепочки получается, что «Зенит» – самая лучшая команда в этом чемпионате. Интересно, знает ли корреспондент теорему о направленных графах?

Таблица 5.19

Команда	Выиграно	Проиграно	Место
«Спартак» Москва	5	1	I
«Уралмаш» Екатеринбург	4	2	II–III
«Торпедо» Москва	4	2	II–III
«Москва»	3	3	IV
«Алания» Сев. Осетия	2	4	V–VI
«Крылья Советов» Самара	2	4	V–VI
«Зенит» Санкт-Петербург	1	5	VII

Приведем без доказательства эту теорему. Пусть имеется направленный полностью связанный граф G, т. е. все вершины связаны со всеми остальными вершинами графа стрелками. Назовем вершину, в которую только входят стрелки и ни одна не выходит из этой вершины, побитой вершиной. Назовем некоторое множество вершин, в которое только входят стрелки и ни одна не выходит из этого множества (причем между вершинами множества стрелки могут иметь произвольное направление), побитым множеством.

Теорема о направленных графах. *Если граф G не содержит побитых вершин и побитых множеств вершин, то всегда в этом графе существует направленный путь, выходящий из* ***любой*** *вершины графа и проходящий через все остальные вершины.*

Таким образом, если ваша любимая команда не проиграла всех игр, у вас имеются шансы утверждать, что она – самая лучшая команда турнира!

5.20. Задачи для контрольной

1. Задан граф списком ребер:

N ребра	1	2	3	4	5	6	7	8	9	10	11	12
Вершины	*A*	*A*	*B*	*B*	*C*	*C*	*D*	*E*	*E*	*G*	*B*	*G*
Вершины	*B*	*B*	*C*	*C*	*D*	*F*	*E*	*F*	*G*	*F*	*F*	*A*

Начертите его графическое изображение на плоскости, постройте его матрицы инциденции и смежности. Определите тремя способами число его ребер.

2. Теорема о направленных графах. Сформулируйте теорему и приведите пример с графом, имеющим не менее семи вершин.

3. Задан граф списком ребер:

N ребра	1	2	3	4	5	6	7	8	9	10	11	12
Вершины	*E*	*A*	*D*	*B*	*C*	*C*	*D*	*E*	*E*	*G*	*B*	*G*
Вершины	*E*	*B*	*D*	*C*	*D*	*F*	*E*	*F*	*G*	*F*	*F*	*A*

Начертите его графическое изображение на плоскости, постройте его матрицы инциденции и смежности. Определите тремя способами число его ребер.

4. Поясните, что такое цикломатическое число графа. Приведите примеры.

5. Задан граф списком ребер:

N ребра	1	2	3	4	5	6	7	8	9	10	11	12
Вершины	*E*	*A*	*D*	*B*	*C*	*E*	*D*	*E*	*E*	*D*	*B*	*G*
Вершины	*E*	*B*	*D*	*C*	*D*	*D*	*E*	*F*	*G*	*D*	*F*	*A*

Начертите его графическое изображение на плоскости, постройте его матрицы инциденции и смежности. Определите тремя способами число его ребер.

6. «Задача о соединении городов». Приведите пример с 8 городами.

7. «Задача коммивояжер». Сформулируйте и приведите пример с 4 городами.

8. Проектирование плоского графа на сферу. Приведите пример плоского графа с 8 вершинами и найдите число его ребер всеми тремя способами.

9. Постройте турнирную таблицу для 8 игроков.

10. Правильные графы и многогранники. Приведите примеры.

11. «Задача о трех домах и трех колодцах». Почему задача не может быть решена?

12. Теорема Эйлера о числе вершин, ребер и граней плоского графа. Примеры.

13. Теорема Жордана для плоских графов.

14. Графы типа «дерево». Основные соотношения.

15. Теорема Эйлера о циклах в графе.

16. Проецирование плоского графа на сферу. Примеры.

17. Постройте турнирную таблицу для 7 игроков.

18. Правильные графы и многогранники. Приведите примеры.

19. Найдите гамильтонову линию на плоском изображении икосаэдра.

20. Формула Эйлера о числе вершин, ребер и граней плоского графа.

21. Найдите гамильтонову линию на плоском изображении додекаэдра.

22. Теорема о четности числа вершин нечетной степени в графе.

23. Граф задан списком ребер:

1	*A*1	*A*2	8	*A*9	*A*8
2	*A*1	*A*2	9	*A*4	*A*7
3	*A*2	*A*3	10	*A*7	*A*8
4	*A*2	*A*9	11	*A*7	*A*8
5	*A*1	*A*9	12	*A*4	*A*5
6	*A*3	*A*4	13	*A*5	*A*7
7	*A*3	*A*7	14	*A*5	*A*6
			15	*A*6	*A*7

Построить графическое изображение и проверить формулу Эйлера для числа вершин, ребер и граней графа.

24. «Задача о наименованиях и переименованиях».

25. Граф задан матрицей инциденции:

	I	II	III	IV	V
1	1	1			
2		1		1	
3	1		1		
4			1	1	
5		1			1
6	1			1	
7	1				1

Постройте его графическое изображение, список ребер и матрицу смежности.

26. Цикломатическое число графа.

27. Найти минимальную линию, соединяющую города A, B, C, D, T, F. Попарные расстояния между городами заданы треугольной таблицей:

B	11				
C	8	15			
D	6	9	11		
E	9	12	7	5	
F	14	8	10	11	7
	A	*B*	*C*	*D*	*E*

28. Теорема о направленных графах. Сформулируйте теорему и приведите пример с графом, имеющим не менее 7 вершин.

6. ТЕОРИЯ ЧИСЕЛ И НЕКОТОРЫЕ ЕЕ ПРИЛОЖЕНИЯ

Одним из разделов дискретной математики является теория чисел, которая первоначально изучала свойства целых чисел. Целое число является одним из древнейших математических понятий, связанных с подсчетом окружающих предметов. Теория чисел возникла из задач арифметики и первоначально оперировала четырьмя арифметическими действиями над натуральными (целыми, положительными) числами. Основными понятиями этой теории являлись *простые числа*, *составные числа*, *квадратные числа* (числа, равные квадрату некоторого другого числа), *совершенные числа* (число, равное сумме своих делителей). В 6 в. до н. э. в Древней Греции было известно решение уравнения $x^2 + y^2 = z^2$ в целых числах. В 3 в. до н. э. Евклид в «Началах» обосновал алгоритм нахождения наибольшего общего делителя двух произвольных целых чисел и доказал, что количество простых чисел является бесконечным. Эратосфен предложил метод нахождения простых чисел («Решето Эратосфена»). Систематизация проблем теории чисел и методов их решений была выполнена в 3 в. н. э. Диофантом в «Арифметике». В 17 в. н. э. Ферма исследовал решения многих уравнений в целых числах и высказал гипотезу, что уравнение $x^n + y^n = z^n$, $n>2$, x, y, z – целые, не имеет решений (великая теорема Ферма). Ему также принадлежит утверждение о том, что если a и p взаимно простые числа (наибольший общий делитель этих чисел равен 1), где a – целое, p – простое, то $a^p - a$ делится на p нацело (малая теорема Ферма). Эйлер доказал великую теорему Ферма при $n = 3$ и обобщил малую теорему Ферма, введя понятие функции $\varphi(m)$ – количества чисел ряда 1, 2, 3, ..., m взаимно простых с m, ныне называемую функцией Эйлера от целого m, и показал, что любое число a, взаимно простое с m, возведенное в степень $\varphi(m)$, при делении на m дает в остатке 1. Проблема нахождения целых положительных остатков при делении одного целого на другое возникла из задач календарных расчетов в Китае (Суньцзы, Цинь Цзюшао) и в современном виде формулируется как китайская теорема об остатках.

Важным понятием теории чисел являются сравнения, основные свойства которых были доказаны Гауссом. Сравнение является свойством эквивалентности чисел, имеющих одинаковые положительные остатки при делении на некоторое целое число – модуль.

Теория чисел тесно связана с другими разделами дискретной математики: теорией графов, комбинаторикой, теорией конечных автоматов, дискретным спектральным анализом и, конечно, с теорией дискретных групп. Так, множество чисел 0, 1, 2, ..., $p-1$ удовлетворяет аксиомам группы с операцией сложения по модулю p. Если считать p простым числом и исключить из множества 0, то оставшееся множество с операцией умножения по модулю p также образует группу. В этом случае множество чисел 0, 1, 2, ..., $p-1$ с двумя заданными на нем операциями сложения и умножения по модулю p образует числовое поле, которое называется полем Галуа и обозначается $GF(p)$ – сокращение от *Galois Field*. Галуа показал, что для любого простого p и целого h существует конечное поле с числом элементов, равным p^h. Такое поле обозначается $GF(p^h)$. Оно является для заданных p и h единственным (с точностью до изоморфизма). В любом поле $GF(p^h)$ в качестве подполя содержится поле $GF(p)$. Обычно поля Галуа вида $GF(p^h)$ не рассматриваются в теории чисел, однако логическая связь этих полей с числовыми полями $GF(p)$, похожие свойства полей и тесное переплетение в технических приложениях позволили рассмотреть их основные свойства в данном пособии.

6.1. Основные понятия и определения

Приведем некоторые определения и свойства целых чисел, которые потребуются для формулировки двух главных теорем теории чисел.

6.1.1. Делимость целых чисел

Что общего между числами множества 9, 16, 23, 30, 37, 44 кроме того, что они все целые? Казалось бы ничего. Однако, если ввести операцию деления с остатком и интересоваться только целым положительным остатком от деления чисел этого множества на 7, то окажется, что все они будут иметь одинаковый остаток, равный 2. Эти числа эквивалентны по этому свойству. Тогда приведенную последовательность можно продолжить дальше: 51, 58, 65, 72, 79... Это множество чисел является бесконечным и счетным, все числа множества объединяет одно общее свойство: при делении на 7 они дают целый положительный остаток 2. Говорят, что эти числа a сравнимы по модулю 7. Такое свойство множества обозначают $a \equiv 2 \bmod 7$.

Можно рассмотреть другое множество чисел, например 3, 12, 21, 30, 39, 49,..., и убедиться в том, что при делении на число 9 все они дают остаток 3, т. е. общее свойство чисел a этого множества можно записать так: $a \equiv 3 \bmod 9$.

Произвольное целое число a единственным образом может быть представлено в виде $a = mt + r$, где $m > 0$ – целое положительное число (делитель), t – частное, r – остаток ($0 \le r < m$). Так, например, если $a = 17$, $m = 5$, то $17 = 5 \cdot 3 + 2$.

В дальнейшем мы будем использовать операцию деления и интересоваться только остатком, не обращая внимание на частное. Так, например, число 16 при делении на 11 дает остаток 5.

Наименьший положительный остаток от деления некоторого числа a на число m обычно называют наименьшим неотрицательным вычетом a по модулю m. Если m делит a нацело, то остаток $r = 0$. Например, наименьший неотрицательный вычет при делении числа 18 на 6 равен 0.

Пусть имеется два числа a и b. Будем говорить, что они сравнимы по модулю m, если при делении на m они дают одинаковый целый положительный остаток. Например, числа 8 и 15 при делении на 7 имеют одинаковый остаток 1, т. е. они сравнимы по модулю 7. Сравнение чисел будем обозначать так: $a \equiv b \bmod m$.

Сравнению $a \equiv 0 \bmod m$ удовлетворяют все числа a, которые делятся на m нацело или, как говорят, кратные m.

6.1.2. Свойства сравнений

От сравнения $a \equiv b \bmod m$ можно перейти к равенству. Сравнение $a \equiv b \bmod m$ справедливо, если выполняется следующее равенство: $a = b + m \cdot t$, где $\cdot$ – умножение, t – некоторое целое (положительное, отрицательное или 0).

Такая связь между сравнениями и равенствами позволяет распространить понятие сравнения не только на положительные, но и на отрицательные числа. Например, можем записать $12 \equiv 7 \equiv 2 \equiv -3 \equiv -8 \equiv -13 \ldots \bmod 5$.

Из связи между сравнениями и равенствами следуют правила эквивалентных преобразований сравнений.

a) Если $a \equiv b \bmod m$ и $b \equiv c \bmod m$, то $a \equiv c \bmod m$.

b) Если $a \equiv b \bmod m$ и $c \equiv d \bmod m$, то $a+b \equiv c+d \bmod m$. Это правило можно сформулировать и так: сравнения по одинаковому модулю можно почленно складывать.

c) Если $a \equiv b \bmod m$, то $a \equiv b+m \cdot t \bmod m$, так как справедливо сравнение $m \cdot t \equiv 0 \bmod m$, т. е. к любой части сравнения можно прибавить модуль, умноженный на любое целое.

d) Если $a \equiv b \bmod m$ и c – любое целое, взаимно простое с m, то $a \cdot c \equiv b \cdot c \bmod m$, т. е. обе части сравнения можно умножить на любое целое, если оно взаимно простое с модулем m.

e) Если $a \equiv b \bmod m$ и c – любое целое, взаимно простое с m, то $a/c \equiv b/c \bmod m$, т. е. обе части сравнения можно разделить на любое целое, если оно взаимно простое с модулем m.

Последнее свойство позволяет распространить понятия сравнения и на дробные числа. Так, например, если имеем сравнение $1/3 \equiv 16/15 \bmod 11$, то так как (15, 11) = 1, т. е. числа 15 и 11 взаимно просты, то обе части сравнения можно умножить на 15, и получим эквивалентное сравнение: $5 \equiv 16 \bmod 11$.

6.1.3. Решение сравнений

Из приведенных правил эквивалентных преобразований сравнений следуют общие приемы решения сравнений. Пусть требуется решить сравнение $27 - 13 \cdot 5 \equiv 10 \cdot X \bmod 7$ относительно неизвестного X. Можно показать, что если в сравнении имеется арифметическое выражение, то любой член его можно заменить остатком от деления на модуль (в общем случае – на любое сравнимое с ним число). Так как $27 \equiv 6 \bmod 7$, $13 \equiv -1 \bmod 7$ и $10 \equiv 3 \bmod 7$, то исходное сравнение можно представить в виде $6 - (-1) \cdot 5 \equiv 3 \cdot X \bmod 7$.

Далее вычисляем $11 \equiv 3 \cdot X \bmod 7$, $18 \equiv 3 \cdot X \bmod 7$, $6 \equiv X \bmod 7$, откуда одно из решений сравнения – $X = 6$. Общее решение $X = 6 + t \cdot 7$.

Упражнения.

Найти общие решения следующих сравнений:

a) $8 \equiv 3X \bmod 11$;

b) $25 \equiv 15\ X \bmod 17$;

c) $3(24-18)/5 \equiv 7X \bmod 19$;

d) $8^{125} - 6^{29} \equiv 5X \bmod 7$;

e) $$\frac{(75 \cdot 1824 + 33 \cdot 2083)}{37 \cdot 21^6} \equiv 23^3\, X \bmod 19;$$

f) $$\frac{36 \cdot 10^{112} + 81 \cdot 12^{58}}{41 \cdot 9^{10}} \equiv 21^6 X \bmod 11.$$

6.1.4. Наименьшее общее кратное и наибольший общий делитель

Пусть имеется n целых чисел: $a_1, a_2, a_3, \ldots, a_n$. Общим кратным этих чисел называется целое число, которое делится нацело на каждое из этих чисел. Наименьшее из этих общих кратных называется наименьшим общим кратным чисел $a_1, a_2, a_3, \ldots, a_n$ и обозначается НОК ($a_1, a_2, a_3, \ldots, a_n$) или $[a_1, a_2, a_3, \ldots, a_n]$.

Пусть имеется n целых чисел $a_1, a_2, a_3, \ldots, a_n$. Общим делителем этих чисел называется число, которое нацело делит каждое их этих чисел. Сре-

ди делителей имеется наибольшее число, которое называется наибольшим общим делителем – НОД $(a_1, a_2, a_3, ..., a_n)$ или $(a_1, a_2, a_3, ..., a_n)$.

6.1.5. Простые числа. Разложение на простые сомножители. Каноническая форма числа

Число, которое не имеет никаких делителей, кроме 1 и самого себя, называется простым числом. Примеры простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Любое число N может быть представлено в виде произведения степеней простых чисел (каноническое представление числа). Такое представление единственно (с точностью до перестановки сомножителей). Так, число $600 = 2^3 3^1 5^2$.

Для представления числа N в канонической форме можно использовать следующий алгоритм. Число N делим на наименьшее простое число 2 до тех пор, пока оно делится нацело, затем на 3, на 5 и т. д.

Например, $N = 10500$. $10500 : 2 = 5250$; $5250 : 2 = 2625$. Это число больше не делится на 2 нацело. Делим его на 3. $2625 : 3 = 875$. Это число на 3 нацело не делится. Делим его на 5. $875 : 5 = 175$. Еще раз делим на 5. $175 : 5 = 35$. Еще раз делим на 5. $35 : 5 = 7$. Число 7 – простое число, поэтому окончательно имеем в канонической форме: $10\,500 = 2^2 3^1 5^3 7^1$.

6.1.6. Определение НОК И НОД чисел

Для произвольного целого числа a и произвольного целого положительного числа b существуют такие числа t и r, что $a = bt + r$, где $0 \le r < b$. Причем такое представление единственное.

Можно показать, что если $b|a$ (b делит a нацело), то $(a, b) = b$, и если $a = bt + r$, то $(a, b) = (b, r)$.

Для нахождения наибольшего общего делителя двух чисел a и b известен алгоритм Евклида: пусть $a \ge b$. Рассмотрим следующую последовательность равенств:

$$a = bt_1 + r_2,\ 0 < r_2 < b;$$
$$b = r_2 t_2 + r_3,\ 0 < r_3 < r_2;$$
$$r_2 = r_3 t_3 + r_4,\ 0 < r_4 < r_3 \ ...$$
$$r_{n-1} = r_n t_n + r_{n+1},\ 0 = r_{n+1}.$$

Поскольку $a \ge b > r_2 > r_3 > ... \ge 0$, то алгоритм имеет конечное число шагов. Согласно вышеприведенным свойствам, $(a, b) = (b, r_2) = (r_2, r_3) = ... = r_n$. Таким образом, наибольший общий делитель чисел a и b равен последнему ненулевому остатку в последовательности равенств, т. е. r_n. А наименьшее общее кратное a и b равно $[a, b] = ab/(a, b)$.

Упражнения.

Используя алгоритм Евклида, найти НОК и НОД чисел:

а) 575 и 155;

β) 840 и 188650;

с) 4851 и 29106;

d) 975 и 616.

Если два числа N_1 и N_2 представлены в канонической форме соответственно: $N_1 = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, $N_2 = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}$, то

$$\text{НОК}\left(N_1, N_2\right) = p_1^{\min(n_1, m_1)} p_2^{\min(n_2, m_2)} p_s^{\min(n_s, m_s)};$$

$$\text{НОД}\ \left(N_1, N_2\right) = p_1^{\min(n_1, m_1)} p_2^{\min(n_2, m_2)} p_s^{\min(n_s, m_s)}.$$

Если в каноническом представлении одного из чисел отсутствует какой-либо простой сомножитель, его можно ввести в нулевой степени. Например, для чисел $N_1 = 2^3 5^2 7^1$ и $N_2 = 3^1 5^1 11^2$, прежде чем находить НОК и НОД, требуется их привести к одинаковой форме, т. е. сделать так, чтобы в каноническом представлении обоих чисел присутствовали бы одинаковые простые числа в соответствующих степенях, а именно: $N_1 = 2^3 3^0 5^2 7^1 11^0$; $N_2 = 2^0 3^1 5^1 7^0 11^2$. Тогда НОК ($N_1$, N_2) = $= 2^3 3^1 5^2 7^1 11^2 = 508200$, НОД ($N_1$, N_2) = $2^0 3^0 5^1 7^0 11^0 = 5$.

Упражнения.

Найти НОК и НОД для пар чисел:

а) $N_1 = 440$; $N_2 = 6050$;

β) $N_1 = 234$; $N_2 = 4125$;

с) $N_1 = 66550$; $N_2 = 40131$;

d) $N_1 = 388$; $N_2 = 1647$.

Приведенный алгоритм легко обобщается на произвольное количество чисел, для которых требуется определить НОК и НОД.

Упражнения.

Найти НОК и НОД для следующих наборов чисел:

а) $N_1 = 60$; $N_2 = 350$; $N_3 = 495$;

β) $N_1 = 265$; $N_2 = 104$; $N_3 = 93$;

с) $N_1 = 2100$; $N_2 = 630$; $N_3 = 5880$; $N_4 = 9450$;

d) $N_1 = 700$; $N_2 = 495$; $N_3 = 104$;

е) $N_1 = 103$; $N_2 = 260$; $N_3 = 121$.

6.1.7. Функция Эйлера для натурального числа φ(m)

Функция Эйлера $\varphi(m)$ определяется для всех целых чисел m как количество чисел ряда 1, 2, 3, ..., m взаимно простых с m. Так, $\varphi(1) = 1$ (по определению), $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$ и т. д. Легко показать, что для $m = p$ (простых чисел) $\varphi(p) = p-1$. Для $m = p^n$ функция

Эйлера $\varphi(p^n) = p^{n-1}(p-1)$. Для произвольного числа m, представленного в канонической форме $m = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, функция Эйлера определяется следующим образом: $\varphi(m) = m(1-1/p_1)(1-1/p_2)\dots(1-1/p_s)$.

Например: $\varphi(11) = 10$; $\varphi(9) = 6$; $\varphi(18) = 6$.

Упражнения.

Вычислить функцию Эйлера $\varphi(m)$ для чисел m = 7, 12, 15, 17, 23, 24, 25, 28, 37, 54, 64.

6.1.8. Сравнимость чисел и классы вычетов

Выпишем все числа от 1 до 8 и вычеркнем все числа не взаимно простые с 8. Количество оставшихся чисел равно $\varphi(m = 8) = 4$, а сами эти числа (1, 3, 5, 7). Множество этих чисел обладает свойством замкнутости относительно операции умножения по модулю $m = 8$. Действительно, перемножая любые пары чисел из множества (1, 3, 5, 7) и находя наименьший положительный остаток по модулю $m = 8$, будем получать всегда одно из этих же чисел. Каждое из этих чисел порождает бесконечный счетный класс чисел: $1+8\cdot t$; $3+8\cdot t$; $5+8\cdot t$; $7+8\cdot t$, где t – любое целое.

Более того, множество классов с порождающими элементами в виде этих чисел обладает свойством замкнутости, а именно: при любых целых t произведение представителей классов ($1+8\cdot t$; $3+8\cdot t$; $5+8\cdot t$; $7+8\cdot t$) дает в результате представителя одного из этих же классов.

Можно показать, что классы вычетов, получаемые в соответствии с функцией Эйлера, всегда образуют абелеву группу по умножению. А это, в частности, означает, что для любого представителя из этих классов можно найти обратный элемент из представителей этих же классов.

Упражнения.

Постройте абелевы группы классов, порождаемые числами 10, 12, 15, 18, 21, 24, 25, 27, 28.

6.1.9. Теоремы Ферма и Эйлера

Теорема Ферма.

Существует мнение, что Ферма не публиковал свои научные труды, а формулировал свои знаменитые теоремы либо в письмах к знакомым математикам, либо на полях рукописей. Так, на полях одной из рукописей Ферма написал, что если p – простое число и $(a, p) = 1$, то $a^{p-1} \equiv 1 \bmod p$.

Пусть $p = 23$, $a = 18$. Очевидно, что (23, 18) = 1, следовательно, $18^{22} \equiv 1 \bmod 23$. Проверить этот результат несложно. Для этого заметим, что $18 \equiv -5 \bmod 23$, поэтому можно написать эквивалентное сравнение: $(-5)^{22} \equiv 1 \bmod 23$ или $5^{22} \equiv 1 \bmod 23$. Последнее сравнение можно представить в виде $(5^2)^{11} \equiv 1 \bmod 23$, и так как $25 \equiv 2 \bmod 23$, то

$2^{11} \equiv 1 \bmod 23$. Полученное сравнение элементарно проверяется: $2048 \equiv 1 \bmod 23$.

Теорема Эйлера.

Если $m > 1$ и $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \bmod m$. Эта теорема обобщает теорему Ферма, так как при $m = p$, $\varphi(m = p) = p - 1$.

Пусть $m = 18$, $a = 5$. Очевидно, что $(5, 18) = 1$.

Функция Эйлера $\varphi(m = 18) = 6$. Поэтому $5^6 \equiv 1 \bmod 18$. Это сравнение проверяется достаточно просто: $5^2 \equiv 7 \bmod 18$, следовательно, $((5^2))^3 \equiv 7^3 = 343 \equiv 1 \bmod 18$.

Упражнения.

На основании теорем Ферма и Эйлера доказать справедливость сравнений:

a) $2^{36} \equiv 3^{36} \equiv \ldots \equiv 36^{36} \equiv 1 \bmod 37$;

b) $2^{100} \equiv 3^{100} \equiv \ldots \equiv 100^{100} \equiv 1 \bmod 101$;

c) $2^8 \equiv 4^8 \equiv 7^8 \equiv 8^8 \equiv 11^8 \equiv 13^8 \equiv 14^8 \equiv 1 \bmod 15$.

6.1.10. Показатели чисел по модулю и примитивные корни

Пусть $(a, m) = 1$. Рассмотрим бесконечную последовательность степеней числа a: $a^0 = 1$, a^1, a^2, a^3, ... В соответствии с теоремой Эйлера существует целое положительное число s, такое, что

$$a^s \equiv 1 \bmod m. \qquad (6.1)$$

В самой теореме $s = \varphi(m)$. Могут существовать и другие целые положительные числа s, удовлетворяющие этому сравнению. Наименьшее из них обозначается $\boldsymbol{e}$ и называется показателем числа a по модулю m. Иногда $\boldsymbol{e}$ называют порядком числа a по модулю m.

Набор степеней числа a вида a^0, a^1, a^2, a^3, ..., a^{e-1} попарно несравнимы между собой по модулю m. Докажем это. Пусть, например, при некоторых n_1 и n_2 выполняется сравнение $a^{n_1} \equiv a^{n_2} \bmod m$, где для определенности $n_1 < n_2 < \boldsymbol{e}$. Умножим обе части сравнения на a^{e-n_2}, тогда получим $a^{(e+n_1-n_2)} \equiv 1 \bmod m$. Но поскольку $n_1 < n_2$, то в левой части сравнения степень числа a меньше $\boldsymbol{e}$, что противоречит тому, что $\boldsymbol{e}$ – наименьшее число, удовлетворяющее сравнению (6.1). Если найдется некоторое k, такое, что $a^k \equiv 1 \bmod m$, то $\boldsymbol{e}$ является делителем k. Очевидно, что всегда e является делителем $\varphi(m)$.

Пример.

Возьмем $m = 45$, $a = 2$, $(45, 2) = 1$. Функция Эйлера $\varphi(45) = 24$, следовательно, $2^{24} \equiv 1 \bmod 45$. Число 24 представляется в канонической форме в виде $24 = 2^3 3$, т. е. имеет 8 разных делителей: 1, 2, 3, 4, 6, 8, 12, 24. Проверка показывает, что наименьшее число $e = 12$, так как $2^{12} \equiv 1 \bmod 45$.

Если показатель ***e*** числа a по модулю m равен $\varphi(m)$, то a называют примитивным элементом по модулю m.

Пример. По каким модулям число $a = 2$ является примитивным элементом? $m = \mathbf{3}, \mathbf{5}, 7, \mathbf{9}, \mathbf{11}, 15, 17, \mathbf{19}$.

6.1.11. Конечные поля (поля Галуа)

В разд. 3 приведены определения математических моделей с одним классом объектов – групп, колец и полей (в частности – полей Галуа).

Можно показать, что числовое конечное поле (поле с конечным числом элементов) существует только при операциях сложения и умножения по модулю p, где p – простое число. Такие поля называются числовыми конечными полями Галуа и обозначаются $GF(p)$ или $F(p)$.

Примеры.

1. Построить конечные поля $F(2)$, $F(3)$, $F(7)$. Для решения этих примеров указать все элементы множества U, найти нейтральные и обратные элементы для групп по сложению и умножению с соответствующим модулем.

2. Показать, что не существует полей $F(6)$, $F(12)$, $F(15)$.

Поля Галуа можно построить в совершенно другой форме, а именно как поля многочленов по модулю некоторого неприводимого многочлена над числовым полем $F(p)$. В этом случае порядок поля (число его элементов) равен p^h, где p – простое, h – целое.

Пусть $F(p)$ – числовое поле Галуа порядка p. Рассмотрим множество многочленов вида

$$f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_kX^k,$$

где $a_i \in F(p)$, $i = 0, 1, 2, 3\ldots, k$, т. е. коэффициенты принимают значения из $F(p)$, операции сложения и умножения чисел выполняются по $\bmod p$. Если $a_k \neq 0$, то многочлен $f(X)$ имеет степень k. Множество всех многочленов, имеющих степень k и меньше, будем обозначать $F^{(k)}[X]$.

Введем операции сложения и умножения многочленов над полем $F(p)$ следующим образом. Пусть

$$f(X) = \sum f_iX^i \text{ и } g(X) = \sum g_iX^i.$$

Тогда

$$f(X) + g(X) = \sum_i (f_i + g_i)X^i;\ f(X)\cdot g(X) = \sum_i \left(\sum_{j=0} f_i g_{i-j} \right) X^i.$$

Например: пусть

$$f(X) = f_0 + f_1 X;\ g(X) = g_0 + g_1 X + g_2 X^2.$$

Тогда

$$f(X) + g(X) = (f_0 + g_0) + (f_1 + g_1)X + g_2 X^2;$$
$$f(X) \cdot g(X) = (f_0 g_0) + (f_0 g_1 + f_1 g_0)X + (f_1 g_1 + f_0 g_2)X^2 + f_1 g_2 X^3.$$

Отсюда видно, что при сложении степень результирующего многочлена равна максимальной степени слагаемых, а при умножении – сумме степеней перемножаемых многочленов.

Упражнения.

Сложить и перемножить следующие пары многочленов:

a) $f(X) = f_0 + f_1 X + f_2 X^2;\ g(X) = g_0 + g_1 X + g_3 X^3;$

b) $f(X) = f_1 X + f_2 X^2 + f_5 X^5;\ g(X) = g_0 + g_1 X^1 + g_4 X^4;$

c) $f(X) = f_1 X + f_2 X^2 + X^5;\ g(X) = g_0 + g_1 X^3 + g_2 X^4.$

А теперь сделайте то же самое, если указано **конечное** числовое поле (модуль):

d) $f(X) = 2X + 3X^2 + X^5;\ g(X) = 4 + 2X^3 + X^4,\ p = 7;$

e) $f(X) = 3X + 2X^2 + 2X^5;\ g(X) = 2 + 4X^1 + 3X^4,\ p = 5.$

Если рассматривать многочлены всех возможных степеней $F(X)$, то с такими операциями сложения и умножения множество многочленов образует кольцо.

Для любых двух многочленов $f(X)$ и $g(X)$ существуют, и притом единственные, многочлены $a(X)$ и $r(X)$, такие, что $f(X) = a(X)g(X) + r(X)$, где степень $g >$ степени r. Переходя к сравнениям многочленов, получаем

$$f(X) \equiv r(X) \bmod (g(X)). \qquad (6.2)$$

Деление многочленов производится так же, как и деление целых чисел. Следует только учитывать, что все операции выполняются в поле $F(p)$. Например, разделим многочлен $g(X) = 1 + X + X^2$ на $f(X) = 1 + X$ в поле $F(2)$:

$(1 + X + X^2)$	$(1 + X)$
$X + X^2$	X
1	

В результате получим $(1 + X + X^2) : (1 + X) = X$, при этом в остатке будет 1. Для деления удобнее записывать многочлены в обратном порядке, начиная со старшей степени. При вычислении в поле $F(2)$ операция сложения имеет специальное обозначение «$\oplus$» и называется «сложение по модулю 2».

Упражнения.

Найти остатки от деления многочленов:

а) $X^5 \oplus X^2 \oplus X$ на $X^3 \oplus X^2 \oplus X \oplus 1$ в поле $F(2)$ **(0)**

b) $2X^4 + X^2 + 2$ на $X^3 + 2X^2 + 2X + 1$ в поле $F(3)$ **($2X^2$)**

Если в (6.2) остаток $r(X) = 0$, то говорят, что $g(X)$ делит $f(X)$. Если в $F(X)$ нет ни одного многочлена степени, большей 0, который бы делил $f(X)$ без остатка, за исключением скалярных кратных $f(X)$, т. е. многочленов вида $bf(X)$, где $b \in F(p)$, то многочлен $f(X)$ называется *неприводимым*.

Найдем неприводимые многочлены некоторых малых степеней.

Имеется два многочлена первой степени: $X \oplus 1$ и X. По определению, они оба считаются неприводимыми.

Многочлен второй степени вида $X^2 \oplus aX \oplus b$ будет неприводимым над полем $F(2)$, если он не будет делиться ни на какой неприводимый многочлен первой степени, т. е. ни на $X \oplus 1$, ни на X. А это означает, что он не должен иметь корней в поле $F(2)$. Таким образом: $F(0) = b \neq 0$, $F(1) = 1 \oplus a \oplus b \neq 0$. Откуда получаем, что $a = 1$, $b = 1$, а сам неприводимый многочлен 2-го порядка имеет вид $X^2 \oplus X \oplus 1$.

Многочлен третьей степени имеет общий вид $X^3 \oplus aX^2 \oplus bX \oplus c$. Он будет неприводимым в поле $F(2)$, если не будет делиться ни на один из неприводимых многочленов первой степени (проверять делимость на многочлен второй степени не требуется). Таким образом, должны выполняться условия: $F(0) = c = 1$, $F(1) = 1 \oplus a \oplus b \oplus 1 = 1$. Следовательно, либо a, либо b должны равняться 1, но не оба вместе, поэтому существуют два неприводимых многочлена третьей степени: $X^3 \oplus X^2 \oplus 1$ и $X^3 \oplus X \oplus 1$.

Приведем табл. 6.1 всех неприводимых многочленов над полем $F(2)$, степень которых не превышает 4.

Возьмем один из неприводимых многочленов степени 2 над числовым полем $F(2)$, например $X^2 \oplus X \oplus 1$. При делении на этот многочлен все многочлены будут давать остатки (вычеты по модулю этого неприводимого многочлена). Приведем все виды остатков: $\{(0), (1), (X), (X \oplus 1)\}$. Каждый из этих остатков образует класс вычетов по модулю неприводимого многочлена, а их совокупность с операциями сложения и умножения по модулю неприводимого многочлена образует поле. Порядок этого поля (число элементов) в общем случае может быть равен p^h, где p – про-

Таблица 6.1

Максимальная степень многочлена	Неприводимые многочлены в поле $F(2)$
1	$X \oplus 1$; X
2	$X^2 \oplus X \oplus 1$
3	$X^3 \oplus X^2 \oplus 1$; $X^3 \oplus X \oplus 1$
4	$X^4 \oplus X^3 \oplus X^2 \oplus X \oplus 1$; $X^4 \oplus X \oplus 1$; $X^4 \oplus X^3 \oplus 1$

стое, h – целое. В приведенном примере $p = 2$, $h = 2$ и порядок поля равен 4.

Упражнение.

Постройте поля Галуа $F(2^3)$, $F(2^4)$ для пяти полиномов (многочленов), взятых из табл. 6.1.

Элемент поля α, такой, что $F(\alpha) = 0$, называется корнем многочлена $f(X)$. В этом случае говорят, что уравнение $f(X)$ имеет корень в поле $F(p)$.

Упражнения.

a) Найдите корни многочлена $X^2 + X + 1$ в полях $F(2)$, $F(3)$, $F(5)$, $F(7)$.

Покажем, как это сделать для поля $F(5)$. В уравнение

$$X^2 + X + 1 = 0 \qquad (6.3)$$

будем последовательно подставлять значения элементов поля: 0, 1, 2, 3, 4. В результате получим:

$$0^2 + 0 + 1 \equiv 1 \bmod 5;$$
$$1^2 + 1 + 1 \equiv 3 \bmod 5;$$
$$2^2 + 2 + 1 \equiv 2 \bmod 5;$$
$$3^2 + 3 + 1 \equiv 3 \bmod 5;$$
$$4^2 + 4 + 1 \equiv 1 \bmod 5,$$

т. е. этот многочлен не имеет корней в поле $F(5)$. Однако он имеет корни в поле $F(7)$. Действительно, при $X = 2$ и $X^2 = 4$ левая часть уравнения (6.3) обращается в 0.

b) Найдите корни многочлена X^4+X^3+1 в тех же полях, что и в примере 1.

Конечное поле $F(p^h)$ содержит p^h элементов. Основное поле $F(p)$, которое является подполем поля $F(p^h)$, содержит p элементов (0, 1, 2, 3,..., $p-1$) и 2 операции: $\oplus \bmod p$ и $\otimes \bmod p$.

Элемент α называется алгебраическим степени h над полем $F(p)$, если и только если α удовлетворяет в $F(p)$ уравнению $P(x) = 0$, где $P(x)$ – многочлен степени h, но не удовлетворяет никакому уравнению с многочленом меньшей степени. Это влечет неприводимость многочлена $P(x)$. Все p^h элементов поля $F(p^h)$ могут быть представлены в виде $\sum c_j \alpha^i$, где $0 \le c_j \le p-1$; $0 \le \alpha^i \le h-1$. При вычислениях степень α^s, где $s \ge h$, заменяется на меньшую в соответствии с уравнением $P(\alpha) = 0$.

Пусть, например, $p = 3$, $h = 2$ и α удовлетворяет уравнению $x^2 - x - 1 = 0$. Элементы поля $F(3^2)$ можно выразить как 0, 1, 2, α, $\alpha + 1$, $\alpha + 2$, 2α, $2\alpha + 1$, $2\alpha + 2$.

В вычислениях понижение степеней производится с использованием равенства $\alpha^2 = \alpha + 1$. Например: $(2\alpha + 1)(\alpha + 2) = 2\alpha^2 + \alpha + 4\alpha + 2 = 2(\alpha + 1) + 5\alpha + 2 = 7\alpha + 4 = \alpha + 1$.

Элемент $\beta \neq 0$ поля $F(p^h)$ называется образующей $F^*(p^h)$ мультипликативной группы ненулевых элементов поля $F(p^h)$, если степени β^i, $i = 1, 2, 3, \ldots, p^h - 1$ пробегают все ненулевые элементы поля $F(p^h)$. Образующая может рассматриваться как основание log. Такие логарифмы называются дискретными логарифмами. Рассмотрим, например, все 8 степеней (кроме нулевой) корня α в приведенном выше примере и запишем результат в виде таблицы:

i	1	2	3	4	5	6	7	8
α^i	α	$\alpha + 1$	$2\alpha + 1$	2	2α	$2\alpha + 2$	$\alpha + 2$	1

Из таблицы видно, что α является образующей. Эта таблица может быть представлена как таблица дискретных логарифмов. Для этого в верхней строке запишем упорядоченные элементы поля, а в нижней – значения степеней образующего элемента, при которых получаем данный элемент поля:

y	1	2	α	$\alpha + 1$	$\alpha + 2$	2α	$2\alpha + 1$	$2\alpha + 2$
$\log_\alpha y$	8	4	1	2	7	5	3	6

Считается, что вычисление дискретных логарифмов является трудной задачей, как и задача факторизации (разложения на множители), что является существенным в криптосистемах с открытым распределением ключей. Таблица логарифмов может использоваться для выполнения умножения и деления элементов поля. Заметим, что операции выполняются по модулю $p^h - 1$, в данном примере – по модулю $3^2 - 1 = 8$.

Для примера: $\log((\alpha + 2)(2\alpha + 1)) = \log(\alpha + 2) + \log(2\alpha + 1) = 7 + 3 = 10 \equiv 2 \bmod 8$. Что соответствует элементу $\alpha + 1$. $\log((\alpha + 1)/(2\alpha + 2)) = 2 - 6 = -4 \equiv 4 \bmod 8$, что соответствует элементу 2.

Можно проверить, что кроме элемента α образующими β также являются элементы $2\alpha + 1$, $\alpha + 2$ и 2α. Если $s = p^h - 1$ есть наименьшая положительная степень, удовлетворяющая уравнению $\beta^s = 1$, то β является образующей. Поэтому число образующих элементов поля равно $\varphi(p^h - 1)$, где φ – функция Эйлера. Для нашего примера $\varphi(8) = 4$.

Упражнения.

Найдите количество образующих элементов для полей Галуа: $F(3^4)$, $F(5^2)$, $F(7^2)$, $F(11^5)$, $F(13^4)$.

6.1.12. Квадратичные вычеты. Символ Лежандра. Символ Якоби

Рассмотрим поле Галуа $F(p^h)$ при $p > 2$ и h – целом. Исключим из элементов поля нулевой элемент, а оставшееся множество обозначим $F^*(p^h)$. Если некоторый элемент $a \in F^*(p^h)$ есть квадрат некоторого элемента $x \in F^*(p^h)$, то a называют *квадратичным вычетом*, если же такого элемента x не найдется в $F^*(p^h)$, то a называют *квадратичным невычетом*.

Пример. Рассмотрим поле $F(3^2)$. Все элементы поля можно представить в виде 0, 1, 2, α, $\alpha + 1$, $\alpha + 2$, 2α, $2\alpha + 1$, $2\alpha + 2$, где α – корень некоторого неприводимого полинома степени 2 над полем $F(3)$. Возьмем в качестве такого полинома $P(X) = X^2 - X - 1$. Тогда $P(\alpha) = \alpha^2 - \alpha - 1 = 0$. При выполнении вычислений будем производить замену: $\alpha^2 = \alpha + 1$. $F^*(3^2)$ будет содержать все те же элементы, кроме элемента 0, а именно: 1, 2, α, $\alpha + 1$, $\alpha + 2$, 2α, $2\alpha + 1$, $2\alpha + 2$. Будем последовательно возводить в квадрат все элементы поля (кроме нулевого) и выявлять квадратичные вычеты:

$$1^2 = \mathbf{1};\ 2^2 = 1;\ \alpha^2 = \boldsymbol{\alpha + 1};\ (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = \alpha + 1 + 2\alpha + 1 = \mathbf{2};$$
$$(\alpha + 2)^2 = \alpha^2 + 4\alpha + 4 = (\alpha + 1) + 4\alpha + 4 = \boldsymbol{2\alpha + 2};\ (2\alpha)^2 = 4\alpha^2 = (\alpha + 1);$$
$$(2\alpha + 1)^2 = 4\alpha^2 + 4\alpha + 1 = \alpha + 1 + 4\alpha + 1 = 2\alpha + 2;$$
$$(2\alpha + 2)^2 = 4\alpha^2 + 8\alpha + 4 = \alpha^2 + 2\alpha + 1 = 2.$$

Таким образом элементы 1, 2, $\alpha = 1$ и $2\alpha + 2$ являются квадратичными вычетами, а остальные элементы α, $\alpha + 2$, 2α и $2\alpha + 1$ – квадратичными невычетами.

Упражнения.

Найдите квадратичные вычеты и квадратичные невычеты в полях Галуа: $F(3^3)$, $F(5^2)$.

Пусть теперь $h = 1$. Рассмотрим поле $F(p)$ с элементами 0, 1, 2,..., $p-1$. Если исключить элемент 0, то для остальных элементов поля можно также определить, являются они квадратичными вычетами или невычетами. Ясно, что элемент a, $1 \le a \le p-1$ будет квадратичным вычетом по модулю p тогда и только тогда, когда выполняется сравнение $x^2 \equiv a \bmod p$, где x также является элементом поля $F(p)$.

Пример. Пусть $p = 7$. Тогда $1^2 \equiv \mathbf{1} \bmod 7$; $2^2 \equiv \mathbf{4} \bmod 7$; $3^2 \equiv \mathbf{2} \bmod 7$; $4^2 \equiv 2 \bmod 7$; $5^2 \equiv 4 \bmod 7$; $6^2 \equiv 1 \bmod 7$. Таким образом, квадратичными вычетами являются числа 1, 2, 4, а квадратичными невычетами – числа 3, 5, 6.

Если a – квадратичный вычет по модулю p, полученный возведением в квадрат числа x, то это же число будет получено возведением в квадрат числа $-x \equiv p - x \bmod p$. Поэтому все квадратичные вычеты по

модулю p можно найти возведением в квадрат чисел 1, 2, 3,..., $(p-1)/2$. Таким образом, для любого p имеется ровно $(p-1)/2$ квадратичных вычетов и столько же квадратичных невычетов.

Упражнения.

Найдите квадратичные вычеты и квадратичные невычеты по простым модулям $p = 11, 13, 17, 19, 23$.

Символ Лежандра для целого a и простого $p > 2$ определяется следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{ если } p \text{ делит } a; \\ 1, \text{ если } a - \text{квадратичный вычет по модулю } p; \\ -1, \text{ если } a - \text{квадратичный невычет по модулю } p. \end{cases}$$

Понятно, что a можно заменить любым целым числом, сравнимым с a по модулю p, при этом символ Лежандра не изменится. Вычисление символа Лежандра удобно производить по формуле

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p.$$

Действительно:

$$\left(\frac{8}{5}\right) = 8^2 \equiv -1 \bmod 5.$$

Упражнения.

Вычислите следующие символы Лежандра:

$$\left(\frac{7}{5}\right), \left(\frac{3}{7}\right), \left(\frac{11}{7}\right), \left(\frac{35}{11}\right), \left(\frac{169}{13}\right), \left(\frac{523}{13}\right).$$

Символ Якоби является обобщением символа Лежандра на случай произвольного нечетного модуля $n > 2$. Пусть число n представлено в канонической форме: $n = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$. Тогда символ Якоби определяется как произведение символов Лежандра:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{s_1} \left(\frac{a}{p_2}\right)^{s_2} \dots \left(\frac{a}{p_k}\right)^{s_k}.$$

Например, пусть $n = 363\,825 = 3^3 5^2 7^2 11^1$. Найдем символ Якоби для числа $a = 863$. Сначала найдем наименьший положительный вычет числа 863 по модулям $p = 3$, 5, 7 и 11:

$$863 \equiv 2 \bmod 3;\ 863 \equiv 3 \bmod 5;\ 863 \equiv 2 \bmod 7;\ 863 \equiv 5 \bmod 11.$$

Тогда символ Якоби можно вычислить следующим образом:

$$\left(\frac{863}{363825}\right)=\left(\frac{863}{3}\right)^3\left(\frac{863}{5}\right)^2\left(\frac{863}{7}\right)^2\left(\frac{863}{11}\right)^1=\left(\frac{2}{3}\right)^3\left(\frac{3}{5}\right)^2\left(\frac{2}{7}\right)^2\left(\frac{5}{11}\right)^1=$$

$$=(2^1\equiv -1 \bmod 3)^3\,(3^2\equiv -1 \bmod 5)^2\,(2^3\equiv 1 \bmod 7)^2\,(5^5\equiv 1 \bmod 11)^1=$$

$$=(-1)(1)(1)(1)=-1,$$

т. е. число 863 является квадратичным невычетом по модулю 363825.

Для произведения чисел выполняется свойство мультипликативности:

$$\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

Тогда

$$\left(\frac{abb}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)\left(\frac{b}{n}\right)=\left(\frac{a}{n}\right).$$

Для некоторых значений a символ Якоби вычисляется без перевода n в каноническую форму следующим образом:

$$\left(\frac{1}{n}\right)=1;\ \left(\frac{-1}{n}\right)=(-1)^{(n-1)/2};\ \left(\frac{2}{n}\right)=(-1)^{(n^2-1)/8}.$$

При вычислении символа Якоби основное сведение выполняется на основе закона взаимности:

$$\left(\frac{m}{n}\right)=(-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right),$$

где m и n – нечетные числа, большие двух.

Если не выполняется сравнение $m \equiv n \equiv 3 \bmod 4$, то

$$\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right).$$

Если же это сравнение выполняется, то

$$\left(\frac{m}{n}\right)=-\left(\frac{n}{m}\right).$$

Пример. Определить, является ли число $a = 369$ квадратичным вычетом или квадратичным невычетом по модулю 247?

$369 \equiv 1 \bmod 4$, поэтому можно вычислить:

$$\left(\frac{369}{247}\right)=\left(\frac{122}{247}\right)=\left(\frac{247}{122}\right)=\left(\frac{3}{122}\right)=\left(\frac{122}{3}\right)=\left(\frac{122}{3}\right)=-1,$$

т. е. 369 является квадратичным невычетом по модулю 247.

Упражнения.

Определить символы Якоби в следующих случаях:

a) $\left(\frac{1815}{1683}\right)$; b) $\left(\frac{361}{5515}\right)$; c) $\left(\frac{2197}{625}\right)$.

Для криптографических систем представляет интерес случай, когда n является произведением двух простых чисел p и q, т. е. $n = pq$. Требуется определить, является ли некоторое число a квадратичным вычетом или квадратичным невычетом по модулю n, т. е. существует ли такое x, что выполняется сравнение $x^2 \equiv a \bmod n$?

Некоторое число a будет квадратичным вычетом по модулю $n = pq$, если и только если оно будет квадратичным вычетом как по модулю p, так и по модулю q. Если рассмотреть множество чисел 1, 2, 3,..., $n-1$ и исключить из него все числа, кратные p и (или) q, то в точности половина из оставшихся чисел будет удовлетворять условию $\left(\frac{a}{n}\right)=1$, а вторая половина будет удовлетворять условию $\left(\frac{a}{n}\right)=-1$. Более того, из чисел a, удовлетворяющих условию $\left(\frac{a}{n}\right)=1$, половина будет квадратичными вычетами, а именно такие числа a, для которых $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=1$. Другая половина, для которых $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$, будет квадратичными невычетами.

Пример. Пусть $p = 3$, $q = 5$, тогда $n = 15$. Квадратичными вычетами по модулю 15 будут числа $a = 1$ и 4. Квадратичными невычетами будут числа $a = 2$ и 8.

Если известно, что некоторое a является квадратичным вычетом по модулю $n = pq$, но простые числа p и q неизвестны, то решение сравнения (нахождение x из сравнения) $x^2 \equiv a \bmod n$ является важной, но очень сложной задачей в криптографии с открытым ключом.

6.2. Использование теории чисел в криптографии и коррекции ошибок при передаче сообщений

Еще 50 лет назад теория чисел считалась одним из «чистых» разделов математики, «не запятнавших» себя какими-либо техническими приложениями. Этот раздел математики изучался только на механико-математических факультетах университетов, в технических вузах

не вводились даже элементарные понятия этой красивой и очень перспективной теории. В настоящее время разделы теории чисел используются в самых разнообразных технических приложениях. Одним из первых приложений этой теории явилось ее использование при построении линейных кодов для коррекции ошибок в каналах связи и кодов для контроля арифметических операций. Следующим шагом явилась идея Э. С. Москалева об использовании полей Галуа для сжатия информации при спектральных преобразованиях [1]. И, конечно, главным применением результатов теории чисел явилось ее использование с середины 70-х годов для построения криптосистем с открытым ключом. Сейчас трудно себе представить инженера-системотехника или инженера-программиста, не владеющего хотя бы азами этой теории.

6.2.1. Использование теории чисел при открытом распределении секретных ключей

Пусть два абонента A и B обмениваются информацией по открытому каналу. Для защиты передаваемой информации может быть использован ключ K, который должен быть как у абонента A, так и у абонента B и больше ни у кого.

Абонент A, передавая сообщение S (двоичная последовательность кодированных букв, цифр, знаков и т. п.), может закодировать его следующим образом: вместо того, чтобы передавать открытое сообщение S, передаст сообщение $S \oplus K$, где $\oplus$ – булева операция сложения по модулю 2. Не зная ключа K, очень трудно расшифровать сообщение S. Если же ключ K известен, то расшифрование производится очень просто: достаточно к полученному сообщению $(S \oplus K)$ прибавить по модулю 2 значение ключа K. Такая криптосистема называется системой Вернама. К. Шеннон [2] показал, что эта система является системой с идеальной секретностью при трех непременных условиях:

– длина ключа K должна равняться длине сообщения S;

– ключ должен быть абсолютно случаен;

– после каждой передачи ключ должен уничтожаться.

Если даже не обращать внимание на то, что абсолютно случайный ключ построить необычайно тяжело, то мы тут же сталкиваемся с другой проблемой: как снабдить абонентов A и B секретным ключом K? Отправить курьера – дорого и опасно, поскольку курьера можно перехватить, отобрать секретный ключ или просто его купить. В связи с этим соображением в криптографии предполагается, что перехватчику информации известно все: и машины для шифрования, и коды. Неизвестным может быть только то, что очень хорошо охраняется (а это дорого) или что еще не успели украсть или купить.

Одна из идей криптографии с открытым ключом основана на трудностях логарифмирования сравнений. Так, если имеется равенство $a^x = b$, где a и b известны, и требуется найти x, то значение x находится элементарно: $x = \log a / \log b$.

Если же имеется сравнение $a^x \equiv b \bmod p$, где известны a, b и p, то для нахождения неизвестного x часто требуется произвести полный перебор.

В классической (симметричной) криптографии важной является проблема распределения ключей. Она частично решается с использованием так называемого несимметричного шифрования. Когда были опубликованы результаты по системам с открытым распределением ключей, большинству специалистов это показалось фантастикой. Два абонента, обмениваясь некоторыми данными по открытой сети, передавали секретные сообщения друг другу или вырабатывали общий ключ для его применения в системах симметричного шифрования. Переворот в криптографии был произведен с использованием модульной арифметики (теории чисел). Позже появились аналогичные системы: *RSA* [2], *ElCamal*, алгоритмы шифрования на эллиптических кривых и некоторые другие.

Двухступенчатая передача сообщений с использованием модульной арифметики

Сообщение может быть передано непосредственно от A к B за несколько шагов при использовании очень больших модулей.

Рассмотрим сначала случай, когда по открытому каналу Алиса и Боб договариваются использовать для шифрования своих сообщений некоторое очень большое простое число P. Пусть, например, P имеет 100 десятичных знаков. Тогда Алиса может зашифровать сообщение m возведением в некоторую степень x, известную только ей, и передать Бобу. Боб может возвести полученное сообщение в степень y, известную только ему, и возвратить Алисе. Алиса «снимет» свою степень x и передаст сообщение Бобу. Боб «снимет» свою степень y и прочитает сообщение. Общая схема выглядит следующим образом.

Алиса берет сообщение m, которое хочет передать Бобу, возводит в некоторую степень x, при этом $(x, P-1) = 1$, т. е. x и $P-1$ взаимно простые числа:

$$m^x \equiv S_1 \bmod P \longrightarrow$$

и передает S_1 Бобу. Боб возводит S_1 в некоторую степень y, $(y, P-1) = 1$:

$$\longleftarrow S_1^Y \equiv m^{xy} \equiv S_2 \bmod P$$

и возвращает S_2 Алисе.

Алиса должна снять свой ключ x, для этого она должна извлечь корень степени x из S_2. Это можно сделать при учете, что $(x, P-1) = 1$, следующим образом. Если возвести S_2 в степень $k_1 = \frac{1+(P-1)t_1}{x}$, где t_1 – некоторое целое, такое, что числитель дроби k_1 делится на x нацело, то в результате будет получено значение

$m^y \equiv S_3 \bmod P$.

Это значение S_3 Алиса передает Бобу.

Для того чтобы снять свой ключ, Боб может возвести S_3 в степень $k_2 = \frac{1+(P-1)t_2}{y}$ и в результате восстановит исходное сообщение m.

Пример. Пусть $P = 103$. $P-1 = 102 = 2 \cdot 51$. Алиса хочет передать сообщение $m = 83$. Алиса возводит число 83 в известную только ей степень, например $x = 35$, $(35, 102) = 1$: $83^{35} \equiv (((((83)^2)^2)^2)^2)^2 \cdot (83)^2 \cdot 83 \equiv ((((91)^2)^2)^2)^2 \cdot 91 \cdot 83 \equiv (((41)^2)^2)^2 \cdot 34 \equiv ((33)^2)^2 \cdot 34 \equiv (59)^2 \cdot 34 \equiv 7 \bmod 103$ и результат (число 7) передает Бобу. Боб полученное число возводит в известную только ему степень, например $y = 41$ (это число также взаимно просто с 102): $(7)^{41} \equiv ((7^3)^3)^3 \cdot (7^3)^3 \cdot 7^3 \cdot 7^2 \equiv (34^3)^3 \cdot 34 \cdot 49 \equiv 61^3 \cdot 61 \cdot 18 \equiv 55 \bmod 103$ и результат (55) возвращает Алисе. Алиса «снимает» свою степень x, решая сравнение $k_1 \equiv \frac{1+102 \cdot 12}{35} \equiv 35 \bmod 103$ и возводя число 55 в степень 35: $(55)^{35} \equiv ((55^3)^3)^3 \cdot ((55^2)^2)^2 \equiv (30^3)^3 \cdot (38^2)^2 \equiv 14^3 \cdot 2^2 \equiv 58 \bmod 103$.

Результат (число 58) Алиса передает Бобу. Боб «снимает» свою степень y, решая сравнение $k_2 \equiv \frac{1+102 \cdot 2}{41} \equiv 5 \bmod 103$ и возводя число 58 в степень 5: $(58)^5 \equiv (58^2)^2 \cdot 58 \equiv 68^2 \cdot 58 \equiv 83 \bmod 103$, получает сообщение, которое было адресовано ему Алисой. Таким образом, Боб расшифровал переданное сообщение, а незаконный перехватчик, получив все числа, которыми обменивались Алиса и Боб, не сумеет расшифровать это сообщение.

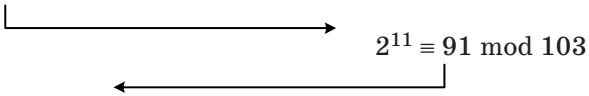
Формирование общего ключа по открытому каналу

Для формирования общего ключа по открытому каналу можно воспользоваться идеей Диффи и Хэллмана [2]. Пусть Алиса и Боб договорились использовать некоторое очень большое простое число P в качестве модуля. Кроме того, Алиса и Боб для этого числа P выбрали первообразный корень g, т. е. такое число, что для него самое малое число a, удовлетворяющее сравнению $g^a \equiv 1 \bmod P$, равно $a = P-1$.

Алиса берет первообразный корень g, возводит его в степень, известную только ей, находит остаток по модулю P: $g^{k_1} \equiv S_1 \bmod P$ и открыто передает остаток S_1 Бобу. Боб возводит первообразный корень g в известную только ему степень k_2, получает остаток S_2 по модулю P и передает S_2 Алисе. Далее Алиса возводит S_2 в степень k_2, а Боб возводит S_1 в степень k_2 по модулю P и оба получают один и тот же ключ $K = g^{k_1 \cdot k_2} \bmod P$. Далее Алиса и Боб могут воспользоваться этим общим ключом, например при применении симметричной криптосистемы *DES*. При необходимости произвести смену ключа операция обмена повторяется, при этом k_1 и k_2 выбираются заново.

Пример. Пусть $P = 103$. Первообразным корнем для данного P будет $g = 2$. Чтобы это проверить, представим $P-1$ в канонической форме: $102 = 2 \cdot 51$. Так как ни 2^2, ни 2^{51} не сравнимы с 1 по модулю 103, то 102 является минимальной степенью, которая обеспечивает сравнение $2^{102} \equiv 1 \bmod 103$ (теорема Ферма). Пусть Алиса выбрала $k_1 = 7$, а Боб выбрал $k_2 = 11$. Тогда они обменяются следующими данными:

$2^7 \equiv 25 \bmod 103$



и оба выработают один и тот же ключ:

Алиса: $91^7 \equiv \mathbf{38} \bmod 103$;

Боб: $25^{11} \equiv \mathbf{38} \bmod 103$.

Незаконный перехватчик, зная P и g и перехватив S_1 и S_2, не сумеет вычислить значение общего ключа $g^{k_1 \cdot k_2} \bmod P$. Эта уверенность исходит из следующих соображений.

Пусть имеется уравнение $a^x = b$, из которого требуется найти x. Прологарифмируем левую и правую части уравнения. Получим $x \log a = \log b$, откуда $x = \dfrac{\log a}{\log b}$, т. е. для степенного уравнения решение находится просто.

Если же имеется сравнение

$$a^x \equiv b \bmod P, \tag{6.1}$$

в котором известны значения a, b и P, то x находится в общем случае с помощью перебора. Задача решения сравнений вида (6.1) называется задачей дискретного логарифмирования. Несмотря на безусловные успехи последних лет в этой области, для произвольных модулей P решение близко к полному перебору. Если же P имеет порядка 100 десятичных разрядов, то и значения k_1 и k_2 имеют примерно тот же порядок, и для решения сравнения требуется производить перебор около 10^{100} вариантов, что является нереализуемым ни за какое приемлемое время.

Криптосистема RSA

Наиболее широко распространенной системой с открытым ключом является криптосистема *RSA* (*Rivest*, *Shamir*, *Adleman*). Идея системы состоит в том, что сложно разложить произведение двух очень больших простых чисел на сомножители, т. е. найти эти сомножители. Сама же идея системы *RSA* исключительно проста.

Пусть p и q – два случайно выбранных простых числа (каждое примерно по 100 десятичных разрядов). Обозначим: $n = pq$ и $\varphi(n) = (p-1)(q-1)$, где $\varphi(n)$ – функция Эйлера от n. Случайно выбирается большое число $d > 1$, такое, что $(d, \varphi(n)) = 1$, и вычисляется e, $1 < e < \varphi(n)$, удовлетворяющее сравнению: $ed \equiv 1 \bmod \varphi(n)$.

Числа n, e и d называются соответственно модулем, экспонентой зашифрования и экспонентой расшифрования.

Числа n и e образуют открытый ключ, а p, q, $\varphi(n)$ и d – секретную лазейку. При этом секретная лазейка включает в себя взаимозависимые величины. Так, если известно p (и, конечно, n и e), то остальные числа лазейки вычисляются просто: $q = n/p$; $\varphi(n) = (p-1)(q-1)$; d находится из условия $ed \equiv 1 \bmod \varphi(n)$.

Зашифрование обеспечивается возведением числового фрагмента текста S в степень e по модулю n. Расшифрование достигается возведением результата предыдущего шага в степень d.

При зашифровании получаем $S^e \equiv C \bmod n$. Здесь C – зашифрованный фрагмент текста. При расшифровании

$$C^d = S^{ed} = S^{1+\varphi(n)k} = S^{\varphi(n)k}\, S \equiv S \bmod n. \qquad (6.2)$$

Справедливость (6.2) легко видна, так как из сравнения $ed \equiv 1 \bmod \varphi(n)$ следует, что $ed = 1 + \varphi(n)k$, где k – некоторое целое.

Пример. Пусть $p = 11$, $q = 13$. Тогда $n = 143$, $\varphi(n) = 120$. Выберем d из условия: $(d, \varphi(n)) = 1$, например, $d = 37$, тогда из сравнения: $ed \equiv 1 \bmod \varphi(n)$ находим $e = 13$. Действительно, $13 \cdot 37 = 481 \equiv 1 \bmod 120$.

Для зашифрования возьмем фрагмент текста, который закодирован, например, числом $S = 42$: $42^{13} \equiv 3 \bmod 143$, т. е. шифр фрагмента $C = 3$.

Для расшифрования возведем число 3 в степень 37: $3^{37} \equiv 42 \bmod 143$. Таким образом, легальный получатель вычисляет значение исходного кода фрагмента. Нелегальный перехватчик не может вычислить передаваемое сообщение.

Передача с открытым ключом ЭльГамаля

Идея ЭльГамаля является аналогом идеи *RSA* и состоит в следующем. Алиса выбирает очень большое простое число P и число g – первообразный корень по модулю P. Вычисляет значение $y \equiv g^x \bmod P$. Открытыми ключами являются P, g и y. Число x является секретным

ключом Алисы. Если Боб решает послать секретное сообщение m Алисе, он придумывает некоторое целое число k, вычисляет $a \equiv g^k \bmod P$ и передает Алисе пару чисел $b \equiv m \cdot y^k \bmod P$ и $a \equiv g^k \bmod P$. Алиса возводит a в известную только ей степень x и решает сравнение

$$\frac{b}{a^x} \equiv \frac{mg^{xk}}{g^{kx}} \bmod P \equiv m \bmod P. \qquad (6.3)$$

В результате Алиса читает переданное ей сообщение m.

Пример. Пусть $P = 113$. Возьмем $g = 3$. Это число является первообразным корнем по модулю 113. Пусть Алиса выбрала $x = 59$. Вычислим $y \equiv 3^{59} \bmod 113 \equiv 86 \bmod 113$.

Открытыми ключами являются $P = 113$, $g = 3$ и $y = 86$. Секретным ключом Алисы является число $x = 59$. Боб хочет послать секретное сообщение Алисе в виде числа $m = 92$. Боб придумывает число $k = 37$, вычисляет $a \equiv 3^{37} \bmod 113 \equiv 24 \bmod 113$ и $b \equiv 92 \cdot 86^{37} \equiv 7 \bmod 113$ и посылает Алисе два числа $a = 24$ и $b = 7$. Алиса вычисляет $\frac{7}{24^{59}} \bmod 113 \equiv \frac{7}{75} \bmod 113 \equiv 92 \bmod 113$. Полученное сообщение полностью соответствует отправленному.

6.2.2. Линейные коды для коррекции ошибок при передаче сообщений

Одним из классов кодов, обнаруживающих или исправляющих ошибки при передаче сообщений в каналах связи, являются линейные коды. В качестве входного алфавита используются полиномы конечного поля Галуа $GF(q)$, где $q = p^h$, p – простое число, h – целое. Если V_n – векторное пространство размерности n над полем $GF(q)$, то подпространства размерности k пространства V_n называются p-ичными линейными кодами длины n с k информационными символами или (n, k)-кодами. При $p = 2$ эти коды называются групповыми кодами.

Пример 1. Пусть число разных передаваемых символов равно 2^{n-1}, например, при передаче двоичных кодов десятичных цифр можно взять $n = 5$. Образуем двоичные последовательности вида $(x_1, x_2, x_3, \ldots, x_{n-1})$ и сопоставим каждую последовательность одному из передаваемых символов. Сформируем еще один символ x_n по следующему правилу: $x_n = x_1 \oplus x_2 \oplus x_3 \oplus \ldots \oplus x_{n-1}$, где операция «$\oplus$» означает сложение по модулю 2. Если при передаче сообщений произошла ошибка в каком-либо одном разряде, то сумма $x_n \oplus x_1 \oplus x_2 \oplus x_3 \oplus \ldots \oplus x_{n-1}$ станет четной, если была изначально нечетной, или наоборот. Такая проверка позволяет обнаружить одиночную ошибку (все ошибки нечетной кратности).

Пример 2. Пусть требуется передать 16 различных сообщений (например, букв или символов). Закодируем эти сообщения 4-разрядными двоичными кодами и поставим им в соответствие последовательность x_3, x_5, x_6, x_7. Зарезервируем дополнительные разряды x_1, x_2, x_4 для контроля. Будем вычислять значения контрольных разрядов по следующему правилу:

$$\begin{pmatrix} 1010101 \\ 0110011 \\ 0001111 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = 0.$$

Таким образом, получаем $x_1 \oplus x_3 \oplus x_5 \oplus x_7 = 0$, $x_2 \oplus x_3 \oplus x_6 \oplus x_7 = 0$, $x_2 \oplus x_3 \oplus x_6 \oplus x_7 = 0$, откуда легко находятся значения контрольных разрядов x_1, x_2, x_4.

Пусть передаваемое сообщение имело вид 1011. Тогда значения контрольных разрядов определятся следующим образом: $x_1 = 0$, $x_2 = 1$, $x_4 = 0$. Вместо сообщения 1011 будет передано сообщение: 0 1 1 0 0 1 1. Пусть теперь в результате одиночной ошибки сообщение при передаче исказится и станет таким 0 1 1 0 0 0 1, т. е. исказился 6-й разряд сообщения. При проверке сообщения получаем двоичный код искаженного разряда: 1 1 0 (6-й разряд). Добавив по модулю 2 единицу в 6-й разряд, мы исправим сообщение. Приведенный пример является совершенным кодом Хэмминга, который исправляет одиночные ошибки.

6.2.3. Арифметические коды

Арифметические коды (или *AN*-коды) предназначены для коррекции ошибок при выполнении арифметических операций. Код определяется значением A, а слова из диапазона 0, 1, 2, ..., $N-1$ кодируются умножением на A.

Вектор одиночной ошибки представляет собой величину +1 или −1, которая арифметически складывается с кодовым словом (с учетом переносов, в отличие от ошибок в каналах связи). Для того чтобы код, порождаемый числом A длины n, исправлял одиночные арифметические ошибки, необходимо и достаточно, чтобы не выполнялось сравнение $2^s \equiv 2^k \bmod A$, где $s \neq k$; $s, k \in \{0, 1, 2, ..., n-1\}$.

Из п. 6.1.10 следует, что если e – показатель числа 2 по модулю A, то число A порождает арифметический код длины $n = e$, исправляющий одиночные ошибки. Совершенный арифметический код, исправляющий одиночные ошибки, может быть получен, если 2 является примитивным корнем по модулю A, причем A в этом случае должен являться простым числом.

Могут быть построены арифметические коды, исправляющие ошибки более высокой кратности, однако их анализ затруднителен. Так, для того, чтобы число A порождало код, исправляющий арифметические ошибки кратности t длины n, необходимо и достаточно, чтобы *не выполнялось* сравнение

$$2^{s_1} \pm 2^{s_2} \ldots \pm 2^{s_t} \equiv 2^{k_1} \pm 2^{k_2} \ldots \pm 2^{k_t} \bmod A, \qquad (6.4)$$

где все s_1, s_2, ... s_t, k_1, k_2, ... k_t – различные числа в диапазоне от 0 до $n-1$.

Единственным результатом, который позволяет строить длинные арифметические коды с большим кодовым расстоянием, удовлетворяющие условию (6.4), является набор теорем, доказанных И. Л. Ерошем и С. Л. Ерошем в 1968 г. [6].

Примеры. Определите длины арифметических кодов, исправляющих одиночные ошибки, порождаемых числами A = 7, 9 11, 19, 23, 25, 27, 29.

6.3. Задачи для контрольной

1. Решите сравнение $(19 \cdot 10^{153} + 37 \cdot 12^{28})$: $(13 \cdot 9) = 3X + 13^2 \bmod 11$.
2. Криптосистема с идеальной секретностью по Шеннону.
3. Проверьте формулу Эйлера для чисел $m = 33$, $a = 5$.
4. Решите сравнение $(38 \cdot 12^{250} + 23 \cdot 11^{25})$: $(18 \cdot 19) = 5X - 10 \bmod 13$.
5. Криптосистема *RSA*. Примеры.
6. Решите сравнение $(25 \cdot 16^{251} + 11 \cdot 15^{25})$: $(8 \cdot 29) = 12 + 3X \bmod 17$.
7. Теорема Ферма. Примеры.
8. Формирование общего ключа (по Диффи и Хэллману). Примеры.
9. Решите сравнение $(32 \cdot 14^{156} + 18 \cdot 12^{218})$: $(23 \cdot 29) = 25 + 3X \bmod 13$.
10. Проверьте форму Эйлера для чисел $m = 45$, $a = 4$.
11. Найдите функцию Эйлера для чисел 215, 360, 2553.
12. Решите сравнение $(16 \cdot 17^{21} + 57 \cdot 18^{25})$: $(8 \cdot 29) = 43X \bmod 19$.
13. Решите сравнение $(38 \cdot 10^{153} + 66 \cdot 12^{28})$: $(13 \cdot 9) = 13X \bmod 11$.
14. Проверьте формулу Эйлера для чисел $m = 63$, $a = 4$.
15. Решите сравнение $(42 \cdot 12^{250} + 75 \cdot 11^{25})$: $(18 \cdot 19) = 8X \bmod 13$.
16. Решите сравнение $(19 \cdot 16^{251} + 18 \cdot 15^{25})$: $(8 \cdot 29) = 5X \bmod 17$.
17. Решите сравнение $(22 \cdot 14^{156} + 31 \cdot 12^{218})$: $(23 \cdot 29) = 3X \bmod 13$.

18. Проверьте формулу Эйлера для чисел $m = 48$, $a = 7$.

19. Решите сравнение $(82 \cdot 12^{250} + 56 \cdot 11^{25}) : (18 \cdot 19) + 18(3 + 11^2) = 43X \bmod 13$.

20. Решите сравнение $(21 \cdot 17^{22} + 83 \cdot 18^{25}) : (8 \cdot 29) = 25X \bmod 19$.

21. Решите сравнение $(33 \cdot 10^{153} + 41 \cdot 12^{28}) : (13 \cdot 9) = 39X \bmod 11$.

22. Решите сравнение $(35 \cdot 12^{250} + 66 \cdot 11^{25}) : (18 \cdot 19) = 28X \bmod 13$.

23. Решите сравнение $(11 \cdot 16^{251} + 62 \cdot 15^{25}) : (8 \cdot 29) = 83X \bmod 17$.

24. Решите сравнение $(53 \cdot 14^{156} + 17 \cdot 12^{218}) : (23 \cdot 29) = 93X \bmod 13$.

25. Решите сравнение $(29 \cdot 12^{250} + 48 \cdot 11^{25}) : (18 \cdot 19) = 103X \bmod 13$.

26. Решите сравнение $(23 \cdot 17^{15} + 16 \cdot 18^{25}) : (8 \cdot 29) = 23X \bmod 19$.

27. Найдите НОК и НОД чисел $N_1 = 2658$; $N_2 = 3184$; $N_3 = 6638$.

28. Вычислите символы Лежандра

$$\left(\frac{17}{5}\right), \left(\frac{3}{17}\right), \left(\frac{11}{19}\right), \left(\frac{35}{23}\right), \left(\frac{169}{31}\right), \left(\frac{523}{43}\right).$$

29. Найдите квадратичные вычеты и невычеты по модулям 13, 17, 19.

30. Определите длину арифметических кодов, порождаемых числами $A = 17, 19, 23$.

Литература

1. *Москалев, Э. С.* Спектральный анализ и синтез дискретных устройств / Э. С. Москалев, М. Г. Карповский. М.: Энергия, 1972.

2. *Арто Саломаа.* Криптография с открытым ключом: [пер. с англ.] / Арто Саломаа. М.: Мир, 1995.

3. *Кассами, Т.* Теория кодирования: [пер. с японского] / Т. Кассами. М.: Мир, 1978. 576 с.

4. *Виноградов, И. М.* Основы теории чисел / И. М. Виноградов. М.: Наука, 1965. 172 с.

5. *Ерош, И. Л.* Элементы теории конечных групп: учеб. пособие / И. Л. Ерош. СПбГУАП. СПб., 1998.

6. *Ерош, И. Л.* Арифметические коды с исправлением многократных ошибок / И. Л. Ерош, С. Л. Ерош // Проблемы передачи информации. 1968. Т. 3. Вып. 4. С. 72–80.

7. *Ерош, И. Л.* Дискретная математика. Теория чисел: учеб. пособие / И. Л. Ерош. СПбГУАП. СПб., 2001. 32 с.

8. *Ерош, И. Л.* Дискретная математика. Математические вопросы криптографии: учеб. пособие / И. Л. Ерош. 2001. 46 с.

9. *Оре О.* Графы и их применение. М.: Мир, 1965. 174 с.

10. *Александров, П. С.* Введение в общую теорию множеств и функций / П. С. Александров. М.; Л., 1948.

11. *Арто Саломаа.* bookz.ru/abc/a-29 html

Заключение

Представленные в пособии разделы далеко не исчерпывают всех потребностей для анализа и синтеза вычислительных систем и сетей связи ни по полноте, ни по глубине. Это пособие нужно рассматривать только как первое знакомство с некоторыми разделами дискретной математики и продолжать их самостоятельное изучение дальше.

В пособие не вошли важные разделы по теории сложности алгоритмов, теории автоматов (методы проектирования цифровых устройств с памятью), нет раздела по дискретному спектральному анализу (ортогональные базисы Уолша, Хаара, интеграл Уолша, Шаудера и др.), который позволяет легко переходить от временного задания функций к спектральному и наоборот. Известно, что некоторые технические задачи легко формулируются и решаются на временном языке, а другие – на спектральном. Этот раздел естественно вытекает из линейных представлений групп, и авторы с трудом удержались от соблазна включить его в пособие.

Авторы надеются в будущем дополнить настоящее пособие, включив в него нерассмотренные разделы, показать связь между ними и привести примеры использования в технических системах.

Оглавление

Учебное издание

Ерош Игорь Львович
Сергеев Михаил Борисович
Соловьев Николай Владимирович

ДИСКРЕТНАЯ МАТЕМАТИКА
Учебное пособие

Редактор *А. Г. Ларионова*
Компьютерная верстка *А. Н. Колешко*
Корректор *Т. Н. Гринчук*

Сдано в набор 07.06.05. Подписано к печати 17.11.05. Формат 60×84 1/16. Бумага офсетная. Печать офсетная. Усл. кр.-отт. 9,9. Усл. печ. л. 8,8. Уч.-изд. л. 9,5. Тираж 1000 экз. Заказ № 8.

Отдел электронных публикаций и библиографии библиотеки
Отдел оперативной полиграфии
ГУАП
190000, Санкт-Петербург, ул. Б. Морская, 67