Министерство образования Республики Беларусь
Белорусский государственный университет
Факультет прикладной математики и информатики
Кафедра дискретной математики и алгоритмики

СОГЛАСОВАНО
Заведующий кафедрой
_____ Котов В.М.
«20»_____марта___ 2025 г.

СОГЛАСОВАНО
Декан факультета
_____Орлович Ю.Л.
« 25 » ____марта___2025 г.

Дискретная математика и математическая логика

В 2 частях. Часть 1.

Электронный учебно-методический комплекс для специальности
6-05-0533-11 «Прикладная информатика»

Регистрационный № 2.4.2-24 / 604

Автор:
Васильков Д. М., кандидат физико-математических наук, доцент.

Рассмотрено и утверждено на заседании Научно-методического совета БГУ 20.03.2025 г., протокол № 8.

Минск, 2025

УДК 519.1(075.8)+510.6(075.8)
В 193

Утверждено на заседании Научно-методического совета БГУ.
Протокол № 8 от 20.03.2025 г.

Решение о депонировании вынес
Совет факультета прикладной математики и информатики.
Протокол № 7 от 25.03.2025.

А в т о р

Васильков Дмитрий Михайлович, доцент кафедры биомедицинской информатики факультета прикладной математики и информатики БГУ.

Рецензенты:

кафедра программного обеспечения информационных технологий, УО «Белорусский государственный университет информатики и радиоэлектроники» (заведующий кафедрой Лапицкая Н.В., кандидат технических наук, доцент);

Шлыков В. В., профессор кафедры математики и методики преподавания математики УО «Белорусский государственный педагогический университет имени Максима Танка», кандидат физ.-мат. наук, доктор пед. наук, доцент.

Васильков, Д. М. Дискретная математика и математическая логика. В 2 частях. Часть 1 : электронный учебно-методический комплекс для специальности 6-05-0533-11 «Прикладная информатика» / Д. М. Васильков ; БГУ, Фак. прикладной математики и информатики, Каф. дискретной математики и алгоритмики. – Минск : БГУ, 2025. – 87 с. : ил. – Библиогр.: с. 85–87.

Электронный учебно-методический комплекс по учебной дисциплине «Дискретная математика и математическая логика. В двух частях. Часть 1.» предназначен для студентов специальности 6-05-0533-11 «Прикладная информатика». В ЭУМК содержатся лекционный материал, задания для практических занятий, список литературы.

ОГЛАВЛЕНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Электронный учебно-методический комплекс (ЭУМК) по учебной дисциплине «Дискретная математика и математическая логика. В двух частях. Часть 1.» предназначен для студентов специальности 6-05-0533-11 «Прикладная информатика». Комплекс подготовлен в соответствии с требованиями Положения об учебно-методическом комплексе на уровне высшего образования, утвержденного Постановлением министерства образования Республики Беларусь от 26.07.2011 № 167.

Содержание разделов ЭУМК соответствует образовательным стандартам, структуре и тематике типовых учебных программ по дисциплине «Дискретная математика и математическая логика» для указанных специальностей. Главные цели ЭУМК: помощь студентам в организации самостоятельной работы, повышение качества подготовки и усиление практико-ориентированности учебного процесса по дисциплинам.

ЭУМК состоит из следующих разделов.

- *Теоретический*. Включает аннотацию ЭУМК, написанного в соответствии с программами дисциплин. Материал данного комплекса, наряду с конспектом лекций, может быть использован для самостоятельной подготовки студентов к контрольным заданиям и экзамену/зачету.
- *Практический*. Содержит набор задач для самостоятельного решения. Данные материалы используются при проведении лабораторных занятий и для самостоятельной работы над курсом.
- *Вспомогательный* раздел включает рекомендуемую литературу.

Основной спецификой учебной дисциплины «Дискретная математика и математическая логика» является их алгоритмическая основа и демонстрация использования дискретности в современной науке. Учебная дисциплина «Дискретная математика и математическая логика» является не только фундаментом математической кибернетики, но и важным звеном математического образования для специалистов в области прикладной математики и информатики. Дисциплина знакомит студентов с такими дискретными объектами, как множества, комбинаторные структуры, графы, булевы функции, грамматики, конечные автоматы и алгоритмы. Указанные объекты определяют основу перечислительной комбинаторики, дискретной оптимизации, криптографии, теории алгоритмов и являются базовыми для многих прикладных областей. Прогресс в их изучении самым непосредственным образом влияет на состояние и развитие информационных технологий.

Для специальности 6-05-0533-11 «Прикладная информатика» дисциплина входит в компонент учреждения образования модуля «Дискретная математика и алгоритмика». Основой для изучения учебной дисциплины является дисциплина

государственного компонента «Математический анализ» модуля «Математический анализ», дисциплина государственного компонента «Основы высшей алгебры» модуля «Геометрия и алгебра», дисциплина государственного компонента «Аналитическая геометрия» модуля «Геометрия и алгебра», дисциплина государственного компонента «Линейная алгебра» модуля «Геометрия и алгебра». Знания, полученные в учебной дисциплине, используются при изучении дисциплины компонента учреждения образования «Алгоритмы и структуры данных» модуля «Дискретная математика и алгоритмика», дисциплины государственного компонента «Теория вероятностей и математическая статистика» модуля «Теория вероятностей и математическая статистика».

Цель преподавания учебной дисциплины «Дискретная математика и математическая логика» состоит в изучении методов решения логических и комбинаторных задач, получении будущими специалистами базового математического образования, необходимого им в дальнейшем для успешной работы, формирование у студентов современного математического кругозора, овладение навыками алгоритмического и логического мышления.

При изложении материала учебной дисциплины целесообразно выделить этап построения математической модели, адекватной реальной проблеме, а также показать возможность использования аппарата теории алгоритмов для анализа и обоснования выбора наиболее эффективных методов и алгоритмов для решения прикладных задач.

Основные задачи, решаемые при изучении учебной дисциплины «Дискретная математика и математическая логика»:

- Ознакомление студентов с такими фундаментальными понятиями как высказывание, предикат, множество, полнота, замкнутость, алгоритм и др.
- Обучение правильной записи математических утверждений с помощью логических и теоретико-множественных конструкций.
- Применение методов математической логики и теории множеств для решения задач перечислительной комбинаторики и теории графов.
- Обучение методам сравнения и классификации массовых проблем и алгоритмов по их сложности.

В результате изучения учебной дисциплины, обучающийся должен
знать:

- основные логические операции и формулы логики высказываний;
- основные понятия логики предикатов;
- базовые понятия и методы теории множеств и комбинаторики;
- основы теории булевых функций;
- основные понятия и результаты теории графов;
- элементы теории формальных грамматик и языков;
- основы теории алгоритмов, понятие о классах сложности P и NP.

уметь:

- переводить высказывания с естественного языка на формальный язык логики высказываний и логики предикатов;
- упрощать логические выражения и оперировать формулами логики предикатов;
- выполнять операции над множествами;
- решать базовые комбинаторные задачи;
- строить реализации булевых функций в заданном базисе, исследовать на полноту системы булевых функций;
- оценивать количественные характеристики графов, исследовать простейшие графы на изоморфизм, связность, двудольность и планарность, вычислять количественные характеристики графов;
- анализировать и строить простейшие грамматики;
- писать элементарные программы на языке машин Тьюринга.

Освоение учебной дисциплины «Дискретная математика и математическая логика» должно обеспечить формирование следующей специализированной компетенции для специальности 6-05-0533-11 «Прикладная информатика»:

СК-2. Решать задачи теоретического и прикладного характера из различных разделов дискретной математики и математической логики, применять решения задач комбинаторики, теории множеств, теории графов, математической логики, булевых функций, формальных языков и грамматик.

Для организации самостоятельной работы студентов и самоподготовки по курсу рекомендуется размещение программы курса, списка необходимой основной и дополнительной литературы, презентации лекций, заданий, тестов, методических рекомендаций на доступных сетевых ресурсах факультета и университета. Эффективность самоподготовки студентов целесообразно проверять в виде текущего и итогового контроля знаний в форме компьютерного тестирования как по отдельным темам, так и по разделам курса на образовательной платформе iRunner. Тесты, разработанные в iRunner, покрывают некоторые разделы учебной дисциплины и генерируются автоматически, что позволяет исключать списывание и делает тесты динамическими.

При составлении заданий УСР по учебной дисциплине необходимо предусмотреть возрастание их сложности: от заданий, формирующих достаточные знания по изученному учебному материалу на уровне узнавания, к заданиям, формирующим компетенции на уровне воспроизведения, и далее к заданиям, формирующим компетенции на уровне применения полученных знаний.

Таким образом, задания УСР по учебной дисциплине рекомендуется делить на три модуля:

1. задания, формирующие достаточные знания по изученному учебному материалу на уровне узнавания;
2. задания, формирующие компетенции на уровне воспроизведения;

3. задания, формирующие компетенции на уровне применения полученных знаний.

Для общей оценки качества усвоения студентами учебного материала рекомендуется использование рейтинговой системы оценивания, когда для каждого задания определен уровень сложности.

В образовательную платформу iRunner интегрирована свободная система управления содержимым (англ. CMS, или Content Management System) под названием MediaWiki. Этот продукт используется в качестве электронного учебника для размещения материалов лекций и практических занятий, в том числе по дискретной математике и математической логике. https://acm.bsu.by/wiki. Опыт показывает, что создавать материалы в вики-формате удобнее, чем публиковать отдельные doc- или pdf-файлы. Вики-страницы можно легко редактировать, сохраняется история изменений. Страницы связаны между собой ссылками. Вики-документы хорошо адаптированы для просмотра на мобильных устройствах, а при необходимости легко получить версию для печати.

1. ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

1.1. ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ

Математическая логика занимается формальными законами построения рассуждений и доказательств. В отличие от обычных рассуждений в математической логике отдельные слова и целые предложения естественного языка заменяются абстрактными символами, а получение новых знаний сводится к построению и анализу логических формул над этими символами. Результатом применения данного подхода к какой-либо прикладной области является создание так называемой *формальной системы*, в основе которой лежат символьные обозначения, набор базовых определений и простые интуитивно истинные утверждения. Из простых утверждений затем выводятся другие, более сложные.

Интерес к логике среди математиков и философов возник еще в древней Греции примерно в IV–VI веках до н.э. Первые серьезные сочинения принадлежат Аристотелю, который сформулировал правила вывода одних утверждений из других. Наибольшее развитие логика получила в XIX веке трудами европейских ученых, таких как Буль, де Морган, Шрёдер, Пирс, Дедекинд, Пеано, Уайтхед, Рассел и др. В частности, работая над обоснованием математики, Уайтхед и Рассел пытались свести всю чистую математику к логике, что, впрочем, не увенчалось успехом. Более ясное понимание роли логики в выработке новых знаний и вообще в человеческом мышлении пришло в 1930-х годах после публикации работ немецкого математика Курта Гёделя, который доказал, что любая формальная система является неполной, то есть не все истинные утверждения могут быть доказаны в рамках этой системы.

Какими бы простыми ни были базовые определения, они должны опираться в своих формулировках на еще более простые неопределяемые (*первичные*) понятия, смысл которых излагается с помощью слов естественного языка. Математическая логика тоже представляет собой формальную систему, и первичным понятием в ней является высказывание.

1.1.1. Высказывания

Под *высказыванием* понимается повествовательное предложение, относительно которого можно сказать, что оно либо истинно, либо ложно, но не то и другое одновременно.

Примеры высказываний:

- «$2 + 3 = 5$»,
- «Человек – это животное о двух ногах и без перьев.»,
- «Сегодня 17 января 1087 года.».

Запись «$2 + 3$» и фраза «17 января 1087 года» высказываниями не являются. Не являются высказываниями также парадоксы типа «Это утверждение ложно.», поскольку не могут быть ни истинными, ни ложными.

В математической логике мы абстрагируемся от смысла конкретных высказываний, обозначая их *логическими переменными* – символами произвольного алфавита, например, $a, b, x, y, \alpha, \beta$ и т.д. Для записи истинности или ложности высказываний используются *логические константы* – 1 или 0. Например, запись $a = 1,\ b = 0$ означает, что высказывание a истинно, а высказывание b ложно. Иногда логические константы обозначают символами И (истина), Л (ложь) или Т (True), F (False).

Среди всех высказываний выделяют простые высказывания, или *атомы*, – это высказывания, истинность или ложность которых не вызывает сомнения. Кроме простых высказываний, рассматриваются их комбинации, связанные логическими знаками, заменяющими слова обычного языка. В отличие от первичного понятия высказывания результаты применения логических связок строго определяются. Ниже перечислены основные логические связки, их обозначение и определение:

$\neg$ НЕ (*отрицание*): высказывание $\neg a$ (читается «не a») истинно тогда и только тогда, когда высказывание a ложно, и наоборот. Часто наряду с обозначением $\neg a$ используется более короткое $\overline{a}$.

$\wedge$ И (*конъюнкция*): высказывание $a \wedge b$ истинно тогда и только тогда, когда истинны одновременно высказывания a и b. Знак конъюнкции часто опускают и пишут просто ab.

$\vee$ ИЛИ (*дизъюнкция*): высказывание $a \vee b$ истинно тогда и только тогда, когда истинно высказывание a или истинно высказывание b или оба высказывания истинны одновременно.

$\oplus$ ИСКЛЮЧАЮЩЕЕ ИЛИ (*сумма по модулю* 2): высказывание $a \oplus b$ истинно тогда и только тогда, когда истинно высказывание a или высказывание b, но не то и другое одновременно.

$\Rightarrow$ СЛЕДУЕТ (*импликация*). По определению, высказывание $a \Rightarrow b$ ложно только в том случае, когда высказывание a истинно, а высказывание b ложно. Во всех остальных случаях высказывание $a \Rightarrow b$ истинно. Такая трактовка импликации означает, что из истинного утверждения не может следовать ложное, а из ложного высказывания может следовать все что угодно.

$\Leftrightarrow$ РАВНОСИЛЬНО (*эквивалентность*): запись $a \Leftrightarrow b$ означает, что a и b истинны или ложны одновременно.

Рассмотрим примеры применения различных логических связок.

1. **Отрицание (НЕ).** Высказывание $a =$ «$3 \leq 5$» является истинным. Его отрицание, то есть высказывание $\overline{a} =$ «$3 > 5$», является ложным.
2. **Конъюнкция (И).** Рассмотрим два высказывания: $a =$ «Принц богатый» и $b =$ «Принц красивый». Истинность конъюнкции $a \wedge b$ означает, что принц одновременно и богатый и красивый. Если эта конъюнкция ложна, то, значит, по крайней мере одно из этих высказываний ложно, например, принц некрасивый.
3. **Дизъюнкция (ИЛИ).** Пусть $a =$ «Этот карандаш цветной» и $b =$ «Этот карандаш короткий» (имеется в виду, что речь идет об одном и том же карандаше). Истинность дизъюнкции $a \vee b$ означает, что по крайней мере одна из характеристик карандаша – цветной или короткий – истинна. Возможно, что карандаш одновременно цветной и короткий.
4. **Сумма по модулю 2 (ИСКЛЮЧАЮЩЕЕ ИЛИ).** Эта связка используется, когда требуется подчеркнуть, что из двух высказываний верно только одно. Например, пусть $a =$ «Этот карандаш синий» и $b =$ «Этот карандаш желтый». Утверждение «Этот карандаш синий или желтый» должно интерпретироваться как «исключающее или» $a \oplus b$, а не как дизъюнкция $a \vee b$, поскольку карандаш не может быть синим и желтым одновременно. Если из смысла высказывания не понятно, о каком «или» идет речь, то это специально оговаривается.
5. **Импликация (СЛЕДУЕТ).** Запись $a \Rightarrow b$ читается следующим образом:
   - **Если** истинно a, **то** истинно b.
   - b истинно **тогда, когда** истинно a.
   - a истинно **только тогда, когда** истинно b.
   - Истинность b есть **необходимое** условие истинности a.
   - Истинность a есть достаточное условие истинности b.

   В естественном языке высказывания могут содержать импликацию в неявном виде, что иногда затрудняет их интерпретацию в виде символьного выражения. Для правильной интерпретации высказывания его необходимо перефразировать в виде одного из приведенных выше вариантов. Например, утверждение

   «Дифференцируемая функция непрерывна»

   означает, что **если** функция является дифференцируемой, **то** она является непрерывной. Поэтому данному высказыванию соответствует запись

   «Функция дифференцируемая» ⇒ «Функция непрерывная».

Другой пример – афоризм Пифагора (видоизменённый):

«Счастливым может быть только человек, живущий настоящим (то есть заботами только сегодняшнего дня)».

Эту же мысль можно перефразировать следующим образом:

«Человек счастлив **только тогда**, **когда** он живет настоящим»,

откуда получаем импликацию

«Человек счастлив» ⇒ «Человек живет настоящим».

Другими словами, «жить настоящим» есть необходимое (но не достаточное) условие для того чтобы «быть счастливым».

6. **Эквивалентность (РАВНОСИЛЬНО)**. Запись $a \Leftrightarrow b$ читается следующим образом:
   - a истинно **тогда и только тогда, когда** истинно b.
   - Истинность a есть **необходимое и достаточное** условие истинности b.

Результаты применения логической связки к одному или двум высказываниям удобно записывать в виде *таблицы истинности*:

a	$\overline{a}$
0	1
1	0

a	b	$a \wedge b$	$a \vee b$	$a \oplus b$	$a \Rightarrow b$	$a \Leftrightarrow b$
0	0	0	0	0	1	1
0	1	0	1	1	1	0
1	0	0	1	1	0	0
1	1	1	1	0	1	1

Если высказывание содержит несколько логических связок, то его истинность устанавливается с помощью последовательного применения этих связок. В качестве примера рассмотрим два высказывания

1. «Неверно, что сегодня идет дождь или идет снег.»
2. «Сегодня не идет дождь и не идет снег.»

Обозначим $s =$ «Идет снег» и $r =$ «Идет дождь». Тогда высказывание «Неверно, что идет дождь или идет снег» можно записать как $\overline{s \vee r}$, а высказывание «Не идет дождь и не идет снег» – как $\overline{s} \wedge \overline{r}$.

Составим таблицу истинности для этих выражений:

s	r	$s \vee r$	$\overline{s \vee r}$	$\overline{s}$	$\overline{r}$	$\overline{s} \wedge \overline{r}$
0	0	0	**1**	1	1	**1**
0	1	1	**0**	1	0	**0**
1	0	1	**0**	0	1	**0**
1	1	1	**0**	0	0	**0**

Из этой таблицы видно, что данные высказывания эквивалентны: их значения совпадают вне зависимости от того, идет или не идет снег и идет или не идет дождь.

Здесь мы впервые столкнулись с любопытным фактом: оказывается, некоторые высказывания могут быть одинаково истинны или ложны *только в силу своей логической структуры*, а не заложенного в них смысла. Структура логических высказываний задается с помощью формул.

1.1.2. Формулы

С помощью простых высказываний, логических констант и логических связок могут быть получены более сложные высказывания. Правильно построенное высказывание называется формулой. Дадим её индуктивное определение.

Определение 1.1.1.

1. Логические константы 0 и 1 есть *формулы*.

2. Переменная есть *формула*.

3. Если A и B – формулы, то $\overline{A}$, $A \wedge B$, $A \vee B$, $A \Rightarrow B$ и $A \Leftrightarrow B$ – тоже *формулы*.

4. Определение закончено.

Пусть a, b, x, y – переменные. Тогда $\overline{0}$, $\overline{a} \wedge b$, $(a \vee b) \Rightarrow \overline{(x \wedge y)}$ – формулы. Выражения вида $(x \Rightarrow \vee\, y)$ или $(\Rightarrow a)$ не могут быть выведены из индуктивного определения и поэтому не являются формулами.

Заметим, что при записи высказываний могут возникнуть неоднозначности в их трактовке. Например, в следующей записи непонятно, в каком порядке следует применять импликации:

$$a \Rightarrow b \Rightarrow c \Rightarrow d.$$

В подобных случаях помогают скобки, например:

$$a \Rightarrow \big(b \Rightarrow (c \Rightarrow d)\big) \text{ или } (a \Rightarrow b) \Rightarrow (c \Rightarrow d).$$

Чтобы уменьшить количество скобок, затрудняющих чтение формулы, вводится следующий порядок применения операций (слева направо):

$$\neg,\ \wedge,\ \vee,\ \Rightarrow,\ \Leftrightarrow.$$

С учетом этого порядка формулу $(a \vee b) \Rightarrow \overline{(x \wedge y)}$ можно переписать без использования скобок: $a \vee b \Rightarrow \overline{x \wedge y}$.

Существует более краткое определение формулы.

Определение 1.1.2.

1. Любая переменная есть *формула*.
2. Если A – формула, то $\overline{A}$ – тоже *формула*.
3. Если A и B – формулы, то $A \Rightarrow B$ – тоже *формула*.
4. Определение закончено.

Докажем эквивалентность этих двух определений. Для этого покажем, что с помощью одних только логических связок $\neg$ и $\Rightarrow$ можно построить любую формулу, содержащую логические связки $\wedge$, $\vee$ и $\Leftrightarrow$, а также логические константы 0 и 1. Действительно:

1. Для записи константы 1 можно использовать формулу $A \Rightarrow A$, а для записи константы 0 – формулу $0 = \overline{1} = \overline{A \Rightarrow A}$. То есть, согласно определению 1.1.2, логические константы являются формулами.
2. Для записи дизъюнкции $A \vee B$ можно использовать формулу

$$\overline{A} \Rightarrow B.$$

3. Конъюнкция $A \wedge B$ может быть выражена через отрицание и дизъюнкцию

$$A \wedge B = \overline{\overline{A} \vee \overline{B}} = \overline{A \Rightarrow \overline{B}}.$$

4. Равносильность $A \Leftrightarrow B$ выражается через конъюнкцию импликаций

$$A \Leftrightarrow B = (A \Rightarrow B) \wedge (B \Rightarrow A) = \overline{(A \Rightarrow B) \Rightarrow \overline{(B \Rightarrow A)}}.$$

Истинность этих равенств легко проверяется с помощью таблиц истинности. Например, для последнего равенства имеем

A	B	$A \Leftrightarrow B$	$A \Rightarrow B$	$B \Rightarrow A$	$\overline{(B \Rightarrow A)}$	$\overline{(A \Rightarrow B) \Rightarrow \overline{(B \Rightarrow A)}}$
0	0	**1**	1	1	0	**1**
0	1	**0**	1	0	1	**0**
1	0	**0**	0	1	0	**0**
1	1	**1**	1	1	0	**1**

1.1.3. Интерпретации, тавтологии и противоречия

Итак, заменив в формуле простые высказывания буквами, мы абстрагируемся от конкретного смысла утверждения, заложенного в этой формуле. Другими словами, в виде формулы мы имеем логическую связку неких фактов, суть которых нас не интересует. По словам Аристотеля, основной задачей логики является установление истинности или ложности утверждения при условии истинности

приведенных фактов, исходя лишь из формальной структуры рассуждения, а не из смысла этого утверждения и самих фактов.

Определение 1.1.3. Пусть $\boldsymbol{A(x_1, \dots, x_n)}$ – формула, где $\boldsymbol{x_1, \dots, x_n}$ – входящие в нее переменные. Конкретный набор $\boldsymbol{I}$ значений переменных называется *интерпретацией* формулы $\boldsymbol{A}$.

Формула может быть истинной при одной интерпретации и ложной при другой. Например, формула $x \Rightarrow y$ истинна при интерпретации $(0, 1)$ и ложна при интерпретации $(1, 0)$.

Определение 1.1.4. Если формула истинна при некоторой интерпретации, то она называется *выполнимой*. Если она истинна при всех возможных интерпретациях, то она называется *тавтологией* (или *общезначимой*). Формула, ложная при всех интерпретациях, называется *противоречием* (или *невыполнимой*).

Например, покажем, что формула $(p \Rightarrow q) \Rightarrow (p \Rightarrow \overline{q})$ является выполнимой. Для этого составим таблицу истинности, заполнив столбцы значениями выражений в скобках и их импликацией:

p	q	$p \Rightarrow q$	$p \Rightarrow \overline{q}$	$(p \Rightarrow q) \Rightarrow (p \Rightarrow \overline{q})$
0	0	1	1	1
0	1	1	1	1
1	0	0	1	1
1	1	1	0	0

Формула является выполнимой, поскольку является истинной при интерпретациях $(0, 0)$, $(0, 1)$ и $(1, 0)$. Доказать выполнимость этой формулы можно и без составления таблицы истинности. Заметим, что данная формула представляет собой импликацию двух выражений в скобках. Причем, если выражение в левой скобке $p \Rightarrow q$ равно 0, то независимо от значения правой скобки, импликация равна 1. Но $p \Rightarrow q = 0$ при $p = 1$ и $q = 0$. Таким образом, при интерпретации $(1, 0)$ формула истинна и поэтому является выполнимой по определению.

Примером тавтологии является формула $x \vee \overline{x}$ – *закон исключенного третьего*. Рассмотрим более сложный пример [20]:

«Один химик высказал предположение, что соли, которые не окрашены, есть соли, не являющиеся органическими соединениями, или органические соединения, которые не окрашены. Верно это или нет?».

Запишем это высказывание в виде формулы. Обозначим буквами следующие простые высказывания:

- с: «Это вещество – соль».
- к: «Это вещество окрашено».
- о: «Это вещество – органическое соединение».

Тогда записанное на языке логики высказываний, утверждение химика выглядит следующим образом

$$(\text{с} \wedge \overline{\text{к}}) \Rightarrow (c \wedge \overline{\text{о}}) \vee (\text{о} \wedge \overline{\text{к}}).$$

Построим таблицу истинности, заполнив столбцы значениями отдельных частей этой формулы и их комбинациями:

с	к	о	$\text{с} \wedge \overline{\text{к}}$	$c \wedge \bar{o}$	$o \wedge \overline{\text{к}}$	$(c \wedge \bar{o}) \vee (o \wedge \overline{\text{к}})$	$(\text{с} \wedge \overline{\text{к}}) \Rightarrow (c \wedge \bar{o}) \vee (o \wedge \overline{\text{к}})$
0	0	0	0	0	0	0	1
0	0	1	0	0	1	1	1
0	1	0	0	0	0	0	1
0	1	1	0	0	0	0	1
1	0	0	1	1	0	1	1
1	0	1	1	0	1	1	1
1	1	0	0	1	0	1	1
1	1	1	0	0	0	0	1

Таким образом, с помощью таблицы истинности мы установили, что с точки зрения формальной логики при любой комбинации истинности или ложности высказываний относительно данного вещества, конечное утверждение истинно, то есть является тавтологией.

Тавтология не сообщает никакой новой информации, поскольку она всегда истинна, независимо от того, о чём вообще идет речь. Чтобы убедиться в этом, подставим вместо высказываний о веществе любые другие, например, фразы из известного монолога Михаила Жванецкого «о раках по 3 и по 5 рублей»:

- с: «Раки – большие.»
- к: «Раки – дорогие.»
- о: «Раки продавались вчера (не сегодня).»

Получим следующее утверждение, которое в силу своей логической структуры всегда верно:

«Если раки на базаре большие и дешевые, значит они большие сегодня или же дешевые, но вчера».

Из определения тавтологии и противоречия вытекают следующие простые утверждения:

Утверждение 1.1.1. *Если A – тавтология, то $\overline{A}$ – противоречие и наоборот.*

Утверждение 1.1.2. *Если формулы A и $A \Rightarrow B$ – тавтологии, то формула B – тоже тавтология.*

Доказательство. Действительно, пусть существует интерпретация I, при которой $B(I) = 0$. По условию $A(I) = 1$, значит для интерпретации I формула

$(A \Rightarrow B)$ является ложной, то есть не является тавтологией, что противоречит условию. ■

Для доказательства того, что данная формула является тавтологией, существует несколько способов. Один из них – с помощью таблицы истинности – мы уже рассмотрели. Он считается простым, но при этом слишком громоздким и пригодным лишь для коротких формул с небольшим числом переменных.

Рассмотрим еще один способ, называемый доказательством «от противного», который особенно эффективен для формул, содержащих много импликаций. В качестве примера докажем, что следующая формула является тавтологией

$$(p \Rightarrow q) \Rightarrow \big((p \Rightarrow \overline{q}) \Rightarrow \overline{p}\big). \qquad (1.1.1)$$

Предположим, что это неверно. Значит, должна существовать интерпретация, при которой формула (1.1.1) ложна, то есть равна 0. Докажем, что такой интерпретации не существует.

Воспользуемся тем фактом, что импликация равна 0 только на одном наборе, а именно $(1, 0)$. Тогда в нашем случае левая и правая части формулы (1.1.1) относительно второго знака импликации должны быть, соответственно, равны

$$(p \Rightarrow q) = 1, \qquad (1.1.2)$$

$$\big((p \Rightarrow \overline{q}) \Rightarrow \overline{p}\big) = 0. \qquad (1.1.3)$$

Рассуждая аналогично, для формулы (1.1.3) получаем $(p \Rightarrow \overline{q}) = 1,\ \overline{p} = 0$, откуда $p = 1$. Подставим это значение в равенство $(p \Rightarrow \overline{q}) = 1$, получаем, что $q = 0$. Подстановка найденных значений p и q в формулу (1.1.2) даёт противоречие $(p \Rightarrow q) = 0$, доказывающее, что для формулы (1.1.1) не существует интерпретации, обращающей её в 0.

1.1.4. Логическое следствие и логическая эквивалентность

Определение 1.1.5. Формула B называется *логическим следствием* формулы A, обозначается $A \vdash B$, если для любой интерпретации, при которой формула A истинна, формула B тоже истинна. В этом случае говорят, что формула (высказывание) B *логически следует* из A.

Определение 1.1.6. Говорят, что формулы A и B *логически эквивалентны*, пишут $A = B$, если они являются логическим следствием друг друга. Логически эквивалентные формулы имеют одинаковые значения при любой интерпретации.

Ниже перечислены основные эквивалентности логики высказываний (для краткости знаки конъюнкции в формулах опущены).

Идемпотентность: $AA = A,$
$A \vee A = A,$

Коммутативность:	$AB = BA,$ $A \vee B = B \vee A,$ $A \oplus B = B \oplus A,$
Ассоциативность:	$A(BC) = (AB)C,$ $A \vee (B \vee C) = (A \vee B) \vee C,$ $A \oplus (B \oplus C) = (A \oplus B) \oplus C,$
Дистрибутивность:	$A(B \vee C) = AB \vee AC,$ $A \vee BC = (A \vee B)(A \vee C),$ $A(B \oplus C) = AB \oplus AC,$
Законы де Моргана:	$\overline{A \vee B} = \overline{A}\,\overline{B},$ $\overline{A \wedge B} = \overline{A} \vee \overline{B},$
Инволютивность:	$\overline{\overline{A}} = A,$
Свойства нуля и единицы:	$A \vee \overline{A} = 1,\ \ A\overline{A} = 0,\ \ A \oplus \overline{A} = 1,$ $A \vee 0 = A,\ \ A \wedge 0 = 0,\ \ A \oplus 0 = A,$ $A \vee 1 = 1,\ \ A \wedge 1 = A,\ \ A \oplus 1 = \overline{A},$
Правила поглощения:	$(A \vee B)A = A,$ $AB \vee A = A,$
Контрапозиция:	$(A \Rightarrow B) = \left(\overline{B} \Rightarrow \overline{A}\right),$
Другие равенства:	$\left(A \vee \overline{B}\right)B = AB,$ $A\overline{B} \vee B = A \vee B,$ $A \Rightarrow B = \overline{A} \vee B,$ $\overline{A \Rightarrow B} = A\overline{B},$ $A \Leftrightarrow B = AB \vee \overline{A}\,\overline{B},$ $A \oplus B = A\overline{B} \vee \overline{A}B.$

С помощью этих и других эквивалентностей можно упрощать и сравнивать формулы для решения различных задач.

В качестве примера продемонстрируем еще один способ доказательства того, что данная формула является тавтологией. Рассмотрим формулу (1.1.1) из предыдущего примера и докажем, что она эквивалентна константе 1. Для этого выпишем цепочку преобразований:

$$\begin{aligned}
(p \Rightarrow q) \Rightarrow \left((p \Rightarrow \overline{q}) \Rightarrow \overline{p}\right) &= \\
\overline{p \Rightarrow q} \vee \left(\overline{p \Rightarrow \overline{q}} \vee \overline{p}\right) &= \\
p\overline{q} \vee pq \vee \overline{p} &= \\
p(\overline{q} \vee q) \vee \overline{p} &= \\
p \vee \overline{p} &= 1.
\end{aligned}$$

Определение 1.1.7. Формула B называется *логическим следствием* формул $A_1, \dots, A_n$, обозначается $A_1, \dots, A_n \vdash B$, если для любой интерпретации, для которой каждая из формул $A_1, \dots, A_n$ истинна, формула B тоже истинна.

Заметим, что для данной интерпретации каждая из формул $A_1, \dots, A_n$ истинна тогда и только тогда, когда для этой интерпретации истинна формула

$$A_1 \wedge \dots \wedge A_n.$$

Например,

$$x, (x \Rightarrow y) \vdash y, \ (x \Rightarrow y), (y \Rightarrow z) \vdash (x \Rightarrow z).$$

Иногда для обозначения логического следствия используют запись:

$$\begin{array}{l} x \\ x \Rightarrow y \\ \hline \therefore y \end{array} \qquad \begin{array}{l} x \Rightarrow y \\ y \Rightarrow z \\ \hline \therefore x \Rightarrow z \end{array}$$

В качестве примера рассмотрим следующие суждения:

«Если стартер на заработает, машина не заведётся.»

«А стартер не заработает, если не исправлен замок зажигания.»

«Но машина завелась.»

«Следовательно, замок зажигания исправен.»

Обозначим простые высказывания символами:

С – «Стартер работает.»,

З – «Замок зажигания исправен.»,

М – «Машина заводится.».

Получаем последовательность из трех формул и их логическое следствие:

$$\overline{\text{С}} \Rightarrow \overline{\text{М}}, \ \overline{\text{З}} \Rightarrow \overline{\text{С}}, \ \text{М} \vdash \text{З}.$$

Мы записали данное умозаключение в символьном виде. Но верно ли оно? Выпишем значения приведенных формул в виде таблицы истинности и рассмотрим строки этой таблицы, в которых значения первых трёх формул равны 1.

С	З	М	$\overline{\text{С}} \Rightarrow \overline{\text{М}}$	$\overline{\text{З}} \Rightarrow \overline{\text{С}}$
0	0	0	1	1
0	0	1	0	1
0	1	0	1	1
0	1	1	0	1
1	0	0	1	0
1	0	1	1	0
1	1	0	1	1
1	**1**	**1**	**1**	**1**

Такая строка всего одна – последняя, соответствующая набору $(1, 1, 1)$. Поскольку формула З, соответствующая логическому следствию, на этом наборе тоже равна 1, заключаем, что логическое следствие верно по определению.

Важно отметить, что логическое следствие является новым знанием, новой информацией, полученной из известных фактов.

Теорема 1.1.1 (Основная теорема логического вывода).

Формула B является логическим следствием формул $A_1, \dots, A_n$ тогда и только тогда, когда формула $A_1 \wedge \dots \wedge A_n \Rightarrow B$ является тавтологией.

Доказательство. $\Rightarrow$ («только тогда, когда…», необходимость). Пусть B – логическое следствие, докажем, что $A_1 \wedge \dots \wedge A_n \Rightarrow B$ – тавтология. Пусть I – произвольная интерпретация. Если все $A_i(I)$ истинны, то, по условию, B также истинна, и стало быть, истинна импликация $A_1 \wedge \dots \wedge A_n \Rightarrow B$. Если же среди $A_i(I)$ имеется хотя бы одно ложное утверждение, то эта импликация также истинна (по определению). Следовательно, эта формула – тавтология.

$\Leftarrow$ («тогда, когда…», достаточность). Известно, что формула – тавтология, докажем, что B – логическое следствие. Пусть I – интерпретация, для которой все A_i истинны. Значит конъюнкция $A_1 \wedge \dots \wedge A_n$ истинна и, стало быть, B тоже истинна, поскольку истинна импликация. ■

Докажем в качестве примера, что суждение про машину верно. Имеем

$$\overline{\mathrm{С}} \Rightarrow \overline{M}, \quad \overline{\mathrm{З}} \Rightarrow \overline{C}, \quad \mathrm{М} \vdash \mathrm{З}.$$

Из основной теоремы логического вывода следует, что это суждение верно тогда и только тогда, когда следующая формула является тавтологией

$$\left(\overline{\mathrm{С}} \Rightarrow \overline{M}\right) \wedge \left(\overline{\mathrm{З}} \Rightarrow \overline{C}\right) \wedge \mathrm{М} \Rightarrow \mathrm{З}.$$

Предположим, что эта формула не является тавтологией. Значит ее часть слева от импликации равна 1, а часть справа равна 0. Отсюда сразу следует, что $\mathrm{М} = 1$ и $\mathrm{З} = 0$. Подставив найденные значения в выражения в скобках, получим, что две импликации $\overline{\mathrm{С}} \Rightarrow 0$ и $1 \Rightarrow \overline{\mathrm{С}}$ должны быть одновременно равны 1, что невозможно при любых значениях переменной С. Полученное противоречие доказывает, что данная формула есть тавтология, и, значит, суждение о машине верно.

Следствие 1.1.1. *Формула B является логическим следствием формул $A_1, \dots, A_n$ тогда и только тогда, когда формула $A_1 \wedge \dots \wedge A_n \wedge \neg B$ является противоречием.*

Доказательство. Формула $A_1 \wedge \dots \wedge A_n \Rightarrow B$ является тавтологией тогда и только тогда, когда $\neg\,(A_1 \wedge \dots \wedge A_n \Rightarrow B)$ – противоречие. Но

$$\begin{aligned} \neg\,(A_1 \wedge \dots \wedge A_n \Rightarrow B) &= \neg(\neg(A_1 \wedge \dots \wedge A_n) \vee B) \\ \text{(по закону де Моргана)} &= \neg\neg(A_1 \wedge \dots \wedge A_n) \wedge \neg B \\ &= A_1 \wedge \dots \wedge A_n \wedge \neg B. \end{aligned}$$ ■

1.1.5. Предикаты

В естественном языке встречаются высказывания, истинность которых может меняться в зависимости от объектов, о которых идет речь. Например, высказывание «Синий кит есть млекопитающее» истинно, а «Белая акула есть млекопитающее» – ложно. В логике высказывание, зависящее от параметров, называется *предикатом*. Как и обычное высказывание, предикат принимает только два значения – 0 (ложь) или 1 (истина).

Например, чтобы записать высказывания о принадлежности животных классу млекопитающих, можно ввести предикат МЛЕКОПИТАЮЩЕЕ(x), который обозначает фразу «x относится к классу млекопитающих».

Тогда МЛЕКОПИТАЮЩЕЕ (*синий кит*) = 1, а МЛЕКОПИТАЮЩЕЕ (*белая акула*) = 0. Другими примерами предикатов являются любые математические равенства и неравенства, такие как $x + y < 3,\ x^n + y^n = z^n$, которые могут быть верными или ложными в зависимости от конкретных значений переменных.

Предикаты могут иметь сложную внутреннюю структуру. Рассмотрим ее более подробно. Пусть M – элементы некоторой предметной области. В нашем примере такими элементами являются виды животных «синий кит» и «белая акула».

Определение 1.1.8. Переменная или константа предметной области M называется *термом*. Высказывание $P(t_1, \dots, t_n)$ относительно термов $t_1, \dots, t_n$ называется *n-местным атомным предикатом*.

Чтобы построить высказывания, охватывающие все элементы предметной области, в логике предикатов вводится дополнительная логическая связка $\forall$, которая читается *для всех*. Запись $(\forall x)P(x)$ читается так: «для всех x выполняется $P(x) = 1$» или «для всех x высказывание $P(x)$ истинно».

Определим рекурсивно понятие формулы логики предикатов.

Определение 1.1.9.

1. Атомный предикат есть *формула*.
2. Если P – формула, то $\overline{P}$ – тоже *формула*.
3. Если P и Q – формулы, то $P \Rightarrow Q$ – тоже *формула*.
4. Если P – формула, а x – переменная предметной области, то $(\forall x)P$ – тоже *формула*.
5. Определение закончено.

Как и в логике высказываний, к предикатам применимы другие логические связки ($\wedge$, $\vee$, $\Leftrightarrow$), которые тоже могут участвовать в построении формул.

Кроме того, вводится еще одна дополнительная связка $\exists$, которая читается как *существует* и определяется через связку *для всех* следующим образом: по определению, формула $(\exists x)P(x)$ эквивалентна формуле

$$\overline{(\forall x)\overline{P}(x)}.$$

Действительно, фраза «существует x такой, что выполняется свойство $P(x)$» эквивалентна другому выражению: «не верно, что для всех x не выполняется свойство $P(x)$».

Новые логические связки ∀ и ∃ называются *кванторами*: ∀ называется *квантором всеобщности*, а ∃ – *квантором существования*.

Переменная предметной области называется *связанной*, если она находится в области действия квантора, в противном случае – свободной. Например, в формуле

$$(\forall x)\big(P(x,y) \vee Q(x,z)\big) \Rightarrow R(y,z)$$

переменная x связанная, а y и z – свободные. Предикатная формула, в которой все переменные связаны, является, по сути, высказыванием, не зависящим от этих переменных.

Рассмотрим пример. Пусть задан одноместный предикат $P(x)$, где переменная x может принимать значения $x_1, \dots, x_n$. Тогда, по определению

$$\begin{aligned} (\forall x)P(x) &= P(x_1) \wedge \dots \wedge P(x_n), \\ (\exists x)P(x) &= P(x_1) \vee \dots \vee P(x_n). \end{aligned} \qquad (1.1.4)$$

Здесь высказывания $P(x_i),\ i = 1, \dots, n,$ имеют конкретные фиксированные значения, не зависящие от переменной предметной области.

Для формул логики предикатов справедливы следующие равносильности, которые непосредственно следуют из соотношений (1.1.4):

- Комбинации кванторов:

$$(\forall x)(\forall y)P(x,y) = (\forall y)(\forall x)P(x,y)$$
$$(\exists x)(\exists y)P(x,y) = (\exists y)(\exists x)P(x,y)$$
$$(\forall x)(\exists y)P(x,y) \neq (\exists y)(\forall x)P(x,y)$$

- Законы де Моргана:

$$\neg(\forall x)P(x) = (\exists x)\neg P(x)$$
$$\neg(\exists x)P(x) = (\forall x)\neg P(x)$$

- Вынесение кванторов за скобки:

$$(\forall x)P(x) \wedge (\forall x)Q(x) = (\forall x)\big(P(x) \wedge Q(x)\big)$$
$$(\exists x)P(x) \vee (\exists x)Q(x) = (\exists x)\big(P(x) \vee Q(x)\big)$$
$$(\exists x)P(x) \wedge (\exists x)Q(x) = (\exists x)(\exists y)\big(P(x) \wedge Q(y)\big)$$
$$(\forall x)P(x) \vee (\forall x)Q(x) = (\forall x)(\forall y)\big(P(x) \vee Q(y)\big)$$

Из этих соотношений следует, в частности, что вынесение квантора за скобки неприменимо к импликации:

$$(\forall x)\big(P(x) \Rightarrow Q(x)\big) \neq (\forall x)P(x) \Rightarrow (\forall x)Q(x).$$

Действительно, левая часть этого выражения эквивалентна формуле

$$(\forall x)\left(\overline{P}(x) \vee Q(x)\right) = (\forall x)\overline{P}(x) \vee (\forall y)Q(y),$$

а правая – другой, неэквивалентной формуле

$$\overline{(\forall x)P(x)} \vee (\forall y)Q(y) = (\exists x)\overline{P}(x) \vee (\forall y)Q(y).$$

По сути, вынесение квантора за скобки сводит предикатную формулу к обычному логическому выражению, которое можно преобразовать и сократить с помощью известных нам формул логики высказываний. Рассмотрим эту операцию более подробно.

Говорят, что предикатная формула находится в *приведенной форме*, если она не содержит логических связок, отличных от ∧, ∨ и ¬, причем отрицание не охватывает кванторы и может применяться только к простым предикатам.

Например, формула $(\forall x)P(x) \vee (\forall y)\overline{Q}(y)$ находится в приведенной форме, а эквивалентная ей формула $\overline{(\forall x)P(x)} \Rightarrow (\forall y)\overline{Q}(y)$ – нет.

Говорят, что формула находится в *нормальной форме*, если она имеет вид

$$(Q_1 x_1) \ldots (Q_k x_k)P(x_1, \ldots, x_k) \text{ или } P(x_1, \ldots, x_k).$$

где символы Q_i обозначают кванторы ∀ или ∃, а формула $P(x_1, \ldots, x_k)$ не содержит кванторов и находится в приведенной форме. Например, формула

$$(\exists x)(\forall y)(P(x) \wedge \overline{Q}(y)$$

находится в нормальной форме, а формулы из примера выше – нет.

Приведем без доказательства следующее утверждение.

Теорема 1.1.2. *Для каждой формулы логики предикатов существует эквивалентная ей формула в нормальной форме.*

Рассмотрим пример. Найдём нормальную форму для формулы

$$(\forall x)P(x) \Rightarrow (\forall x)Q(x).$$

Выпишем эквивалентные преобразования:

$$\begin{aligned}
&\overline{(\forall x)P(x)} \vee (\forall x)Q(x) = \\
&(\exists x)\overline{P}(x) \vee (\forall x)Q(x) = \\
&(\exists x)\overline{P}(x) \vee (\forall y)Q(y) = \\
&(\exists x)(\forall y)\left(\overline{P}(x) \vee Q(y)\right).
\end{aligned}$$

1.1.6. Метод математической индукции

Этот метод является эффективным инструментом построения доказательств в различных областях математики.

Пусть $A(n)$ – высказывание, зависящее от натурального числа n, истинность которого требуется доказать для *всех* натуральных n. В упрощенной форме принцип математической индукции можно записать в виде следующей формулы логики предикатов:

$$\Big(A(1) \wedge (\forall k)\big(A(k) \Rightarrow A(k+1)\big)\Big) \Rightarrow (\forall n)A(n).$$

Утверждение $A(1)$ называется *базой индукции*, предикат $A(k)$ – *индуктивным предположением*, а формула $A(k) \Rightarrow A(k+1)$ – *индуктивным переходом*.

Если доказаны база индукции и индуктивный переход, то утверждение $A(n)$ является верным для всех натуральных n. При этом верность импликации достаточно доказать лишь для случая, когда истинно индуктивное предположение $A(k)$. Таким образом, доказательство с помощью математической индукции состоит из трех шагов:

1. Формулировка и доказательство базы индукции.

2. Формулировка индуктивного предположения.

3. Доказательство индуктивного перехода.

Рассмотрим пример. Пусть требуется доказать, что для любого положительного числа n число $n^3 - n$ делится на 3.

Сначала сформулируем и докажем базу индукции. Для $n = 1$ имеем:

$$1^3 - 1 = 0 \text{ делится на } 3.$$

Далее формулируем индуктивное предположение: пусть утверждение истинно для $\mathrm{k} \geq 1$, то есть равенство $k^3 - k = 3m$ верно для некоторого неотрицательного m. Покажем, что истинность этого предположения влечет истинность утверждения для $k+1$, то есть $(k+1)^3 - (k+1)$ делится на 3.

Действительно, имеем

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1)\\ &= (k^3 - k) + 3(k^2 + k)\\ &= 3m + 3(k^2 + k).\end{aligned}$$

Получили число, которое очевидно делится на 3. ■

1.2. МНОЖЕСТВА И ОТНОШЕНИЯ

1.2.1. Основные понятия и обозначения

Множество – фундаментальное неопределяемое математическое понятие. Под множеством понимают произвольную совокупность отличных друг от друга объектов, рассматриваемых как единое целое. Например, множество членов данной семьи, множество книг на полке, множество всех атомов во вселенной, множество всех натуральных чисел и т.д.

Объекты, из которых состоит множество, называются его *элементами*. Множества обозначаются, как правило, заглавными буквами: $A, X, \mathbb{N}$, а элементы – строчными: a, x, n. Для записи множества используют фигурные скобки:

$$A = \{a_1, a_2, a_3\}, \quad \mathbb{N} = \{1, 2, 3, \dots\}.$$

Если A – множество, а a – его элемент, то пишут $a \in A$, в противном случае пишут $a \notin A$. Множество, не содержащее ни одного элемента, называется *пустым* и обозначается символом $\emptyset$.

Определение 1.2.1. Два множества A и B называются *равными*, пишут $A = B$, если они состоят из одних и тех же элементов, то есть

$$(A = B) \Leftrightarrow (\forall x)\big((x \in A) \Leftrightarrow (x \in B)\big).$$

Например, $\{1, 3, 7\} = \{7, 1, 3\}$. Из этого определения следует, что

$$\{a, \dots, a\} = \{a\}.$$

Существует два основных способа задания множеств:

1. Перечисление всех его элементов.
2. Описание свойства, по которому можно определить, какие элементы принадлежат данному множеству, а какие ему не принадлежат.

Понятно, что первый способ годится только для множеств с небольшим числом элементов. Свойство, описывающее множество, задается в виде условия (предиката), которое выполняется для всех элементов данного множества и только для них. Если $P(x)$ – предикат, то для задания множества используют запись вида $\{\, x \mid P(x) \,\}$, которая читается «множество всех x, для которых выполняется свойство P».

Например, для задания множества натуральных чисел от 1 до 1000 пишут

$$\{\, x \mid (x \in \mathbb{N}) \wedge (1 \le x \le 1000) \,\}.$$

1.2.2. Подмножества, операции над множествами

Определение 1.2.2. Множество A называется *подмножеством* множества B, пишут $A \subseteq B$, если любой элемент A является также элементом B:

$$(A \subseteq B) \Leftrightarrow (\forall\, x)\big((x \in A) \Rightarrow (x \in B)\big).$$

Например:

$$\{a, e\} \subseteq \{a, b, c, d, e\},$$

$$\{x \mid (x \in \mathbb{N}) \wedge (1 \leq x \leq 20)\} \subseteq \mathbb{N}.$$

Если A – подмножество B, то говорят, что A *содержится* в B или что B *включает* A. Если $A \subseteq B$ и при этом $A \neq B$, то говорят, что A есть *собственное* подмножество B, и пишут $A \subset B$. По определению, $M \subseteq M$ и $\emptyset \subseteq M$ для любого множества M.

Рассмотрим следующие операции над множествами:

- *Объединение* множеств A и B есть множество

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}.$$

- *Пересечение* множеств A и B есть множество

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}.$$

- *Разность* множеств A и B есть множество

$$A \backslash B = \{x \mid (x \in A) \wedge (x \notin B)\}.$$

- *Симметрическая разность* множеств A и B есть множество

$$A \oplus B = (A \backslash B) \cup (B \backslash A) = (A \cup B) \backslash (A \cap B)).$$

- *Дополнение* множества $A \subseteq U$ есть множество

$$\overline{A} = \{x \in U \mid x \notin A\}.$$

Эта операция определена при условии, что существует некое универсальное множество U, называемое *универсум*, содержащее A. Тогда, по определению,

$$\overline{A} = U \backslash A.$$

Рассмотрим пример. Пусть $A = \{ 1, 2, 3, 4, 5, 6 \}$ и $B = \{ 2, 4, 6, 8 \}$. Тогда

$$A \cup B = \{1, 2, 3, 4, 5, 6, 8\},$$

$$A \cap B = \{2, 4, 6\},$$

$$A \backslash B = \{1, 3, 5\},$$

$$A \oplus B = \{1, 3, 5, 8\},$$

$$\overline{A} = \{x \mid (x \in \mathbb{N}) \wedge (x > 6)\}.$$

Пусть U – универсум, $A, B, C \subset U$. Тогда выполняются следующие соотношения:

Идемпотентность:	$A \cap A = A, \ A \cup A = A,$
Коммутативность:	$A \cap B = B \cap A, \ A \cup B = B \cup A,$
Ассоциативность:	$A \cap (B \cap C) = (A \cap B) \cap C,$ $A \cup (B \cup C) = (A \cup B) \cup C,$

Дистрибутивность:	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
Законы де Моргана:	$\overline{A \cup B} = \overline{A} \cap \overline{B}$,
	$\overline{A \cap B} = \overline{A} \cup \overline{B}$,
Инволютивность:	$\overline{\overline{A}} = A$,
Свойства нуля и единицы:	$A \cup \overline{A} = U, \ \ A \cap \overline{A} = \emptyset$,
	$A \cup \emptyset = A, \ \ A \cap \emptyset = \emptyset$,
	$A \cup U = U, \ A \cap U = A$,
Правила поглощения:	$(A \cup B) \cap A = A$,
	$(A \cap B) \cup A = A$.

Согласно свойствам коммутативности и ассоциативности результат объединения или пересечения двух и более множеств не зависит от порядка выполнения операций, поэтому часто используется сокращенная форма записи

$$A_1 \cup \ldots \cup A_n = \bigcup_{i=1}^{n} A_i, \ \ A_1 \cap \ldots \cap A_n = \bigcap_{i=1}^{n} A_i.$$

Операции над множествами удобно иллюстрировать с помощью *диаграмм Эйлера*, изображенных на рисунке 1.2.1. Диаграммы Эйлера также могут использоваться для доказательства приведенных выше соотношений. Однако, здесь важно понимать, что в общем случае множества могут находиться в разных отношениях: пересекаться или не пересекаться, входить друг в друга или не входить, одно или несколько множеств могут быть пустыми и т.д. Поэтому, чтобы проанализировать всевозможные такие комбинации, потребуется не одна, а много диаграмм – даже в простейших случаях, не говоря уже о большом количестве множеств.

К счастью, существует строгий формальный способ доказательства соотношений между множествами с помощью определений и формул логики высказываний. Например, докажем закон де Моргана для пары множеств:

$$\begin{aligned}
\overline{A \cup B} &= \{x \mid x \notin A \cup B\} \\
&= \left\{x \mid \overline{x \in A \cup B}\right\} \\
&= \left\{x \mid \overline{(x \in A) \vee (x \in B)}\right\} \\
&= \left\{x \mid \overline{x \in A} \wedge \overline{x \in B}\right\} \\
&= \{x \mid (x \notin A) \wedge (x \notin B)\} \\
&= \left\{x \mid \left(x \in \overline{A}\right) \wedge \left(x \in \overline{B}\right)\right\} \\
&= \overline{A} \cap \overline{B}.
\end{aligned}$$

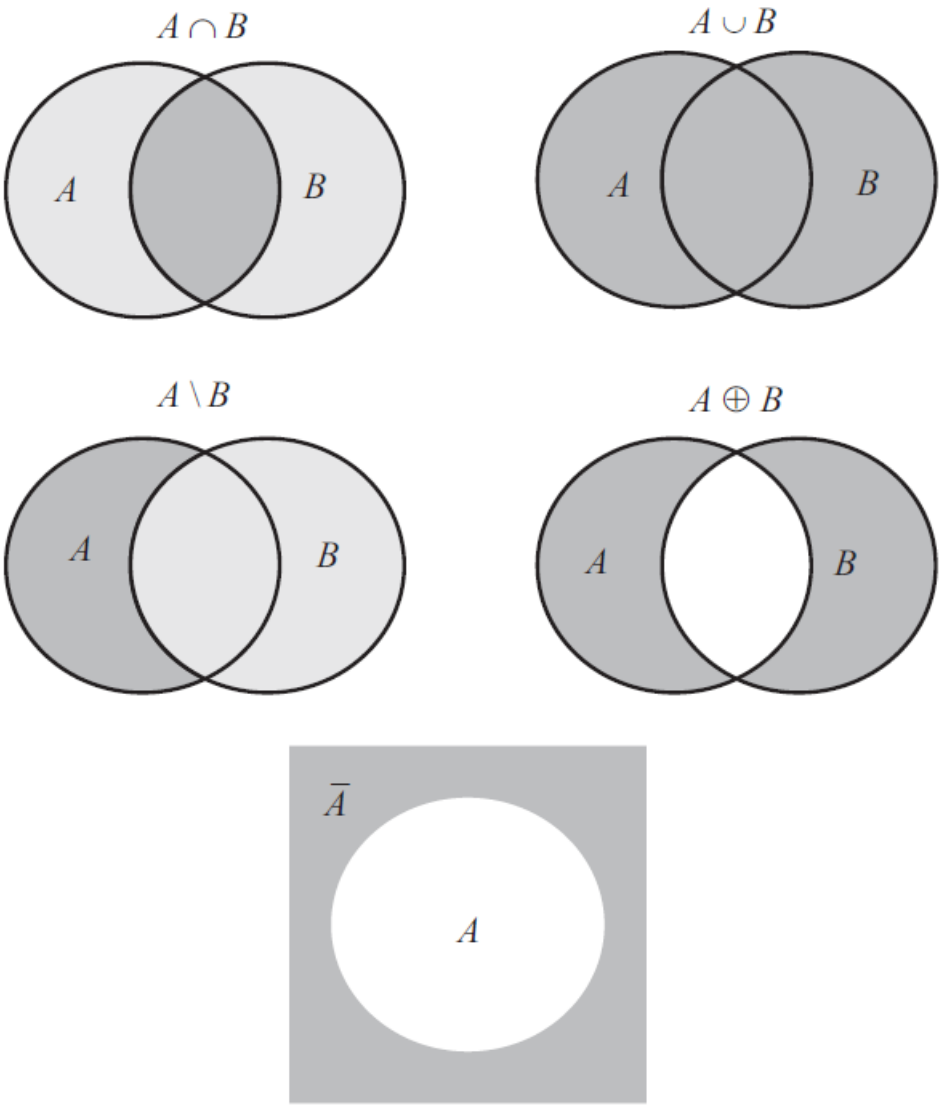

Рисунок 1.2.1 Диаграммы Эйлера

Рассмотрим более сложный пример, включающий операции над множествами и понятие подмножества. Пусть требуется доказать, что

$$\big((\mathrm{A} \cap \mathrm{B}) \cup \mathrm{C} = \mathrm{A} \cap (\mathrm{B} \cup \mathrm{C})\big) \Leftrightarrow \mathrm{C} \subseteq \mathrm{A}.$$

Для сокращения записи введем предикат $a(x)$, обозначающий утверждение «$x \in A$», аналогично $b(x)$ для множества B и т.д. Нужно доказать, что

$$(\forall x)\big(a(x)b(x) \vee c(x) = a(x)b(x) \vee a(x)c(x)\big) \Leftrightarrow (\forall x)\big(c(x) \Rightarrow a(x)\big).$$

Докажем необходимость ($\Rightarrow$). Перепишем правую часть выражения в виде

$$(\forall \mathrm{x})\big(\overline{\mathrm{c}}(\mathrm{x}) \vee \mathrm{a}(\mathrm{x})\big),$$

и предположим, что она ложна. Другими словами, $(\exists x_0)\, c(x_0)\overline{a}(x_0)$, то есть одновременно $c(x_0) = 1$ и $a(x_0) = 0$. Подставим x_0 в формулу в левой части:

$$a(x_0)b(x_0) \vee c(x_0) = a(x_0)b(x_0) \vee a(x_0)c(x_0),$$

то есть $1 = 0$ – противоречие, поскольку левая часть выполняется не для всех x.

Достаточность (⇐). Нужно доказать, что если истинна правая часть, что истинна и левая. Но правая часть истинна, если для всех x выполняется $c(x) = 0$ или $a(x) = 1$. Простой проверкой убеждаемся, что левая часть верна для обоих вариантов.

1.2.3. Декартово произведение

Часто при рассмотрении множества из двух элементов $\{a, b\}$ важно учитывать порядок взаимного расположения этих элементов друг относительно друга. Таким образом, возникает потребность в новом термине – упорядоченная пара. Хотя понятие упорядоченности интуитивно понятное, мы приведем его строгое определение, основанное на уже известных нам понятиях множества и подмножества.

Определение 1.2.3 (Куратовский, 1921). *Упорядоченной парой элементов a и b*, обозначается (a, b), называется множество $\{\{a\}, \{a, b\}\}$.

Из данного определения следует важное утверждение, в котором формулируется отличие упорядоченной пары от неупорядоченной.

Теорема 1.2.1. $(a, b) = (c, d) \Leftrightarrow (a = c) \wedge (b = d)$.

Доказательство. *Достаточность*. Если $a = c$ и $b = d$, то $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$, то есть, по определению, $(a, b) = (c, d)$.

Необходимость. По определению, имеем

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}.$$

Рассмотрим два случая: $a = b$ и $a \neq b$. Пусть $a = b$, тогда

$$\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, a\}\} = \{\{a\}\}.$$

Значит, $\{\{c\}, \{c, d\}\} = \{\{a\}\}$, то есть $\{c\} = \{c, d\} = \{a\}$, откуда следует, что $c = a$ и $d = a$. По предположению, $a = b$, значит $b = d$.

Рассмотрим случай $a \neq b$. От противного: предположим, что $a \neq c$. Тогда $\{a\} \neq \{c\}$, значит $\{a\} = \{c, d\}$, значит $c = d = a$, откуда

$$\{\{c\}, \{c, d\}\} = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}.$$

Но тогда $\{\{a\}, \{a, b\}\}$ тоже равно $\{\{a\}\}$, то есть $b = a$, что противоречит предположению, что $a \neq b$. Таким образом, $a = c$, откуда $\{a\} = \{c\}$ и $\{a, b\} = \{c, d\}$, то есть $\{a, b\} = \{a, d\}$, откуда $d = b$. ■

Аналогичным образом определяется *упорядоченный набор длины* n:

$$(a_1, \dots, a_n) = \{\{a_1\}, \{a_1, a_2\}, \dots, \{a_1, \dots, a_n\}\}.$$

В наборе $(a_1, \dots, a_n)$ элемент a_i называется его *i-й компонентой* или *i-й координатой*. Для упорядоченного набора часто используют термин *вектор* или *кортеж*, а вместо круглых скобок используют угловые: $\langle a_1, \dots, a_n \rangle$.

Определение 1.2.4. *Декартовым произведением* множеств A и B, обозначается $A \times B$, называется множество всех упорядоченных пар таких, что первый элемент каждой пары принадлежит множеству A, а второй – множеству B:

$$A \times B = \{(a, b) \mid (a \in A) \wedge (b \in B)\}.$$

Например, для множеств $A = \{1, 2, 3\}$ и $B = \{a, b\}$ их декартово произведение есть множество

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

Декартово произведение n множеств определяется аналогично:

$$A_1 \times \ldots \times A_n = \left\{ (a_1, \ldots, a_n) \;\middle|\; \bigwedge_{i=1}^{n} (a_i \in A_i) \right\}.$$

Степенью множества A называется декартово n-кратное произведение этого множества самого на себя:

$$A^n = \underbrace{\{A \times \ldots \times A\}}_{n \text{ раз}}.$$

1.2.4. Отношения

Определение 1.2.5. *Бинарным отношением* R из множества A в множество B называется подмножество декартова произведения этих множеств: $R \subseteq A \times B$.

Множество D_R первых элементов пар, входящих в R, называется *областью определения* бинарного отношения:

$$D_R = \{\, a \in A \mid (a, b) \in R \,\}.$$

Множество V_R вторых элементов этих пар называется *множеством значений* бинарного отношения:

$$V_R = \{\, b \in B \mid (a, b) \in R \,\}.$$

Часто для краткости вместо $(a, b) \in R$ пишут aRb. Если $A = B$, то говорят, что R есть отношение *на множестве* A.

Рассмотрим два примера.

1. Из арифметики нам хорошо известны отношения на множестве чисел, обозначаемые привычными символами: $=, \neq, <, >, \leq, \geq$. В частности, отношение $<$ на множестве $\mathbb{N}$ представляет собой множество пар вида

$$\{(n, m) \mid (\exists k)(k \in \mathbb{N}) \wedge (m = n + k)\}.$$

2. Отношения $\subset, \subseteq, =$ определяются на множествах. Например, по определению, $\subseteq$ есть множество пар вида

$$\{\, (A, B) \mid (\forall x)(x \in A) \Rightarrow (x \in B) \,\}.$$

Бинарные отношения называют также 2-местными. По аналогии, n-*местным* или n-*арным* отношением R на множествах $A_1, \ldots, A_n$ называется подмножество декартова произведения этих множеств:

$$R \in A_1 \times \ldots \times A_n.$$

Далее мы будем рассматривать только бинарные отношения.

Определение 1.2.6. Пусть $R_1 \subseteq A \times C$ и $R_2 \subseteq C \times B$ – два отношения. *Композицией отношений* R_1 и R_2 называется отношение $R \subseteq A \times B$, которое определяется следующим образом:

$$R = \{(a, b) \mid (a \in A) \wedge (b \in B) \wedge (\exists c \in C)((a, c) \in R_1 \wedge (c, b) \in R_2)\}.$$

Если отношение R есть композиция отношений R_1 и R_2, то пишут

$$R = R_2 \circ R_1.$$

Степенью отношения R называется композиция вида

$$R^n = \underbrace{R \circ \ldots \circ R}_{n \text{ раз}}.$$

Рассмотрим пример композиции родственных отношений. На рисунке 1.2.2 изображена схема, где пунктиром обозначены пары, составляющие отношение «зять- теща», которое является композицией двух отношений – «жених-невеста» и «невеста-мама».

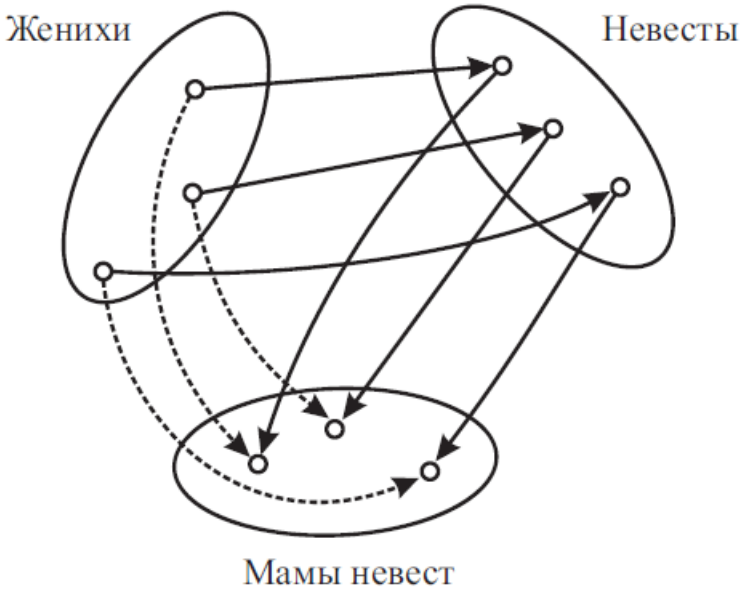

Рисунок 1.2.2 Композиция родственных отношений:
«зять-теща» = «дочка-мама» ∘ «жених-невеста».

1.2.5. Типы и свойства отношений

Определение 1.2.7. Пусть R – отношение на множестве A. Тогда отношение R называется

пустым,	если	$R = \emptyset$,
рефлексивным,	если	$(\forall a)\ aRa$,
антирефлексивным,	если	$(\forall a)(\forall b)\ aRb \Rightarrow a \neq b$,
симметричным,	если	$(\forall a)(\forall b)\ aRb \Rightarrow bRa$,
антисимметричным,	если	$(\forall a)(\forall b)\ aRb \wedge bRa \Rightarrow a = b$,
транзитивным,	если	$(\forall a)(\forall b)(\forall c)\ aRc \wedge cRb \Rightarrow aRb$,
линейным,	если	$(\forall a)(\forall b)\ a \neq b \Rightarrow aRb \vee bRa$,
универсальным,	если	$R = A^2$.

Например, отношение $\leq$ на множестве $\mathbb{N}$ является рефлексивным, антисимметричным, транзитивным и линейным. Отношение $\subset$ на множестве 2^M является антирефлексивным, антисимметричным и транзитивным, но не является линейным.

Отношение $R^{-1} = \{\ (b,a) \mid (a,b) \in R\ \}$ называется *обратным* к отношению R, а отношение $\overline{R} = \{\ (a,b) \mid (a,b) \notin R\ \}$ – *дополнением* к отношению R.

Определение 1.2.8. Рефлексивное и транзитивное отношение на множестве A называется *предпорядком* на A. Отношение предпорядка, обладающее свойством симметричности, называется отношением *эквивалентности*. Если R – отношение эквивалентности и $(a,b) \in R$, то пишут $a \sim b$ или $a \equiv b$ и говорят, что a и b *эквивалентны по отношению* R.

Примерами отношения эквивалентности являются отношение конгруэнтности фигур на плоскости, отношение параллельности прямых, отношение равенства чисел и множеств.

Еще один пример связан с понятиями покрытия и разбиения множеств. *Покрытием* множества X называется семейство подмножеств $\mathcal{X} = \{X_1, \ldots, X_k\}$ таких, что $X \subseteq \bigcup_{i=1}^{n} X_i$. Если при этом $X_i \cap X_j = \emptyset$ для $i \neq j$, и $X = \bigcup_{i=1}^{n} X_i$, то семейство $\mathcal{X}$ называется *разбиением* множества X.

Верно следующее утверждение: всякое отношение эквивалентности на множестве X определяет разбиение множества X. И наоборот, всякое разбиение множества X, не содержащее пустых элементов, определяет отношение эквивалентности. Другими словами, на любом множестве X можно задать отношение эквивалентности, построив произвольное разбиение этого множества. Элементы X, относящиеся к одному подмножеству, входящему в разбиение, будут считаться эквивалентными.

Определение 1.2.9. Отношение предпорядка, обладающее свойством антисимметричности, называется отношением *частичного* порядка. Если R – отношение частичного порядка на множестве X, то пара (X, R) называется *частично-упорядоченным множеством*.

Если при этом отношение R является линейным, то множество (X, R) называют *линейно упорядоченным*.

Отношение $\subseteq$ на множестве 2^X всех подмножеств множества X является отношением частичного порядка, а отношение $\leq$ на множестве $\mathbb{N}$ натуральных чисел является отношением линейного порядка. Читателю предлагается доказать оба эти утверждения самостоятельно.

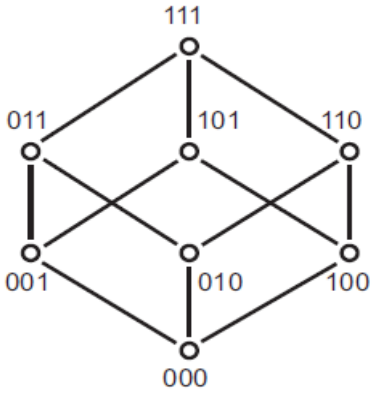

Рисунок 1.2.3 Диаграмма Хассе частично-упорядоченного множества $(\mathbb{B}^3, \leq)$

Частично-упорядоченное множество (X, R) удобно изображать в виде диаграммы Хассе (рисунок 1.2.3), где точки, представляющие элементы $a, b \in X$, соединены отрезком тогда и только тогда, когда $(a, b) \in R$ и не существует $c \in X$ такого, что $(a, c) \in R$ и $(c, b) \in R$.

1.2.6. Функции

Определение 1.2.10. *Функцией* или *отображением* называется отношение f из множества A в множество B такое, что для любого элемента $a \in A$ существует единственный элемент $b \in B$ такой, что $(a, b) \in f$:

$$(\forall a \in A)(\exists b \in B)(\forall c \in B)\big((a, b) \in f\big) \wedge \big((a, c) \in f\big) \Rightarrow (b = c).$$

Такое свойство отношения f называется *однозначностью* или *функциональностью*. Заметим, что если f – функция, то по определению $D_f = A$.

Говорят, что функция f *отображает* множество A в множество B и используют запись $f : A \to B$. Если $(a, b) \in f$, то пишут $b = f(a)$. При этом элемент $a \in A$ называется *аргументом*, а $b \in B$ – *значением*[1] функции f.

Функция вида $f : A_1 \times \ldots \times A_n \to B$ называется *функцией n аргументов*. Если $\big((a_1, \ldots, a_n), b\big) \in f$, то пишут $b = f(a_1, \ldots, a_n)$.

Определение 1.2.11. Пусть $f : A \to B$. Тогда f называется:

- *инъективной* (*инъекцией*), если

$$f(a) = f(b) \Rightarrow a = b$$

(каждому значению функции соответствует ровно один ее аргумент);

[1] Другие названия: a – *прообраз* b, а b – *образ* a. Или: a – *независимая переменная*, а b – *зависимая переменная*.

- *сюръективной* (*сюръекцией*), если $V_f = B$, то есть

$$(\forall b \in B)(\exists a \in A)\left((a,b) \in f\right)$$

(говорят, что сюръективная функция отображает множество A *на* множество B);

- *биективной* (*биекцией* или *взаимно-однозначной*), если она является одновременно инъективной и сюръективной.

Теорема 1.2.2. *Если f – инъекция, то $a \neq b \Rightarrow f(a) \neq f(b)$.*

Доказательство. Утверждение теоремы есть контрапозиция формулы, используемой в определении инъекции. ■

Рисунок 1.2.4 иллюстрирует отличия между отношениями и функциями различных типов.

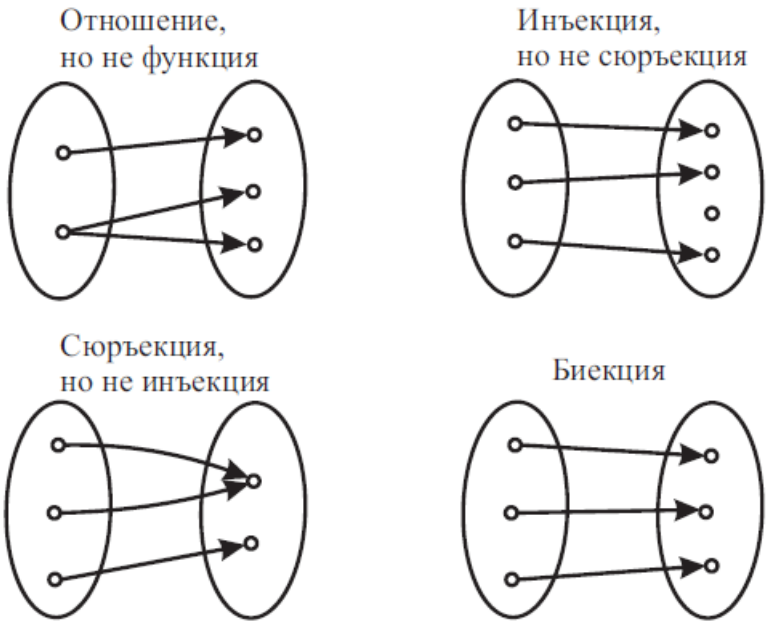

Рисунок 1.2.4 Типы функций

Пусть $f : A \to B$ – функция. Тогда отношение f^{-1}, обратное к отношению f, называется функцией, *обратной* к f. По определению,

$$y = f(x) \Leftrightarrow x = f^{-1}(y).$$

Теорема 1.2.3. *Пусть функция $f: A \to B$ – биекция. Тогда f^{-1} – тоже биекция и $D_{f^{-1}} = B$.*

Доказательство. Покажем, что

1. $D_{f^{-1}} = B$.
2. f^{-1} есть функция.

3. f^{-1} есть инъекция.

4. f^{-1} есть сюръекция.

(1) По условию f – сюръекция. Значит, $(\forall b \in B)(\exists a \in A)(a,b) \in f$, откуда $(\forall b \in B)(\exists a \in A)(b,a) \in f^{-1}$, то есть $D_{f^{-1}} = B$.

(2) Пусть $(c,a) \in f^{-1}$ и $(c,b) \in f^{-1}$. Тогда $(a,c) \in f$ и $(b,c) \in f$, то есть $f(a) = c$ и $f(b) = c$. Поскольку f – инъекция, значит $a = b$, откуда заключаем, что f^{-1} есть функция по определению.

(3) Пусть $f^{-1}(b) = a$ и $f^{-1}(c) = a$, то есть $(b,a) \in f^{-1}$ и $(c,a) \in f^{-1}$. Тогда $(a,b) \in f$ и $(a,c) \in f$. Поскольку f – функция, имеем $b = c$. Значит f^{-1} – инъекция.

(4) Имеем: $D_f = A$, значит $(\forall a \in A)(\exists b \in B)\ (a,b) \in f$, то есть $(b,a) \in f^{-1}$, значит f^{-1} – сюръекция по определению. ■

Пусть $f: A \to B$ и $g: B \to C$ – две функции. Композиция отношений f и g называется *композицией функций*: $g \circ f : A \to C$. Из определения композиции отношений следует, что $(g \circ f)(a) = g\big(f(a)\big)$.

Например, пусть $f(x) = x^2 + 3$ и $g(y) = \sqrt{y}$. Тогда

$$(g \circ f)(x) = g\big(f(x)\big) = \sqrt{\{x^2 + 3\}}.$$

Теорема 1.2.4. *Пусть $f: A \to C$ и $g: C \to B$ – биекции. Тогда*

1. $(\forall a \in A)(f^{-1} \circ f)(a) = a$.
2. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Доказательство. Первое утверждение следует непосредственно из определения обратной функции. Докажем второе утверждение. Действительно,

$$\begin{aligned}(g \circ f)^{-1} &= \{\,(b,a) \mid (a,b) \in g \circ f\} \\ &= \big\{\,(b,a) \mid (\exists c \in C)\big((a,c) \in f\big) \wedge \big((c,b) \in g\big)\big\} \\ &= \big\{\,(b,a) \mid (\exists c \in C)\big((b,c) \in g^{-1}\big) \wedge \big((c,a) \in f^{-1}\big)\big\} \;=\; f^{-1} \circ g^{-1}.\ \blacksquare\end{aligned}$$

1.2.7. Мощность множества

В предыдущих разделах мы специально не рассматривали такое важное свойство множества как его размер, и для этого были серьезные основания. Если размер конечного множества можно определить как число входящих в него элементов, то как поступить с бесконечным множеством? Можно ли сравнивать между собой бесконечные множества? Можно ли ответить на вопрос, каких чисел больше – натуральных или действительных?

Для того, чтобы сравнивать бесконечные множества нам потребуется ввести понятие мощности, основанное на уже определенных ранее понятиях отношения

эквивалентности и взаимно-однозначной функции. Начнем с определения конечного множества и его мощности.

Определение 1.2.12. Пустое множество есть *множество мощности* 0. Если существует взаимно-однозначное соответствие между множеством A и множеством $\{1, \dots, n\}$, то говорят, что A есть *конечное множество мощности* n и пишут $|A| = n$.

Например, множество $A = \{a, b, c\}$ есть множество мощности 3 ($|A| = 3$), так как существует биекция из A в множество $\{1, 2, 3\}$. Таким образом, для конечных множеств понятие мощности естественно ассоциируется с привычным понятие числа элементов, входящих в множество.

Определение 1.2.13. Непустое множество, не являющееся конечным, называется *бесконечным*.

Другими словами, бесконечное множество – это такое непустое множество, для которого не существует биективного отображения в множество $\{1, \dots, n\}$ ни для какого натурального n.

Определение 1.2.14. Множества A и B называются *равномощными*, если существует биекция из A в B.

Введем для множеств отношение эквивалентности M таким образом, что эквивалентными буду считаться равномощные множества. (Докажите, что отношение равномощности есть отношение эквивалентности.) Тогда мощность множества A можно определить не как *число* элементов, а как *класс* всех множеств, эквивалентных A относительно M.

Определение 1.2.15. Множество, равномощное множеству $\mathbb{N}$ натуральных чисел, называется *счетным*.

Другими словами, все элементы счетного множества A можно занумеровать натуральными числами и определить таким образом бесконечную последовательность вида

$$(a_n)_{n=1}^{\infty} = a_1, a_2, \dots$$

Теорема 1.2.5. *Любое подмножество счетного множества либо конечное, либо счётное.*

Доказательство. Пусть A – счетное множество и $B \subseteq A$. По условию теоремы существует бесконечная последовательность $(a_n)_{n=1}^{\infty}$, включающая все элементы множества A. Определим отображение $\varphi : \mathbb{N} \to B$ следующим образом. Пусть $\varphi(1) = a_{m_1}$, где m_1 – минимальный номер элемента последовательности (a_n), такой что $a_{m_1} \in B$. Пусть далее $\varphi(2) = a_{m_2}$, где m_2 – следующий после m_1 номер такой, что $a_{m_2} \in B$ и т. д. Очевидно, φ – биекция. Если существует такое число $N > 0$, что $B = \{a_{m_i} \in A \mid 1 \le i \le N\}$, то, по определению, B – конечное множество мощности N, если нет, то B – счетное. ■

Теорема 1.2.6. *Если A и B – счетные множества, то их объединение* A ∪ B *тоже счетное.*

Доказательство. Сначала докажем данное утверждение для случая, когда A и B – непересекающиеся множества. По условию теоремы существуют биективные отображения $\alpha : \mathbb{N} \to A$ и $\beta : \mathbb{N} \to B$. Определим новое биективное отображение $\gamma : \mathbb{N} \to A \cup B$ следующим образом:

$$\gamma(n) = \begin{cases} \alpha\left(\dfrac{n+1}{2}\right), & \text{если } n \text{ нечётное,} \\ \beta\left(\dfrac{n}{2}\right), & \text{если } n \text{ чётное.} \end{cases}$$

В частности, $\gamma(1) = \alpha(1), \gamma(2) = \beta(1), \gamma(3) = \alpha(2), \gamma(4) = \beta(2)$ и т. д.

Заметим, что бесконечная последовательность $\gamma(n)$ может быть построена также в случае, когда одно из множеств, например A, является конечным. Действительно, пусть $|A| = N_A$. Тогда, для $n = 1, \dots, 2N_A$ вычислим значения $\gamma(n)$ по формулам, приведенным выше, а начиная с $n = 2N_A + 1$, положим

$$\gamma(n) = \beta(n - N_A).$$

Пусть теперь A и B – произвольные счетные множества. Верно соотношение $A \cup B = (A \backslash B) \cup B$, где $A \backslash B \subset A$, а множества $A \backslash B$ и B не пересекаются. Из теоремы 1.2.5 следует, что множество $A \backslash B$ конечное или счетное. Значит, множество $A \cup B$ тоже счетное. ■

Теорема 1.2.7. *Если* S *– счетное множество, то множество* S × S *также счетное.*

Доказательство. Покажем сначала, что множество $\mathbb{N} \times \mathbb{N}$ счетно. Построим взаимно-однозначное соответствие $\varphi : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ следующим образом. Положим $\varphi(1) = (1, 1)$. Пусть $\varphi(i) = (m, n)$ для некоторого $i \geq 1$. Тогда

$$\boldsymbol{\varphi(i+1)} = \begin{cases} \boldsymbol{(m+1, n-1)}, & \text{если } \boldsymbol{n \geq 2}, \\ \boldsymbol{(1, m+n)} & \text{иначе.} \end{cases}$$

Определенная таким образом функция перечисляет по порядку пары с одинаковой суммой элементов, равной сначала $2 = (1 + 1)$, затем $3 = (1 + 2) = (2 + 1)$, и т. д. (см. рисунок 1.2.5), и является биективной. Следовательно, множество $\mathbb{N} \times \mathbb{N}$ счетно. Установим теперь взаимно-однозначное соответствие между этим множеством и множеством $S \times S$. Поскольку множество S – счетное, существует биекция $\theta : \mathbb{N} \to S$. Определим искомое отображение $\Theta : \mathbb{N} \times \mathbb{N} \to S \times S$ как $\Theta\big((m, n)\big) = \big(\theta(m), \theta(n)\big)$. ■

Теорема 1.2.8. *Множество* Q_+ *положительных рациональных чисел счетное.*

Доказательство. Из алгебры известно, что любое положительное рациональное число представимо единственным образом в виде дроби $\frac{p}{q}$, где p и q – взаимно простые натуральные числа.

Другими словами, существует биективное отображение множества Q_+ на подмножество M множества $\mathbb{N} \times \mathbb{N}$, состоящее из пар вида (p, q), образованных взаимно простыми числами. Из теорем 1.2.5 и 1.2.7 следует, что множество M счетное. Значит множество Q_+ тоже счетное. ■

Возникает вопрос, а существуют ли вообще множества, не являющиеся счетными? Ответ дает следующая теорема.

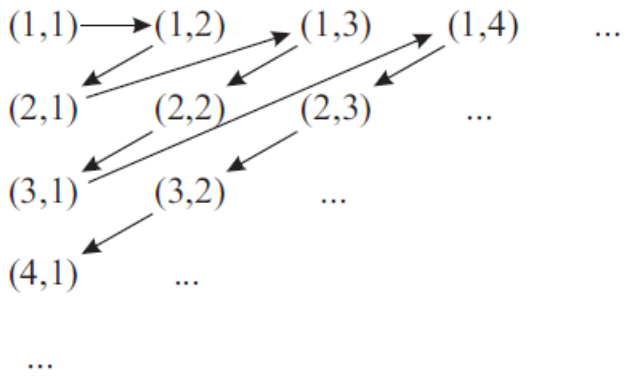

Рисунок 1.2.5 Последовательность элементов множества $\mathbb{N} \times \mathbb{N}$

Теорема 1.2.9. Множество $I = \{ x \mid (x \in \mathbb{R}) \wedge (0 < x < 1) \}$ не является счетным.

Доказательство. Описанный ниже метод доказательства называется *диагональным методом Кантора*. Известно, что каждому действительному числу из интервала $(0,1)$ соответствует одна и только одна бесконечная десятичная дробь вида $0.a_1a_2$ ... с бесконечным числом отличных от нуля цифр (конечные десятичные дроби тоже имеют бесконечное представление, например, $0.123 = 0.122999$ ...).

Предположим, что теорема не верна и существует взаимно-однозначное соответствие между множествами $\mathbb{N}$ и I. Тогда числа из I можно выписать по порядку:

$$\begin{aligned} a_1 &= 0.a_{11}\, a_{12}\, a_{13} \ldots a_{1k} \ldots, \\ a_2 &= 0.a_{21}\, a_{22}\, a_{23} \ldots a_{2k} \ldots, \\ \ldots &\quad \ldots\ldots\ldots\ldots\ldots\ldots \\ a_k &= 0.a_{k1}\, a_{k2}\, a_{k3} \ldots a_{kk} \ldots, \\ \ldots &\quad \ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Построим теперь действительное число $b = 0.b_1\, b_2\, b_3$ ..., выбирая цифры b_i так, чтобы выполнялось условие $b_i \neq a_{ii}$. Получается, что, с одной стороны,

число b принадлежит интервалу $(0,1)$, а с другой – оно не совпадает ни с одним из чисел a_k из этого интервала, так как не совпадают их k-е разряды b_k и a_{kk}. Полученное противоречие доказывает теорему. ■

Определение 1.2.16. Бесконечные множества, не являющиеся счетными, называются *несчетными*. Множества, равномощные множеству I, называются множествами *мощности континуум*.

Из теоремы 1.2.9 следуют важные утверждения.

Следствие 1.2.1. *Множество* $\mathbb{R}$ *действительных чисел несчетно.*

Действительно, если бы $\mathbb{R}$ было счетным, то, согласно теореме 1.2.5, любое его подмножество, включая I, должно быть счетным.

Предлагаем читателю доказать самостоятельно следующие утверждения.

Следствие 1.2.2. *Множество иррациональных чисел несчетно.*

Следствие 1.2.3. *Множество* 2^{A} *всех подмножеств любого счетного множества* A *несчетно.*

(Подсказка: рассмотрите взаимно-однозначное соответствие между множеством 2^A и множеством бесконечных 0-1-векторов и примените к этим векторам диагональный метод Кантора).

1.2.8. Наивная теория множеств

В 1901 году британский логик Бертран Рассел сформулировал парадокс, относящийся к бесконечным множествам. Звучит он следующим образом. Все множества можно разбить на два типа: те, которые содержат себя в качестве элемента, и все остальные. Например, множество всех идей само по себе является идеей, поэтому оно содержит себя в качестве элемента. Другой пример – каталог всех каталогов, который сам тоже является каталогом, или контейнер всех контейнеров.

Рассмотрим теперь *множество всех множеств, не содержащих себя в качестве элемента*. Обозначим его через R. Парадокс проявляется в попытке ответить на вопрос, к какому из двух типов относится R. Действительно, если $R \in R$, то, по определению, $R \notin R$. И наоборот, если $R \notin R$, то $R \in R$.

Вариантом парадокса Рассела является *парадокс деревенского парикмахера:* «Жил был в деревне парикмахер, который брил только тех, кто не брил сам себя. Вопрос: брил ли этот парикмахер сам себя?» Оба ответа – да и нет – неверны. Конечно, можно просто заявить, что такого парикмахера просто не может существовать, так как описывающие его свойства противоречивы. Но в варианте с множеством R дело обстоит намного серьезнее, поскольку речь идет о множестве, которое описывается с помощью простого предиката. Поначалу, по словам немецкого ученого Дэвида Гильберта, парадокс Рассела был воспринят математическим миром как катастрофа.

Дальнейший анализ этого парадокса привел математиков к пониманию того, что в нем неявно используется аксиома, согласно которой для *любого* одноместного предиката $P(x)$ верна формула

$$(\exists Y)(\forall x)(x \in Y) \Leftrightarrow P(x).$$

Иными словами, для любого предиката P всегда найдется множество Y, которое он описывает.

В случае с парадоксом Рассела множество R множеств, не содержащих себя в качестве элемента, описывается предикатом $P(x) = x \notin x$. То есть аксиома утверждает, что верна формула

$$(\exists R)(\forall x)(x \in R) \Leftrightarrow (x \notin x).$$

Но если подставить вместо x само множество R, то получим противоречие $(R \in R) \Leftrightarrow (R \notin R)$.

Отсюда следует, что для задания множества годится не любой предикат. Теория множеств, использующая указанную выше аксиому, получила обидное название *наивной теории множеств*. Позже попытки избавить теорию множеств от подобных парадоксов привели к пересмотру ее аксиоматики, одним из результатов которого является, в частности, теория множеств Цермело-Френкеля, рассмотрение которой лежит за рамками нашего курса.

1.3. ЭЛЕМЕНТЫ КОМБИНАТОРИКИ

Изучая теорию множеств, мы умышленно избегали давать количественные характеристики множеств и отношений. Исследованием этих характеристик занимается специальная область дискретной математики – *комбинаторика*.

1.3.1. Основной принцип комбинаторики

Рассмотрим следующую задачу: сколько существует различных вариантов перелета из Минска в Нью-Йорк, если существуют n_1 авиарейсов из Минска в Варшаву, n_2 рейсов из Варшавы в Лондон и n_3 рейсов из Лондона в Нью-Йорк? Обозначим через $A = \{a_1, \dots, a_{n_1}\}$ авиарейсы из Минска в Варшаву, через $B = \{b_1, \dots, b_{n_2}\}$ – авиарейсы из Варшавы в Лондон и через $C = \{c_1, \dots, c_{n_3}\}$ – авиарейсы из Лондона в Нью-Йорк. Очевидно, решение задачи сводится к подсчету элементов декартова произведения $A \times B \times C$, или, другими словами, числа всевозможных троек вида (a_i, b_j, c_k), равного $n_1 \times n_2 \times n_3$.

Сформулируем это решение в виде общего утверждения.

Утверждение 1.3.1 (Основной принцип комбинаторики). *Пусть требуется выполнить k действий, причем i-е действие можно выполнить n_i способами. Тогда число способов выполнить все k действий равно*

$$n_1 \times \dots \times n_k = \prod_{i=1}^{k} n_i.$$

Из этого простого принципа следует ряд полезных утверждений, которые нам потребуются в дальнейшем.

Следствие 1.3.1. *Верны следующие соотношения*:

1. $|\mathbb{B}^n| = 2^n$,
2. $|2^M| = 2^{|M|}$,
3. $|A_1 \times \dots \times A_n| = \prod_{i=1}^{n} |\mathrm{A_i}|$ (*правило произведения*),
4. $|A^n| = |A|^n$.

Доказательство. Формула (1) следует непосредственно из основного принципа комбинаторики: действительно, число различных булевых векторов, то есть векторов, компоненты которых могут принимать только два значения – 0 или 1, равно 2^n.

Согласно формуле (2), число всех подмножеств n-множества тоже равно 2^n. Покажем, что существует биекция между подмножествами n-множества и булевыми векторами длины n. Для этого рассмотрим произвольный 0-1-вектор $(a_1, \dots, a_n)$ и поставим ему в соответствие подмножество $\{i_1, \dots, i_m\}$, $0 \le m \le n$, n-множества M по следующему правилу: $i_j \in M$, если $a_{i_j} = 1$, и $i_j \notin M$, если

$a_{i_j} = 0$. Например, для множества $M = \{ 1, 2, 3 \}$ данное соответствие выглядит следующим образом:

$\emptyset$	$(0, 0, 0)$
$\{1\}$	$(1, 0, 0)$
$\{2\}$	$(0, 1, 0)$
$\{3\}$	$(0, 0, 1)$
$\{1, 2\}$	$(1, 1, 0)$
$\{1, 3\}$	$(1, 0, 1)$
$\{2, 3\}$	$(0, 1, 1)$
$\{1, 2, 3\}$	$(1, 1, 1)$

Очевидно, что построенное таким образом отображение биективно, поэтому число всех подмножеств n-множества равно числу всех булевых векторов длины n, то есть 2^n.

Равенства (3) и (4) непосредственно следуют из основного принципа комбинаторики. ■

Утверждение 1.3.2 (Правило суммы). *Для разбиения* $\{ X_1, \dots, X_k \}$ *множества* X *справедливо равенство*

$$|X| = \sum_{i=1}^{n} |X_i|.$$

Утверждение 1.3.3 (Мощность объединения множеств).

$$|X_1 \cup X_2| = |X_i| + |X_2| - |X_1 \cap X_2|.$$

Доказательство. Нетрудно показать, что

$$X_1 \cup X_2 = (X_1 \backslash X_2) \cup (X_2 \backslash X_1) \cup (X_1 \cap X_2).$$

Поскольку $X_1 \backslash X_2$, $X_2 \backslash X_1$ и $X_1 \cap X_2$ – непересекающиеся множества, из правила суммы имеем

$$|X_1 \cup X_2| = |X_1 \backslash X_2| + |X_2 \backslash X_1| + |X_1 \cap X_2|. \qquad (1.3.1)$$

С другой стороны,

$$X_1 = (X_1 \backslash X_2) \cup (X_1 \cap X_2) \Rightarrow |X_1 \backslash X_2| = |X_1| - |X_1 \cap X_2|,$$
$$X_2 = (X_2 \backslash X_1) \cup (X_1 \cap X_2) \Rightarrow |X_2 \backslash X_1| = |X_2| - |X_1 \cap X_2|.$$

Подставив полученные выражения в равенство (1.3.1), получим утверждение теоремы. ■

Это утверждение является частным случаем общего принципа «включения и исключения», дающего формулу для подсчета элементов объединения любого количества множеств.

1.3.2. Размещения, перестановки и сочетания

В задачах комбинаторного анализа интерес представляют не сами элементы множества, а их количество. Поэтому любое множество, состоящее из n элементов, называют *n-множеством*, а вектор длины n – *n-вектором*. Введем также обозначение для множества первых n натуральных чисел: $[n] = \{1, \dots, n\}$.

Определение 1.3.1. Произвольный m-вектор с координатами из n-множества называется *размещением с повторениями из n элементов по m*.

Например, векторы $(8, 8, 10)$, $(1, 10, 7)$ и $(2, 2, 2)$, состоящие из элементов множества $[10] = \{1, \dots, 10\}$, являются размещениями с повторениями из 10 по 3. Возникает вопрос, сколько всего существует различных размещений с повторениями? Ответ следует непосредственно из основного принципа комбинаторики.

Теорема 1.3.1. *Число различных размещений с повторениями из n элементов по m равно n^m.*

Определение 1.3.2. m-вектор с попарно различными координатами из n-множества называется *размещением из n элементов по m*.

Оценим число P_n^m всех различных размещений из n по m. Но сначала введем важное обозначение, широко применяемое в комбинаторных формулах.

Произведение первых n натуральных чисел, обозначается $n!$, называется *n-факториалом*: $n! = 1 \times \dots \times n$. По определению $0! = 1$.

Факториал – это очень быстро растущая функция:

$$
\begin{aligned}
0! &= 1,\\
1! &= 1,\\
2! &= 2,\\
3! &= 6,\\
4! &= 24,\\
5! &= 120,\\
6! &= 720,\\
7! &= 5040,\\
8! &= 40320,\\
9! &= 362880,\\
10! &= 3628800,\\
&\dots
\end{aligned}
$$

Теорема 1.3.2. *Число различных размещений из n по m равно*

$$P_n^m = n(n-1)\dots(n-m+1) = \frac{n!}{(n-m)!}.$$

Доказательство. Действительно, первый элемент m-вектора можно выбрать n способами. Для каждого из вариантов выбора первого элемента существует ровно $n-1$ вариант выбора второго элемента, не совпадающего с первым. Для каждого из вариантов выбора первых двух элементов существует уже $n-2$ способа выбора третьего элемента и т.д. Таким образом, из основного принципа комбинаторики получаем утверждение теоремы. ■

Рассмотрим пример. По теореме

$$P_3^2 = \frac{3!}{(3-2)!} = 3! = 6.$$

Чтобы убедиться в этом, выпишем всевозможные размещения из 3 по 2 для элементов множества [3]: $(1,2),(1,3),(2,1),(2,3),(3,1),(3,2)$.

Определение 1.3.3. Размещение из n элементов по n называется *перестановкой* n-множества.

Все перестановки данного множества можно получить, выписывая их в виде векторов, отличающихся только порядком следования элементов. Обозначим через P_n число всех перестановок n-множества.

Теорема 1.3.3. $P_n = n!$.

Доказательство следует непосредственно из теоремы 1.3.2. Например, для множества $\{1,2,3\}$ имеем: $P_3 = 3! = 6$. Соответствующие перестановки:

$$(1,2,3),(1,3,2),(2,1,3),(2,3,1),(3,1,2),(3,2,1).$$

Размещения с повторениями и без повторений являются векторами, то есть упорядоченными подмножествами некоторого множества. Оценим теперь число обычных (неупорядоченных) подмножеств.

Определение 1.3.4. m-подмножество n-множества называется *сочетанием из n элементов по m*.

Число различных сочетаний из n по m обозначается C_n^m или $\binom{n}{m}$.

Теорема 1.3.4.

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

Доказательство. Рассмотрим все m-размещения данного n-множества и сгруппируем их таким образом, чтобы в каждую группу входили размещения, отличающиеся друг от друга только порядком своих элементов. Каждой группе можно поставить в соответствие в точности одно m-подмножество (сочетание)

данного n-множества, состоящее из элементов m-размещений, входящих в эту группу. Таким образом, искомое число сочетаний равно числу групп. Имеем: число всех размещений равно P_n^m, число размещений в группе равно числу различных перестановок элементов m-размещения, то есть $m!$, откуда

$$C_n^m = \frac{P_n^m}{m!}. \qquad \blacksquare$$

Подсчитаем число костей домино с попарно различными значениями. Это число равно количеству способов выбора двух разных значений из семи возможных – от нуля («пусто») до шести, то есть числу сочетаний из 7 по 2. Получаем

$$C_7^2 = \frac{7!}{2!\,5!} = \frac{7 \times 6 \times 5!}{2 \times 5!} = \frac{42}{2} = 21.$$

Непосредственно из формулы для числа сочетаний вытекают следующие полезные соотношения:

1. $C_n^m = C_n^{n-m}$, (1.3.2)
2. $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$ (*треугольник Паскаля*) (1.3.3)
3. $\sum_{m=0}^{n} C_n^m = 2^n.$ (1.3.4)

Равенство (1.3.2) очевидно: действительно, достаточно подставить в формулу для числа сочетаний значение $n - m$ вместо m. Эта формула имеет также геометрическую интерпретацию. Рассмотрим так называемый *шахматный город* – прямоугольную сетку размера m на n, где m и n – натуральные числа (рисунок 1.3.1). Возникает вопрос: сколько существует различных путей, ведущих из точки

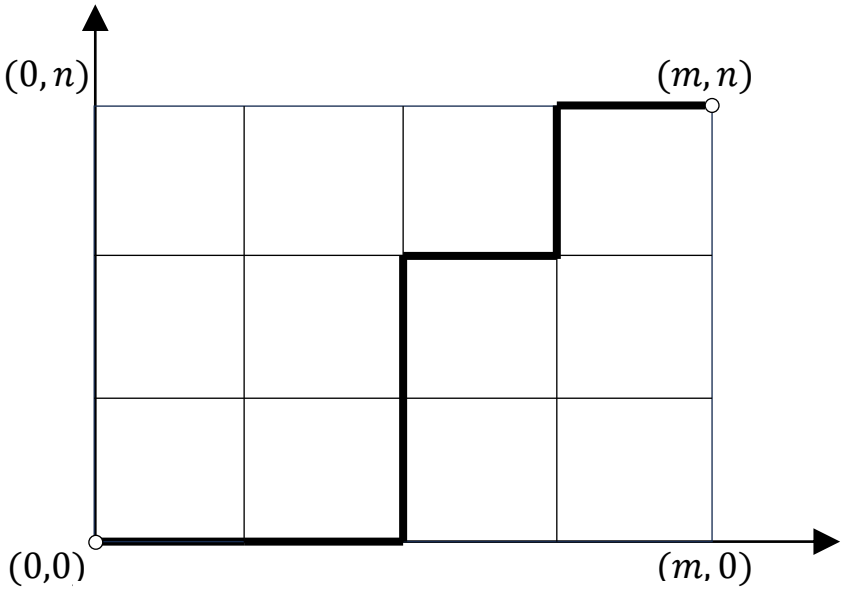

Рисунок 1.3.1 Шахматный город

$(0,0)$ в точку (m,n) и состоящих из горизонтальных и вертикальных отрезков единичной длины, направленных, соответственно, вправо и вверх?

Заметим, что длина любого пути из точки $(0,0)$ в точку (m,n) равна $m+n$, причем любой путь включает ровно m горизонтальных и n вертикальных отрезков. Обозначим через символ h горизонтальный отрезок и через v – вертикальный отрезок. Тогда путь, изображенный на рисунке, можно представить в виде вектора

$$(h,h,v,v,h,v,h).$$

Заметим также, что в этом векторе любой путь однозначно определяется позициями, в которых размещены m символов h среди $m+n$ возможных позиций. В частности, путь на рисунке задается позициями $\{1,2,5,7\}$. Таким образом, существует взаимно-однозначное соответствие между сочетаниями из $m+n$ по m и путями из точки $(0,0)$ в точку (m,n). Значит, число этих путей равно C_{m+n}^{m}.

Все эти рассуждения также применимы для вертикальных отрезков, откуда получаем, что число путей равно C_{m+n}^{n}. Значит, $C_{m+n}^{m}=C_{m+n}^{n}$. Если теперь в эту формулу вместо n подставить $n-m$, получим формулу (1.3.2).

Докажем формулу (1.3.3). Действительно,

$$C_{n-1}^{m}+C_{n-1}^{m-1}=\frac{(n-1)!}{m!\,(n-m-1)!}+\frac{(n-1)!}{(m-1)!\,(n-m)!}=$$

$$=\frac{(n-1)!\,(n-m)+(n-1)!\,m}{m!\,(n-m)!}=\frac{n!}{m!\,(n-m)!}=C_{n}^{m}.$$

Эту формулу можно также доказать, используя идею шахматного города (см. задачу 17 из раздела 2.3).

Формула (1.3.4) следует из определения C_{n}^{m} и оценки числа всех подмножеств n-множества. Действительно, в левой части равенства стоит сумма числа сочетаний размера от 0 до n, то есть *всех* подмножеств данного n-множества, которая, как мы знаем, равна 2^n.

1.3.3. Бином Ньютона

Рассмотрим формулу разложения квадрата суммы, хорошо известную из школьного курса математики:

$$(x+y)^2=x^2+2xy+y^2.$$

Нетрудно заметить, что ее можно переписать, используя числа C_{n}^{m}:

$$(x+y)^2=C_2^0x^2y^0+C_2^1x^1y^1+C_2^2x^0y^2.$$

Оказывается, существует общая закономерность, благодаря которой числа C_{n}^{m} получили специальное название – *биномиальные коэффициенты*.

Теорема 1.3.5 (Формула бинома Ньютона).

$$(x+y)^n = C_n^0 x^n y^0 + C_n^1 x^{n-1} y^1 + \cdots + C_n^n x^0 y^n = \sum_{m=0}^{n} C_n^m x^{n-m} y^m.$$

Доказательство. Используем индукцию по n. Для $n = 1$ имеем:

$$(x+y)^1 = C_1^0 x^1 y^0 + C_1^1 x^0 y^1 = x + y.$$

Равенство верно, следовательно база индукции доказана. Предположим, что формула бинома верна для степени $n-1$. Покажем, что она верна для степени n.

Имеем:

$$(x+y)^n = (x+y)\sum_{m=0}^{n-1} C_{n-1}^m x^{n-m-1} y^m =$$

$$= \sum_{m=0}^{n-1} C_{n-1}^m x^{n-m} y^m + \sum_{m=0}^{n-1} C_{n-1}^{(m+1)-1} x^{n-(m+1)} y^{m+1} =$$

$$= \sum_{m=0}^{n-1} C_{n-1}^m x^{n-m} y^m + \sum_{m=1}^{n} C_{n-1}^{m-1} x^{n-m} y^m =$$

$$= \sum_{m=1}^{n-1} C_{n-1}^m x^{n-m} y^m + C_{n-1}^0 x^n y^0 + \sum_{m=1}^{n-1} C_{n-1}^{m-1} x^{n-m} y^m + C_{n-1}^{n-1} x^0 y^n.$$

Поскольку $C_{n-1}^0 = C_n^0 = 1$ и $C_{n-1}^{n-1} = C_n^n = 1$, а также в силу равенства (1.3.3), последнее выражение преобразуется к виду:

$$C_n^0 x^n y^0 + \sum_{m=1}^{n-1} (C_{n-1}^m + C_{n-1}^{m-1}) x^{n-m} y^m + C_n^n x^0 y^n = \sum_{m=0}^{n} C_n^m x^{n-m} y^m. \qquad \blacksquare$$

Из формулы бинома Ньютона можно получить множество других полезных соотношений, в частности, равенство (1.3.4) – для этого достаточно подставить в формулу значения $x = 1$ и $y = 1$. Если заменить на 1 только y, то получим более компактный вариант биномиальной формулы

$$(x+1)^n = \sum_{m=0}^{n} C_n^m x^m.$$

1.3.4. Мультимножества и перестановки с повторениями

Рассмотрим понятие мультимножества, то есть «множества» с повторяющимися элементами. Обозначим $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Определение 1.3.5. Пусть задано конечное множество X и функция $f: X \to \mathbb{N}_0$. Пара (X, f) называется *мультимножеством* на множестве X с *функцией кратности* f.

Значение $f(x)$, $x \in X$, есть число повторений элемента x в данном мультимножестве. Два мультимножества на множестве X называются *равными*, если равны их функции кратности. Если число элементов X невелико, то для описания мультимножества используют сокращенную запись, указывая кратности всех элементов множества X. Например, мультимножество $\{1, 1, 1, 1, 1\}$ на множестве $\{1, 2, 3\}$ можно записать в виде $\{1^5, 2^0, 3^0\}$. Кроме того, если зафиксировать порядок записи элементов множества X, то для задания мультимножества достаточно просто указать значения функции кратности:

$$\{1, 1, 1, 1, 1\} = \{1^5, 2^0, 3^0\} = (5, 0, 0).$$

Число $\sum_{x \in X} f(x)$ называется *мощностью* мультимножества. Мультимножество мощности n будем называть *n-мультимножеством*.

Определение 1.3.6. Произвольный n-вектор с элементами из множества X, в котором элемент $x \in X$ присутствует ровно $f(x)$ раз, называется *перестановкой на мультимножестве* (X, f) или *перестановкой с повторениями на множестве X с функцией кратности f*.

Рассмотрим n-мультимножество $([m], f)$. Обозначим $k_i = f(i)$, $i = 1, \dots, m$, и оценим число $C_n(k_1, \dots, k_m)$ различных перестановок на этом мультимножестве. Для большей наглядности будем рассматривать не числа от 1 до m, а алфавит из m букв $A = \{a_1, \dots, a_m\}$. Таким образом, требуется подсчитать число всевозможных слов длины n, составленных из букв алфавита A, в которых буква a_i встречается k_i раз.

Выберем в слове длины n подмножество позиций, в которых может стоять буква a_1. По определению, данное подмножество есть сочетание из n по k_1, поэтому число способов расстановки букв a_1 в слове равно $C_n^{k_1}$. Для каждого способа расстановки букв a_1 букву a_2 можно разместить уже в $n - k_1$ позициях, и число вариантов таких размещений равно $C_{n-k_1}^{k_2}$ и т.д. Из основного принципа комбинаторики получаем, что общее число вариантов расстановки всех m букв равно

$$C_n^{k_1} \cdot C_{n-k_1}^{k_2} \cdot \dots \cdot C_{n-k_1-\dots-k_{m-1}}^{k_m} =$$
$$= \frac{n!}{k_1!\,(n-k_1)!} \cdot \frac{(n-k_1)!}{k_2!\,(n-k_1-k_2)!} \cdot \dots \cdot \frac{(n-k_1-\dots-k_{m-1})!}{k_m!\,(n-k_1-\dots-k_m)!} =$$
$$= \frac{n!}{k_1!\,k_2!\,\dots\,k_m!}.$$

Мы доказали следующую теорему:

Теорема 1.3.6. *Число различных перестановок с повторениями равно*

$$C_n(k_1, \dots, k_m) = \frac{n!}{k_1!\, k_2! \dots k_m!}.$$

Числа $C_n(k_1, \dots, k_m)$ называются *полиномиальными коэффициентами*.

Подсчитаем, сколько различных перестановок с повторениями можно составить из букв слова *шалаш*. В этом слове буквы *ш*, *л* и *а* встречаются, соответственно, 2, 2 и 1 раз. По формуле находим

$$C_5(2,2,1) = \frac{5!}{2!\, 2!\, 1!} = 30.$$

1.3.5. Сочетания с повторениями

Обозначим через $\left(\binom{X}{m}\right)$ множество всех m-мультимножеств на множестве X. Например:

$$\left(\binom{[3]}{2}\right) = \{\, \{1,1\}, \{2,2\}, \{3,3\}, \{1,2\}, \{1,3\}, \{2,3\} \,\},$$

или через функции кратности:

$$\left(\binom{[3]}{2}\right) = \{\, (2,0,0), (0,2,0), (0,0,2), (1,1,0), (1,0,1), (0,1,1) \,\}.$$

Определение 1.3.7. m-мультимножество на n-множестве называется *сочетанием с повторениями* из n элементов по m. Число всех сочетаний с повторениями из n по m обозначается H_n^m или $\left(\binom{n}{m}\right)$.

Теорема 1.3.7. $H_n^m = C_{n+m-1}^m$.

Доказательство. Построим взаимно-однозначное соответствие между сочетаниями с повторениями из n по m и сочетаниями без повторений из $n + m - 1$ по m, то есть между элементами множеств $\left(\binom{[n]}{m}\right)$ и $\binom{[n+m-1]}{m}$. Пусть некоторое m-сочетание с повторениями из элементов множества $[n]$ состоит из элементов $a_1, \dots, a_m$, $1 \le a_i \le n$. Поскольку порядок элементов в мультимножестве не имеет значения, предположим, не теряя общности, что эти элементы расположены в порядке неубывания значений: $a_1 \le \dots \le a_m$. Поставим в соответствие этому m-сочетанию с повторениями m-сочетание без повторений $\{\, b_1, \dots, b_m\}$, $1 \le b_i \le n + m - 1$, по следующему правилу:

$$b_i = a_i + i - 1, \quad 1 \le i \le m.$$

Очевидно, построенное отображение является биективным, а элементы построенного m-сочетания попарно различны, поскольку $b_1 < \dots < b_m$. ■

В качестве примера оценки числа сочетаний с повторениями посчитаем, сколько существует костей домино. Каждая кость содержит два из семи возможных значений, которые могут повторяться. Поэтому ответ такой:

$$H_7^2 = C_8^2 = \frac{8!}{2!\,6!} = \frac{56}{2} = 28.$$

1.3.6. Числовые разложения и разбиения

Определение 1.3.8. *m-разложением* натурального числа n называется m-вектор $(x_1, \dots, x_m)$ натуральных чисел, такой что

$$x_1 + \cdots + x_m = n.$$

Например, для $n = 4$ существуют ровно три 3-разложения:

$$1 + 1 + 2,\ \ 1 + 2 + 1,\ \ 2 + 1 + 1.$$

Возникает вопрос: сколько существует различных m-разложений числа n? Представим число n схематично в виде n точек:

$$\cdot\cdot\cdot\cdot \quad (n = 4)$$

Тогда разложение числа n в виде m слагаемых можно изобразить с помощью $m - 1$-го разделителя, которые можно расположить в $n - 1$-й позиции, например:

$$\cdot\,|\,\cdot\cdot\,|\,\cdot \quad (1 + 2 + 1)$$

Значит, число различных m-разложений числа n равно C_{n-1}^{m-1}.

Попутно мы доказали следующую теорему.

Теорема 1.3.8. *Число различных решений в натуральных числах уравнения*

$$x_1 + \cdots + x_m = n$$

равно C_{n-1}^{m-1}.

Определение 1.3.9. *Слабым m-разложением* натурального числа n называется m-вектор целых неотрицательных чисел $(x_1, \dots, x_m)$, такой что

$$x_1 + \cdots + x_m = n.$$

Если в этом уравнении положить $y_i = x_i + 1$, то получим обычное m-разложение числа $n + m$:

$$y_1 + \cdots + y_m = n + m.$$

Примененное здесь отображение векторов $(y_1, \dots, y_m)$ на вектора $(x_1, \dots, x_m)$ биективно, откуда следует, что число различных слабых m-разложений числа n равно C_{n+m-1}^{m-1}.

Например, число слабых 2-разложений числа 3 равно $C_4^1 = 4$:

$$0 + 3,\ \ 3 + 0,\ \ 1 + 2,\ \ 2 + 1,$$

что соответствует числу (обычных) 2-разложений числа 5:

$$1+4,\ \ 4+1,\ \ 2+3,\ \ 3+2.$$

Определение 1.3.10. *m-разбиением* натурального числа n называется m-мультимножество $\{x_1, \dots, x_m\}$ на множестве натуральных чисел, такое что

$$x_1 + \cdots + x_m = n.$$

Разбиение рассматривается как представление числа в виде суммы натуральных слагаемых, порядок следования которых игнорируется. Таким образом, выражения $1+2+1$ и $2+1+1$ задают одно и тоже разбиение.

Обозначим через $p(n)$ число различных разбиений числа $n \in \mathbb{N}$. Например, $p(4) = 5$. Соответствующие разбиения выглядят следующим образом:

$$4,\ \ 3+1,\ \ 2+2,\ \ 2+1+1,\ \ 1+1+1+1.$$

Ответ на вопрос, как вычислить число $p(n)$, был получен лишь в начале XX века. Асимптотическое представление для $p(n)$ было впервые опубликовано английским математиком Г. Харди (1887–1947) и индийским математиком С. Рамануйана (1887–1920), а затем уточнено немецким математиком Г. Радемахером (1892–1969).

Теорема 1.3.9.

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n)\sqrt{k}\,\frac{d}{dn}\left(\frac{\sinh\left(\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right)}{\sqrt{n-\frac{1}{24}}}\right),$$

где

$$A_k(n) = \sum_{\substack{0 \le m < k;\\ m,k-\text{взаимно}\\ \text{простые}}} e^{\pi i \sigma(m,k) - 2\pi i \frac{m}{k}},$$

$\sigma(m,k)$ – сумма Дедекинда:

$$\sigma(m,k) = \frac{1}{4k} \sum_{n=1}^{k-1} \cot\frac{\pi n}{k} \cot\frac{\pi n m}{k}.$$

Как заметил Г. Эндрюс [32], «это необычайное тождество, в котором левой частью служит простая арифметическая функция $p(n)$, а правой – бесконечный ряд, включающий в себя π, квадратные корни, комплексные корни из единицы и производные гиперболических функций...».

1.3.7. Подстановки

Определение 1.3.11. Взаимно однозначная функция $f: X \to X$ называется *подстановкой* на множестве X.

Не ограничивая общности, будем считать, что $X = [n]$. Тогда подстановку удобно записывать в виде таблицы из двух строк: первая строка содержит аргументы функции f, а вторая – ее значения. Например:

$$f = \begin{vmatrix} 1\,2\,3\,4\,5 \\ 3\,5\,4\,1\,2 \end{vmatrix}, \quad g = \begin{vmatrix} 1\,2\,3\,4\,5 \\ 1\,3\,2\,5\,4 \end{vmatrix}.$$

К подстановкам применима операция композиции:

$$g \circ f = \begin{vmatrix} 1\,2\,3\,4\,5 \\ 2\,4\,5\,1\,3 \end{vmatrix}.$$

Функция, обратная к подстановке, называется *обратной подстановкой*. Заметим, что по определению обратная подстановка всегда существует. Для подстановки f имеем:

$$f^{-1} = \begin{vmatrix} 3\,5\,4\,1\,2 \\ 1\,2\,3\,4\,5 \end{vmatrix} = \begin{vmatrix} 1\,2\,3\,4\,5 \\ 4\,5\,1\,3\,2 \end{vmatrix}.$$

Подстановки имеют наглядное графическое представление в виде ориентированных графов (рисунок 1.3.2). *Циклом* подстановки f называется последовательность элементов $x_1, \ldots, x_k$ множества X такая, что

$$f(x_1) = x_2, \ldots, f(x_{k-1}) = x_k, f(x_k) = x_1.$$

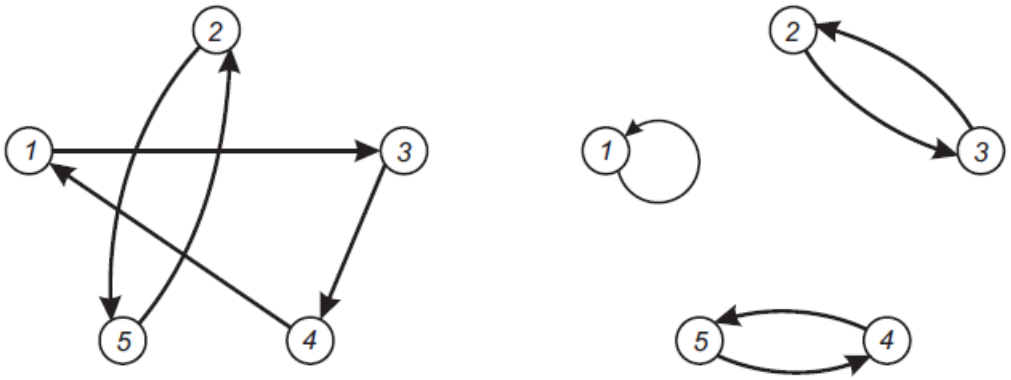

Рисунок 1.3.2 Графы подстановок f и g из приведенных выше примеров: подстановка слева содержит цикл длины 3 и цикл длины 2, подстановка справа содержит цикл длины 1 и два цикла длины 2.

Число k называется *длиной цикла*. Подстановка на n-множестве называется *транспозицией*, если она содержит один цикл длины 2 и $n - 2$ цикла длины 1. Композиция какой-либо подстановки и транспозиции меняет местами два элемента этой подстановки, например:

$$f = \begin{vmatrix} 1\,2\,3\,4\,5 \\ 5\,3\,1\,2\,4 \end{vmatrix}, \quad t = \begin{vmatrix} 1\,2\,3\,4\,5 \\ 1\,\underline{3}\,\underline{2}\,4\,5 \end{vmatrix}, \quad f \circ t = \begin{vmatrix} 1\,2\,3\,4\,5 \\ 5\,\underline{1}\,\underline{3}\,2\,4 \end{vmatrix}.$$

Транспозиция, которая меняет местами соседние элементы i и $i+1$ подстановки, называется *стандартной*.

Не теряя общности, будем считать, что элементы в верхней строке таблицы всегда упорядочены по возрастанию. Тогда элементы в нижней строке представляют собой перестановку множества X. Другими словами, существует взаимнооднозначное соответствие между подстановками на множестве X и перестановками его элементов.

Определение 1.3.12. Пара (x_i, x_j) элементов перестановки называется *инверсией*, если $i < j$ и $x_i > x_j$.

Например, перестановка $(5, 3, 1, 2, 4)$ имеет 6 инверсий. Тождественная перестановка $(1, 2, 3, 4, 5)$ не имеет инверсий.

Обозначим через $I(f)$ число инверсий в перестановке f.

Теорема 1.3.10. *Произвольную перестановку f можно представить в виде композиции $I(f)$ стандартных транспозиций.*

Доказательство. Обозначим через e тождественную подстановку:

$$e = \begin{vmatrix} 1 \dots n \\ 1 \dots n \end{vmatrix}.$$

Если $f = e$, то $I(f) = 0$, и утверждение теоремы верно. Пусть $f \neq e$ и пара $(x_i,\ x_{i+1})$ является инверсией. Тогда соответствующая стандартная транспозиция t_1 удаляет эту инверсию (и только ее): $I(f \circ t_1) = I(f) - 1$. Применив $I(f)$ стандартных транспозиций, получим подстановку, в которой отсутствуют инверсии, то есть тождественную подстановку

$$f \circ t_1 \circ \dots \circ t_{I(f)} = e.$$

Рассмотрим подстановку, обратную к композиции подстановок в левой части данного равенства

$$T^{-1} = \left(t_1 \circ \dots \circ t_{I(f)}\right)^{-1} = t_{I(f)}^{-1} \circ \dots \circ t_1^{-1}$$

и применим ее к обеим его частям

$$\left(f \circ t_1 \circ \dots \circ t_{I(f)}\right) \circ T^{-1} = \ e \circ T^{-1},$$

что равносильно

$$f = t_{I(f)}^{-1} \circ \dots \circ t_1^{-1}. \qquad \blacksquare$$

Идея упорядочения элементов заданной перестановки путем последовательного исключения инверсий соседних элементов заложен в основу простейшего алгоритма сортировки, известного как «метод пузырька». Пары соседних элементов просматриваются и сравниваются между собой, и в случае обнаружения инверсии элементы пары меняются местами. Процесс повторяется до тех пор, пока в данной перестановке не будут исключены все инверсии.

1.4. БУЛЕВЫ ФУНКЦИИ

В современных цифровых устройствах, таких как мобильный телефон или компьютер, информация хранится в двоичном представлении, то есть в виде векторов с элементами из булева множества $\mathbb{B} = \{0, 1\}$. В ходе вычислений функциональные элементы процессора дискретно, периодически с заданным интервалом времени выполняют преобразование одного двоичного вектора длины n в другой двоичный вектор длины m, то есть *преобразуют* информацию. Например, логическое дискретное цифровое устройство, называемое *сумматор*, преобразует вектор длины $2n$, хранящий два n-разрядных целых числа, в вектор длины n, хранящий сумму этих чисел.

Таким образом, возникает задача построения функции вида $F\colon \mathbb{B}^n \to \mathbb{B}^m$ по заданным значениям аргументов, подаваемым на вход, и результирующим значениям, которые должны получаться на выходе. Преобразователь информации, реализующий функцию F, можно изобразить в виде «черного ящика» (рисунок 1.4.1). Решение общей задачи построения нужной функции можно свести к решению несколько более простых задач, заменив функцию F на m функций вида $f_i : \mathbb{B}^n \to \mathbb{B}$, $i = 1, \ldots, m$. Внутренняя схема преобразователя с учетом такой декомпозиции показана на рисунке 1.4.2.

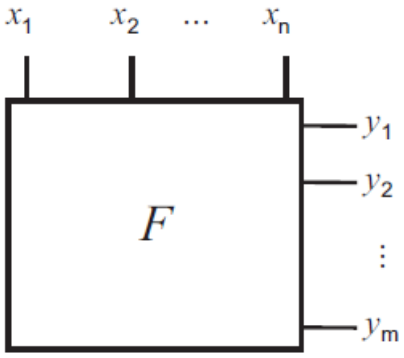

Рисунок 1.4.1 Преобразователь информации в виде «черного ящика»

Определение 1.4.1. Функция вида $f\colon \mathbb{B}^n \to \mathbb{B}$ называется функцией *алгебры логики* или *булевой* функцией (по имени английского математика Джорджа Буля (George Boole, 1815–1864).

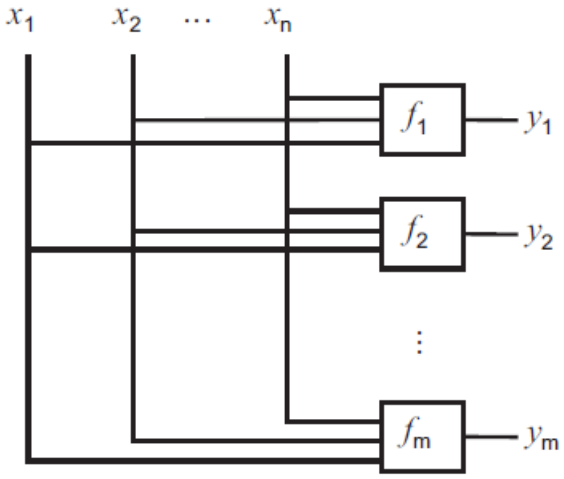

Рисунок 1.4.2 Общая схема преобразователя информации вида $F\colon \mathbb{B}^n \to \mathbb{B}^m$

Множество всех булевых функций от n переменных обозначается P_n. Булеву функцию можно задать таблицей истинности:

x_1	…	x_n	$f(x_1, \dots, x_n)$
0	…	0	$f(0, \dots, 0)$
…	…	…	…
1	…	1	$f(1, \dots, 1)$

Такая таблица содержит 2^n строк, поэтому число различных вариантов заполнения нулями и единицами правого столбца этой таблицы равно 2^{2^n}. Таким образом, число булевых функций от n переменных равно 2^{2^n}.

Определение 1.4.2. Говорят, что булева функция f *существенно зависит от переменной* x_i, если существует набор значений переменных $a_1, \dots, a_n$ такой, что

$$f(a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n).$$

Рассмотрим пример. Пусть булевы функции $f_1(x_1, x_2)$ и $f_2(x_1, x_2)$ заданы следующими таблицами истинности:

x_1	x_2	$f_1(x_1, x_2)$	$f_2(x_1, x_2)$
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1

Для первой функции несущественной является переменная x_2, для второй – переменная x_1: $f_1(x_1, x_2) = \overline{x_1}$, $f_2(x_1, x_2) = x_2$.

Определение 1.4.3. Булевы функции *равны*, если одна из другой получается введением или удалением несущественной переменной.

В дальнейшем будем рассматривать и сравнивать булевы функции, зависящие от одних и тех же переменных (некоторые из которых могут оказаться несущественными).

Среди всего множества булевых функций выделяют множество F_0 *элементарных* булевых функций от одной и двух переменных:

x	0	1	$\overline{x}$
0	0	1	1
1	0	1	0

x	y	0	$\wedge$	$\vee$	$\oplus$	$\mid$	$\downarrow$	$\Rightarrow$	$\Leftrightarrow$	1
0	0	0	0	0	0	1	1	1	1	1
0	1	0	0	1	1	1	0	1	0	1
1	0	0	0	1	1	1	0	0	0	1
1	1	0	1	1	0	0	0	1	1	1

Большинство из этих функций нам известны из раздела 1.1.1, но есть и новые. Функции 0 и 1 называются, соответственно, *константа ноль* и *константа один*. Функция $\mid$ имеет название *штрих Шеффера* или *НЕ-И*, поскольку $x \mid y = \overline{xy}$. Функция $\downarrow$ называется *стрелка Пирса* или *НЕ-ИЛИ*: $x \downarrow y = \overline{x \vee y}$.

Часто для задания булевой функции пользуются *векторным представлением*: вместо всей таблицы истинности данной функции записывают только её правый столбец. Например, импликация записывается в виде (1101), а стрелка Пирса как (1000).

1.4.1. Формулы

Пусть задано некоторое непустое множество булевых функций $F \subseteq P^n$, (например, множество F_0). Рассмотрим индуктивное определение формулы над множеством F.

Определение 1.4.4.

1. Каждая булева функция $f \in F$ называется *формулой над* F.
2. Пусть $f \in F$ и $A_1, \dots, A_n$ – формулы над F. Тогда $f(A_1, \dots, A_n)$ есть *формула над* F. Функция f называется *суперпозицией* формул A_i, а сами формулы A_i – *подформулами* формулы f.
3. Других определений формулы нет.

По определению, любую формулу над F можно представить как суперпозицию функций из F. Например, формула $(x \oplus y) \vee (\overline{x} \oplus \overline{y})$ является суперпозицией суммы по модулю 2, дизъюнкции и отрицания.

Каждой формуле $A(x_1, \dots, x_n)$ над множеством F можно сопоставить булеву функцию $f(x_1, \dots, x_n) = A(x_1, \dots, x_n)$. Говорят, что формула A является *реализацией* функции f.

Одна и та же булева функция может иметь множество реализаций. Формулы A и B, реализующие одну и ту же булеву функцию, называются *эквивалентными* (или *равносильными*). При этом пишут $A = B$. Основные равносильности формул над множеством F_0 приведены в разделе 1.1.4.

1.4.2. Принцип двойственности

Определение 1.4.5. Булева функция $f^*(x_1, \dots, x_n) = \overline{f}(\overline{x}_1, \dots, \overline{x}_n)$ называется *двойственной* к функции $f(x_1, \dots x_n)$.

Из определения двойственной функции следует, что $(f^*)^* = f$. В следующей таблице приведены двойственные пары некоторых элементарных функций.

f	0	1	x	$\overline{x}$	xy	$x \oplus y$	$x \mid y$
f^*	1	0	x	$\overline{x}$	$x \vee y$	$x \Leftrightarrow y$	$x \downarrow y$

Определение 1.4.6. Функция f называется *самодвойственной*, если $f = f^*$.

Например, функции x и $\overline{x}$ являются самодвойственными.

Из этого определения следует, что функция является самодвойственной тогда и только тогда, когда на противоположных наборах переменных она принимает противоположные значения.

Теорема 1.4.1 (О двойственной функции). *Если булева функция $\varphi(x_1, \dots, x_n)$ реализована формулой*

$$A = f\big(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\big),$$

то булева функция $\varphi^*(x_1, \dots, x_n)$ реализуется формулой

$$A^* = f^*\big(f_1^*(x_1, \dots, x_n), \dots, f_m^*(x_1, \dots, x_n)\big).$$

Доказательство.

$$\begin{aligned}
\varphi^*(x_1, \dots, x_n) &= \overline{\varphi}\,(\overline{x}_1, \dots, \overline{x}_n) = \\
&= \overline{f}\big(f_1(\overline{x}_1, \dots, \overline{x}_n), \dots, f_m(\overline{x}_1, \dots, \overline{x}_n)\big) = \\
&= \overline{f}\left(\overline{\overline{f}}_1(\overline{x}_1, \dots, \overline{x}_n), \dots, \overline{\overline{f}}_m(\overline{x}_1, \dots, \overline{x}_n)\right) = \\
&= \overline{f}\left(\overline{f_1^*}(x_1, \dots, x_n), \dots, \overline{f_m^*}(x_1, \dots, x_n)\right) = \\
&= f^*\big(f_1^*(x_1, \dots, x_n), \dots, f_m^*(x_1, \dots, x_n)\big).
\end{aligned}$$

■

Следствие 1.4.1 (Принцип двойственности).
Пусть $F = \{ f_1, \dots, f_m\}$ и $F^* = \{ f_1^*, \dots, f_m^*\}$. Если формула A над F реализует функцию φ, то формула A^* над F^*, полученная из A заменой f_i на f_i^*, реализует функцию φ^*.

Формула A^* называется *двойственной* к формуле A. Для формул над множеством функций

$$F = \{\, 0,\ \ 1,\ \ x \wedge y,\ \ x \vee y,\ \ x \oplus y,\ \ x \Leftrightarrow y,\ \ x \mid y,\ \ x \downarrow y \,\}$$

принцип двойственности можно сформулировать следующим образом: для получения формулы A^*, двойственной формуле A над F, нужно в формуле A заменить функции из F, соответственно, на функции

$$F^* = \{\, 1,\ \ 0,\ \ x \vee y,\ \ x \wedge y,\ \ x \Leftrightarrow y,\ \ x \oplus y,\ \ x \downarrow y,\ \ x \mid y \,\}.$$

Следствие 1.4.2. Если $A_1 = A_2$, то $A_1^* = A_2^*$.

В частности, из формулы де Моргана $\overline{x \vee y} = \overline{x}\,\overline{y}$ следует двойственная формула $\overline{xy} = \overline{x} \vee \overline{y}$.

1.4.3. Разложения булевых функций по переменным

Введем обозначение: $x^y = (x \Leftrightarrow y)$. По определению, $x^y = 1$ тогда и только тогда, когда $x = y$. Кроме того, переменная y может служить параметром, с помощью которого к переменной x можно применять или не применять отрицание:

$$\mathrm{x}^0 = \overline{\mathrm{x}},\ \ \mathrm{x}^1 = \mathrm{x}.$$

Теорема 1.4.2 (О разложении булевых функций по переменным).

$$f(x_1, \dots, x_n) = \bigvee_{(\sigma_1,\dots,\sigma_m)} x_1^{\sigma_1} x_2^{\sigma_2} \dots x_m^{\sigma_m} f(\sigma_1, \dots, \sigma_m, x_{m+1}, \dots, x_n)\,,$$

где дизъюнкция берется по всем наборам $(\sigma_1, \dots, \sigma_m)$.

Доказательство. Рассмотрим произвольный набор значений переменных $a = a_1, \dots, a_m, a_{m+1}, \dots, a_n$ и оценим значение дизъюнкции на этом наборе:

$$\bigvee_{(\sigma_1,\dots,\sigma_m)} a_1^{\sigma_1} a_2^{\sigma_2} \dots a_m^{\sigma_m} f(\sigma_1, \dots, \sigma_m, a_{m+1}, \dots, a_n).$$

Для всех наборов $\sigma_1, \dots, \sigma_m$, содержащих $\sigma_i \neq a_i,\ \ 1 \leq i \leq m$, соответствующая конъюнкция $a_1^{\sigma_1} \dots a_m^{\sigma_m}$ равна 0, поэтому под знаком дизъюнкции останется единственная ненулевая конъюнкция

$$a_1^{a_1} \dots a_m^{a_m} f(a_1, \dots, a_m, a_{m+1}, \dots, a_n) = f(a_1, \dots, a_n). \qquad \blacksquare$$

Следствие 1.4.3 (Случай для $m = 1$). *Для любого* $1 \leq i \leq n$ *выполняется*

$$f(x_1, \dots, x_n) = x_i f(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) \vee \overline{x}_i f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n).$$

Следствие 1.4.4 (Случай для $m = n$).

$$f(x_1, \dots, x_n) = \bigvee_{(\sigma_1,\dots,\sigma_n)} x_1^{\sigma_1} \dots x_n^{\sigma_n} f(\sigma_1, \dots, \sigma_n) = \bigvee_{f(\sigma_1,\dots,\sigma_n)=1} x_1^{\sigma_1} \dots x_n^{\sigma_n}. \qquad (1.4.1)$$

Таким образом, мы получили способ построения формулы, реализующей произвольную таблично заданную булеву функцию. Например:

$$x \oplus y = \bigvee_{\substack{(0,1)\\(1,0)}} x^{\sigma_x} y^{\sigma_y} = x^0 y^1 \vee x^1 y^0 = \overline{x} y \vee x \overline{y}.$$

Член разложения $K = x_1^{\sigma_1} \ldots x_n^{\sigma_n}$ называется *элементарной конъюнкцией*.

Определение 1.4.7. Представление булевой функции $f(x_1, \ldots, x_n)$ в форме дизъюнкции элементарных конъюнкций вида $\bigvee_{i=1}^{m} K_i$ называется *дизъюнктивной нормальной формой* (*ДНФ*) функции f. Если каждая элементарная конъюнкция $K_i,\ 1 \le i \le m$, содержит в точности по одной переменной $x_j,\ 1 \le j \le n$ (с отрицанием или без отрицания), то такая ДНФ называется *совершенной* (сокращенно *СДНФ*).

Из формулы (1.4.1) следует, что представление функции в виде СДНФ единственно.

Рассмотрим еще одну форму представления булевой функции. Для этого запишем СДНФ функции f^*, двойственной к f

$$f^*(x_1, \ldots, x_n) = \bigvee_{f^*(\sigma_1,\ldots,\sigma_n)=1} x^{\sigma_1} \ldots x^{\sigma_n}$$

и получим двойственную к ней формулу

$$f(x_1, \ldots, x_n) = \left(f^*(x_1, \ldots, x_n)\right)^* = \bigwedge_{\overline{f}\,(\overline{\sigma}_1,\ldots,\overline{\sigma}_n)=1} x^{\sigma_1} \vee \ldots \vee x^{\sigma_n} =$$

$$= \bigwedge_{f(\sigma_1,\ldots,\sigma_n)=0} x^{\overline{\sigma}_1} \vee \ldots \vee x^{\overline{\sigma}_n}. \qquad (1.4.2)$$

Правая часть равенства (1.4.2) называется *совершенной конъюнктивной нормальной формой* (*СКНФ*). Формула, двойственная к ДНФ, называется *конъюнктивной нормальной формой* (*КНФ*).

Например, представление суммы по модулю 2 в виде СКНФ выглядит следующим образом:

$$x \oplus y = \bigwedge_{\substack{(0,0)\\(1,1)}} x^{\overline{\sigma}_x}\ y^{\overline{\sigma}_y} = (x^1 \vee y^1)(x^0 \vee y^0) = (x \vee y)(\overline{x} \vee \overline{y}).$$

1.4.4. Минимизация булевых функций

В отличие от СДНФ представление булевой функции в виде ДНФ не является единственным. Рассмотрим в качестве примера два разложения функции $f(x, y, z) = (\bar{x} \vee y) \oplus\ yz(x \vee z)$:

1. $\bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}y\bar{z} \vee xy\bar{z}$ (СДНФ),
2. $\bar{x}\bar{y} \vee y\bar{z}$.

На основе этих разложений могут быть синтезированы две различные по сложности схемы преобразователей информации, реализующие одну и ту же булеву функцию (рисунок 1.4.3). Эти схемы содержат разное число элементов и связей, поэтому созданные на их основе электронные устройства будут иметь разную скорость преобразования входного сигнала (x, y, z) в выходной сигнал $f(x, y, z)$.

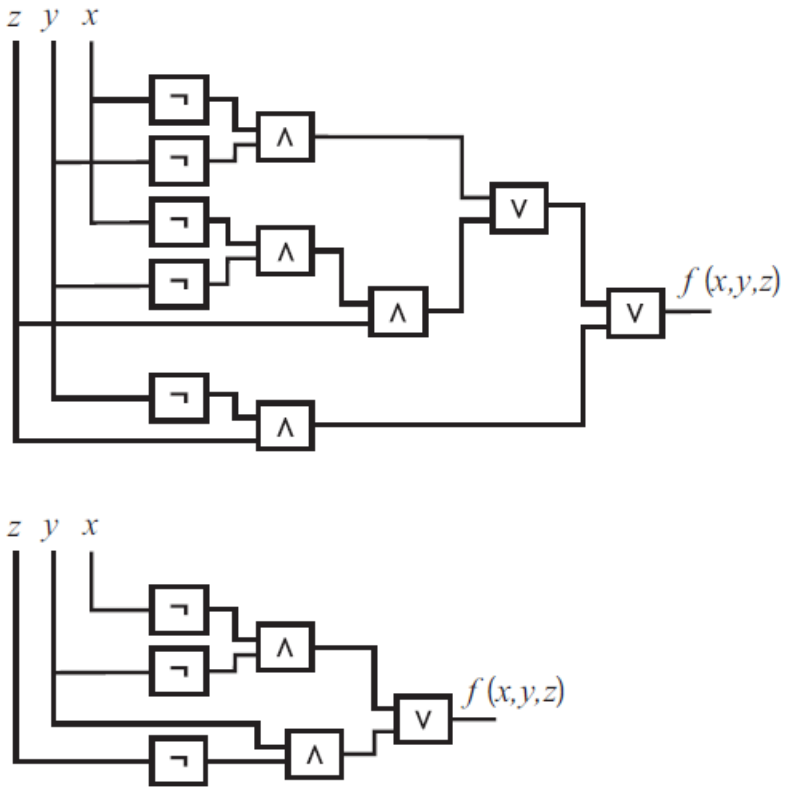

Рисунок 1.4.3 Две схемы преобразователей информации, реализующих одну и ту же булеву функцию

Таким образом, возникает задача минимизации сложности схемы, реализующей заданную булеву функцию формулой над заданным множеством элементарных булевых функций. Относительно множества $\{\wedge, \vee, \neg\}$ задача формулируется как поиск ДНФ минимальной сложности.

Формализуем понятие сложности ДНФ. Для этого рассмотрим два способа сокращения числа переменных в составе ДНФ, основанных на следующих формулах:

1. $xK \vee \bar{x}K = K$,
2. $K \vee xK = K$,

где K обозначает некоторую переменную или элементарную конъюнкцию.

Определение 1.4.8. ДНФ называется

- *тупиковой* или *локально минимальной*, если в ней отсутствуют слагаемые вида $xK \vee \bar{x}K$ и $K \vee xK$;

- *минимальной*, если она содержит наименьшее количество переменных и их отрицаний среди всех возможных ДНФ, реализующих данную булеву функцию.

Из двух ДНФ в приведенном выше примере первая не является тупиковой, поскольку содержит пару $\bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z$, которая сокращается до $\bar{x}\bar{y}$. Вторая ДНФ является тупиковой и минимальной.

Заметим, что минимальная ДНФ является тупиковой, но не всякая тупиковая ДНФ является минимальной. В общем случае поиск минимальной ДНФ является весьма сложной задачей при том, что для поиска тупиковых ДНФ существуют сравнительно простые алгоритмы. Ниже мы рассмотрим два из них.

1.4.5. Метод Квайна

Этот метод, названный так в честь его разработчика Вилларда Квайна (Willard V. Quine), основан на последовательном преобразовании СДНФ к более короткой формуле с помощью двух элементарных операций:

- $xK \vee \bar{x}K = xK \vee \bar{x}K \vee K$ (склеивание),
- $K \vee xK = K$ (поглощение).

Выделенная в операции склеивания конъюнкция K называется *простой импликантой*. На первом этапе все входящие в СДНФ конъюнкции попарно анализируются и с помощью операции склеивания из них выделяются простые импликанты с меньшим числом переменных. Выделенные импликанты также попарно анализируются, из них, по возможности, также выделяются более короткие импликанты и т.д. Эти действия повторяются до тех пор, пока из выделенных импликант могут быть получены более короткие.

Рассмотрим описанные действия на примере. Для краткости и удобства будем задавать булеву функцию $f(x, y, z)$ в *векторном* виде, то есть в виде правого столбца таблицы истинности этой функции. Например, импликации соответствует векторное представление $(1, 1, 0, 1)$.

Построим СДНФ и выпишем в столбец пронумерованные конъюнкции:

1	$\bar{x}\bar{y}\bar{z}$
2	$\bar{x}\bar{y}z$
3	$\bar{x}yz$
4	$x\bar{y}\bar{z}$
5	$xy\bar{z}$
6	xyz

Заметим, что из первой и второй конъюнкции с помощью операции склеивания можно выделить импликанту $\bar{x}\bar{y}$, из первой и четвертой – импликанту $\bar{y}\bar{z}$ и т.д. Выпишем полученные импликанты:

1-2 $\bar{x}\bar{y}$
1-4 $\bar{y}\bar{z}$
2-3 $\bar{x}z$
3-6 yz
4-5 $x\bar{z}$
5-6 xy

Сравнивая их попарно, убедимся, что более короткие импликанты (то есть содержащие только одну переменную) выделить не получается.

На втором этапе метода Квайна выполняется поглощение исходных конъюнкций простыми импликантами, полученными на предыдущем этапе (заметим, что $xK \vee \bar{x}K \vee K = K$). При этом одна и та же конъюнкция может быть поглощена несколькими различными импликантами. Например, конъюнкция 1 ($\bar{x}\bar{y}\bar{z}$) поглощается импликантами 1-2 ($\bar{x}\bar{y}$) и 1-4 ($\bar{y}\bar{z}$). С другой стороны, одна и та же импликанта могла быть выделена из нескольких различных пар конъюнкций и поэтому может поглотить более двух конъюнкций.

Таким образом, возникает задача выбора минимального набора импликант, поглощающих все конъюнкции исходной СДНФ. Для упрощения поиска такого набора используется *таблица Квайна*, строкам которой соответствуют исходные конъюнкции, а столбцам – простые импликанты. Для удобства вместо конъюнкций и простых импликант будем записывать их номера (заметим, что номера импликант содержат номера конъюнкций, которые они поглощают). Для нашего примера таблица Квайна выглядит следующим образом:

	1-2	1-4	2-3	3-6	4-5	5-6
1	+	+				
2	+		+			
3			+	+		
4		+			+	
5					+	+
6				+		+

В ячейках таблицы ставится плюс, если импликант в данном столбце поглощает конъюнкцию, соответствующую данной строке. Будем говорить, что столбец *покрывает* строку, если он содержит плюс на пересечении с данной строкой. Таким образом, требуется найти минимальное подмножество столбцов, покрывающих все строки. В нашем примере существуют два таких подмножества {1-2, 3-6, 4-5} и {1-4, 2-3, 5-6}, которым соответствуют два подмножества импликант $\{\bar{x}\bar{y}, yz, x\bar{z}\}$ и $\{\bar{y}\bar{z}, \bar{x}z, xy\}$. Таким образом, полученные тупиковые ДНФ равноценны по числу переменных:

$$f(x,y,z) = \bar{x}\bar{y} \vee yz \vee x\bar{z} = \bar{y}\bar{z} \vee \bar{x}z \vee xy.$$

1.4.6. Геометрический метод

Рассмотрим булев куб $\mathbb{B}^n$ и булеву функцию $f(x_1, \dots, x_n)$. Обозначим через N_f множество вершин $(x_1, \dots, x_n) \in \mathbb{B}^n$ таких, что $f(x_1, \dots, x_n) = 1$. Очевидно, что отображение из f в N_f биективно. На рисунке 1.4.4 изображен булев куб $\mathbb{B}^3$ и множество N_f для функции $f(x, y, z)$ из рассмотренного выше примера.

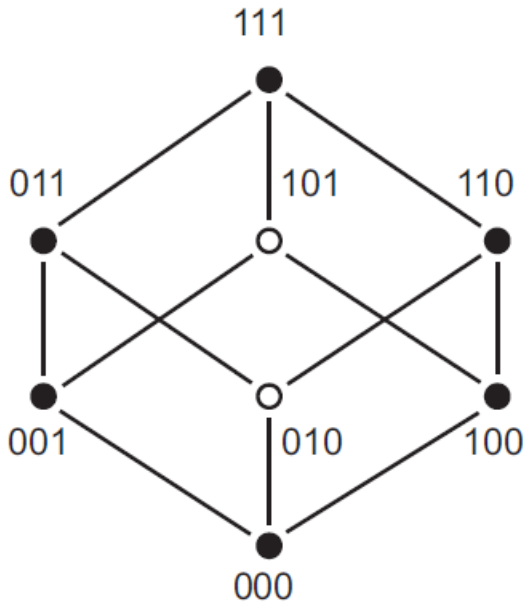

Рисунок 1.4.4 Булев куб $\mathbb{B}^3$ и подмножество вершин N_f (обозначены черным цветом)

Подмножество вершин $\mathbb{B}^n$, r координат которых совпадают $(1 \le r \le n)$, называется $(n-r)$-*мерной гранью* булева куба. В частности, вершины куба $\mathbb{B}^3$ является его 0-мерными гранями, ребра – 1-мерными, а стороны – 2-мерными. Весь булев куб $\mathbb{B}^3$ также представляет собой грань – 3-мерную.

Рассмотрим элементарную конъюнкцию

$$K = K(x_1, \dots, x_n) = x_{i_1}^{\sigma_1} \dots x_{i_r}^{\sigma_r}$$

и соответствующее ей множество N_K вершин $\mathbb{B}^n$. Заметим, что $K = 1$ тогда и только тогда, когда $x_{i_j} = \sigma_j$, $1 \le j \le r$, поэтому N_K представляет собой $(n-r)$-мерную грань.

Заметим также, что чем меньше переменных в конъюнкции, тем выше размерность соответствующей грани. В качестве примера рассмотрим три конъюнкции (рисунок 1.4.5) и соответствующие им грани:

$K_1(x, y, z) = \bar{x}yz$: $N_{K_1} = \{ (0,1,1) \}$

$K_2(x, y, z) = \bar{x}\bar{y}$: $N_{K_2} = \{ (0,0,0), (0,0,1) \}$,

$K_3(x, y, z) = x$: $N_{K_3} = \{ (1,0,0), (1,0,1), (1,1,0), (1,1,1) \}$.

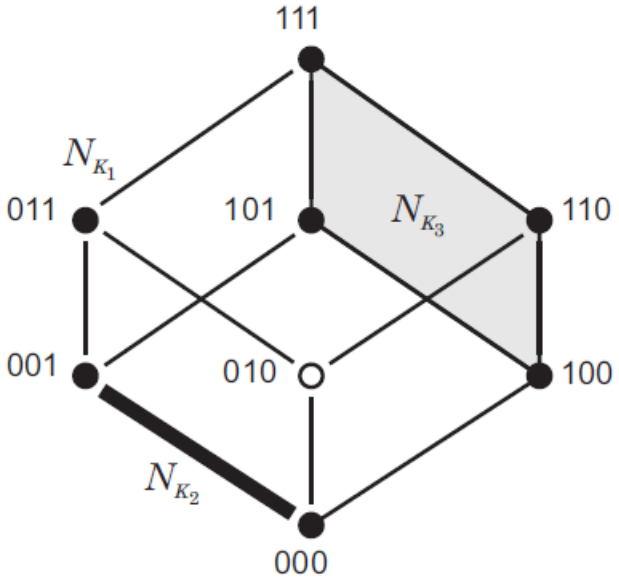

Рисунок 1.4.5 Булев куб $\mathbb{B}^3$ и грани, соответствующие конъюнкциям K_1, K_2 и K_3

Геометрический метод минимизации ДНФ основан на следующем утверждении.

Теорема 1.4.3.
Если $f(x_1, \dots, x_n) = g(x_1, \dots, x_n) \vee h(x_1, \dots, x_n)$, *то* $N_f = N_g \cup N_h$.

Доказательство. Обозначим $x = (x_1, \dots, x_n)$. Из условия теоремы, имеем

$$N_f = \{\, x \mid f(x) \,\} = \{x \mid g(x) \vee h(x) \,\} = \{\, x \mid \big(x \in N_g\big) \vee (x \in N_h) \,\} = N_g \cup N_h. \quad \blacksquare$$

Другими словами, система множеств $\{\, N_g, N_h \,\}$ есть покрытие множества N_f. В частности, если функция f представима в виде ДНФ $f = K_1 \vee \dots \vee K_m$, то

$$N_f = N_{K_1} \cup \dots \cup N_{K_m}.$$

Отсюда следует, что всякой ДНФ взаимно-однозначно соответствует некоторое покрытие множества N_f некоторыми гранями булева куба.

Обозначим через $\dim K_i$ размерность грани N_{K_i}. Число

$$\sum_{i=1}^{m} dim\ K_i$$

называется *размерностью покрытия*. Тогда задача о минимизации булевой функции имеет следующую геометрическую интерпретацию: *для данного множества* N_f *необходимо найти такое его покрытие гранями* $N_{K_1} \cup \dots \cup N_{K_m}$, *которое имеет максимальную размерность.*

Из этой интерпретации следует алгоритм построения тупиковой ДНФ, применимый для функций f небольшого числа переменных:

1. На кубе $\mathbb{B}^n$ отметить множество вершин N_f.
2. Найти покрытие множества N_f максимальной размерности.
3. Каждой из полученных граней N_i найденного покрытия поставить в соответствие элементарную конъюнкцию искомой ДНФ.

Рассмотрим пример. Для функции из предыдущего примера (раздел 1.4.5) обозначим на булевом кубе $\mathbb{B}^3$ множество вершин N_f (рисунок 1.4.6 *а*).

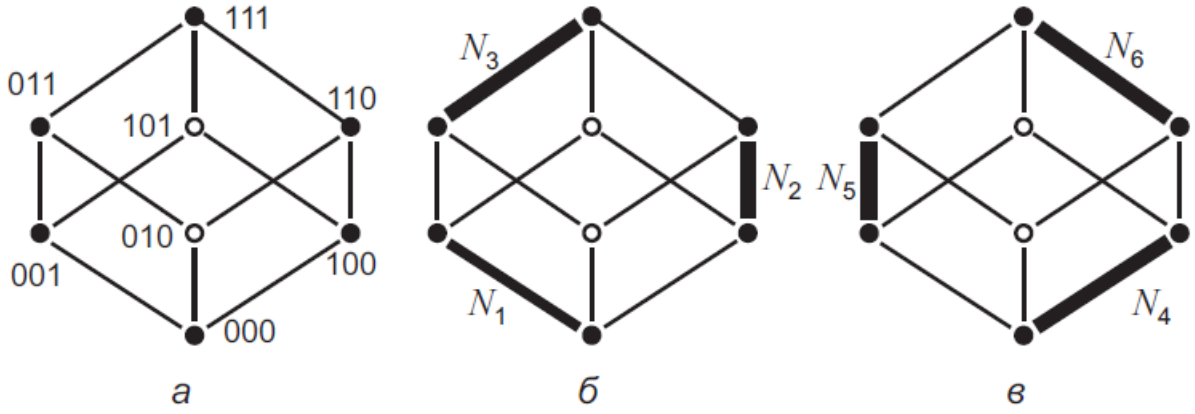

Рисунок 1.4.6. Множество вершин N_f (а) и два варианта его покрытия – (б) и (в)

Нетрудно заметить, что существует ровно два способа покрытия выделенного множества вершин гранями максимальной размерности (рисунки 1.4.6 *б* и *в*):

$$N_1 = \{(0,0,0),(0,0,1)\} \qquad N_4 = \{(0,0,0),(1,0,0)\}$$
$$N_2 = \{(1,0,0),(1,1,0)\} \quad \text{и} \quad N_5 = \{(0,0,1),(0,1,1)\}$$
$$N_3 = \{(0,1,1),(1,1,1)\} \qquad N_6 = \{(1,1,0),(1,1,1)\}$$

Данным покрытиям соответствуют две эквивалентные тупиковые ДНФ, построенные с помощью метода Квайна в предыдущем разделе:

$$\bar{x}_1\bar{x}_2 \vee x_1\bar{x}_3 \vee x_2x_3 = \bar{x}_2\bar{x}_3 \vee \bar{x}_1x_3 \vee x_1x_2.$$

1.4.7. Базис и замыкание

Из единственности СДНФ вытекает следующая теорема:

Теорема 1.4.4. *Любая булева функция может быть представлена в виде суперпозиции только трех элементарных функций: конъюнкции, дизъюнкции и отрицания.*

Определение 1.4.9. *Функционально полным базисом* (или просто *базисом*) называется множество булевых функций, суперпозицией которых может быть представлена любая булева функция.

Таким образом, множество функций $\mathcal{B} = \{\neg, \wedge, \vee\}$ образуют базис, который называется *базисом Буля*.

Ответим на следующие вопросы:

1. Существуют ли другие системы булевых функций, отличные от $\mathcal{B}$ и обладающие свойством полноты?
2. Является ли базис $\mathcal{B}$ минимальным по количеству входящих в него функций?
3. Как определить, образует ли базис данное множество булевых функций? Другими словами, какие отличительные особенности делают данный набор булевых функций базисом?

Определение 1.4.10. *Замыканием* множества F булевых функций, обозначается $[F]$, называется множество всех булевых функций, которые могут быть получены суперпозицией функций из F.

Из определения замыкания вытекают следующие свойства.

1. $F \subseteq [F]$.
2. $\big[[F]\big] = [F]$.
3. $F \subseteq G \Rightarrow [F] \subseteq [G]$.
4. Если F – базис, и $F \subseteq [G]$, то G – тоже базис.

Доказательство первого свойства очевидно: любая функция из F является суперпозицией, состоящей из одной этой функции. Второе свойство следует из первого. Действительно, имеем $[F] \subseteq \big[[F]\big]$. Но суперпозиция суперпозиций над F также является суперпозицией над F, поэтому $\big[[F]\big] \subseteq [F]$. Свойство (3) по сути означает, что суперпозиция над подмножеством некоторого множества булевых функций является также суперпозицией над всем этим множеством, что очевидно. Из условия свойства (4) следует, что любая функция из F есть суперпозиция над G, поэтому любая булева функция может быть представлена суперпозицией функций из G.

Это последнее свойство позволяет получить новые базисы на основе известного базиса. Рассмотрим примеры других функционально полных систем булевых функций, отличных от базиса Буля.

1. Множество булевых функций $\{\neg,\ \wedge\}$ является базисом, поскольку
$$x \vee y = \overline{\bar{x}\bar{y}}.$$
2. Множество булевых функций $\{\neg,\ \vee\}$ является базисом, поскольку
$$xy = \overline{\bar{x} \vee \bar{y}}.$$
3. Множество $\{\ |\ \}$ является базисом, поскольку
$$\bar{x} = x \mid x,\ \ xy = \overline{x \mid y} = (x \mid y) \mid (x \mid y).$$
4. Множество $\{\downarrow\}$ является базисом, поскольку

$$\bar{x} = x \downarrow x, \;\; x \vee y = \overline{x \downarrow y} = (x \downarrow y) \downarrow (x \downarrow y).$$

Таким образом, мы ответили на первые два вопроса, поставленные в начале этого раздела: да, другие базисы существуют, причем некоторые из них меньше по размеру, чем базис Буля.

1.4.8. Полином Жегалкина и линейные функции

Рассмотрим отдельно систему булевых функций $\{1, \wedge, \oplus\}$. Если в формуле, включающей только функции данного множества, раскрыть скобки, то получим сумму по модулю 2 логических произведений (конъюнкций) переменных, то есть полином. Такой полином называется полиномом *Жегалкина*.

Теорема 1.4.5. *Любая булева функция может быть представлена в виде полинома Жегалкина, причем единственным образом. Другими словами, множество функций* $\{1, \wedge, \oplus\}$ *образует базис*.

Доказательство. Заметим, что с помощью функций этого множества можно выразить отрицание: $\bar{x} = 1 \oplus x$. Поскольку в это множество уже входит конъюнкция, то, согласно четвертому свойству замыкания, оно образует базис. ■

В качестве примера представим дизъюнкцию в виде полинома Жегалкина:

$$\begin{aligned} x \vee y = \overline{\bar{x}\bar{y}} &= 1 \oplus (1 \oplus x)(1 \oplus y) = \\ &= 1 \oplus 1 \oplus x \oplus y \oplus xy = \\ &= x \oplus y \oplus xy. \end{aligned}$$

Существует несколько простых методов построения полинома Жегалкина для функций, заданных векторном виде или в виде таблицы истинности. Ниже мы рассмотрим два из них, но прежде рассмотрим представление полинома Жегалкина *в общем виде*. Для простоты ограничимся тремя переменными, для большего числа переменных общее представление строится аналогично.

Назначим каждому конъюнкту соответствующий ему набор переменных в таблице истинности. Например, $(0,0,1) - z$, $(1,1,0) - xy$, $(0,1,1) - yz$ и т.д. Затем пронумеруем коэффициенты полинома в порядке следования этих наборов в таблице. Получим следующее общее представление полинома Жегалкина для трех переменных

$$a_0 \oplus a_1 z \oplus a_2 y \oplus a_3 yz \oplus a_4 x \oplus a_5 xz \oplus a_6 xy \oplus a_7 xyz, \;\; a_i \in \mathbb{B}.$$

Метод неопределенных коэффициентов

Этот метод часто применяется в линейной алгебре для нахождения коэффициентов неизвестного полинома при условии, что известны его значения на некотором наборе значений переменных. Рассмотрим как он работает на примере булевой функции от трех переменных.

Пусть $\mathrm{f} = (1,1,0,1,1,0,1,1)$. Поочередно подставим значения функции и соответствующие им наборы переменных в общее представление полинома Жегалкина. Для набора $(0,0,0)$ имеем $\mathrm{f}(0,0,0) = 1$, значит

$$a_0 \oplus a_1 0 \oplus a_2 0 \oplus a_3 00 \oplus a_4 0 \oplus a_5 00 \oplus a_6 00 \oplus a_7 000 = 1,$$

откуда получаем $a_0 = 1$. Для следующего набора $(0,0,1)$ имеем $f(0,0,1) = 1$. Подставим эти значения в общее представление с учетом уже вычисленного значения $a_0 = 1$, получим

$$1 \oplus a_1 1 \oplus a_2 0 \oplus a_3 01 \oplus a_4 0 \oplus a_5 01 \oplus a_6 00 \oplus a_7 001 = 1,$$

откуда следует, что $1 \oplus a_1 = 1$, то есть $a_1 = 0$. Аналогичным образом вычисляются остальные коэффициенты:

$$f(0,1,0) = 0:\ a_2 = 1,$$
$$f(0,1,1) = 0:\ a_3 = 1,$$
$$f(1,0,0) = 0:\ a_4 = 0,$$
$$f(1,0,1) = 0:\ a_5 = 1,$$
$$f(1,1,0) = 0:\ a_6 = 1,$$
$$f(1,1,1) = 0:\ a_7 = 0.$$

Подставив найденные коэффициенты в общее представление полинома Жегалкина, получим $f(x,y,z) = 1 \oplus y \oplus yz \oplus xz \oplus xz$.

Метод треугольника

Рассмотрим следующую таблицу, в первом столбце которой записаны значения функции из предыдущего примера.

f, a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
1							
1							
0							
1							
1							
0							
1							
1							

Заполним столбец a_1 суммами соседних элементов столбца a_0

$$a_{i,1} = a_{i,0} \oplus a_{i+1,0},\ i = 1, m-1,$$

где $m = 2^3$ – число элементов первого столбца:

f, a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
1	0						
1	1						
0	1						
1	0						
1	1						
0	1						
1	0						
1							

Повторим те же действия для элементов столбца a_2, вычисляя их значения как суммы элементов столбца a_1:

f, a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
1	0	1					
1	1	0					
0	1	1					
1	0	1					
1	1	0					
0	1	1					
1	0						
1							

Действуя таким образом, заполним всю таблицу:

f, a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
1	0	1	1	0	1	1	0
1	1	0	1	1	0	1	
0	1	1	0	1	1		
1	0	1	1	0			
1	1	0	1				
0	1	1					
1	0						
1							

Первая строка этой таблицы содержит искомые коэффициенты полинома Жегалкина.

Определение 1.4.11. Булева функция называется *линейной*, если соответствующий этой функции полином Жегалкина имеет вид

$$a_0 \oplus \bigoplus_{i=1}^{n} a_i x_i, \quad a_i \in \{0,1\}.$$

Полином Жегалкина линейной функции не содержит конъюнкций переменных. Например, отрицание является линейной функцией, а дизъюнкция – нет, поскольку содержит произведение переменных. Чтобы определить, является ли функция линейной, необходимо построить ее полином Жегалкина и проверить, содержит ли этот полином конъюнкции переменных.

1.4.9. Замкнутые классы булевых функций

Определение 1.4.12. Класс F булевых функций называется *замкнутым*, если он равен своему замыканию: $[F] = F$.

Рассмотрим следующие классы булевых функций:

1. Класс функций, *сохраняющих* 0:
$$T_0 = \{ f \mid f(0, \dots, 0) = 0 \}.$$
2. Класс функций, *сохраняющих* 1:
$$T_1 = \{ f \mid f(1, \dots, 1) = 1 \}.$$
3. Класс *самодвойственных* функций:
$$T_* = \{ f \mid f^* = f \}.$$
4. Класс {монотонных} функций:
$$T_\leq = \{ f \mid (\forall x, y \in \mathbb{B}^n)\ \ (x \leq y) \Rightarrow f(x) \leq f(y) \},$$
где $(x \leq y) \Leftrightarrow (x_i \leq y_i),\ 1 \leq i \leq n.$
5. Класс *линейных* функций:
$$T_L = \left\{ f \mid f = a_0 \oplus \bigoplus_{i=1}^{n} a_i x_i,\ \ a_i \in \mathbb{B} \right\}.$$

Теорема 1.4.6. *Классы T_0, T_1, T_*, $T_\leq$ и T_L замкнуты.*

В качестве примера исследуем простейшие функции на принадлежность некоторым из указанных классов.

- Конъюнкция принадлежит классам T_0, T_1 и $T_\leq$. Действительно
$$0 \wedge \dots \wedge 0 = 0,$$
$$1 \wedge \dots \wedge 1 = 1,$$
$$(x_1, \dots, x_n) \leq (y_1, \dots, y_n) \Rightarrow \bigwedge_{i=1}^{n} x_i \leq \bigwedge_{i=1}^{n} y_i.$$
- Отрицание не является монотонной функцией, так как $0 \leq 1$, но $\bar{0} > \bar{1}$, и является линейной: $\bar{x} = 1 \oplus x$.

- Дизъюнкция не является линейной функцией, поскольку соответствующий полином Жегалкина содержит конъюнкцию переменных:

$$x \vee y = x \oplus y \oplus xy.$$

В следующей теореме сформулировано то самое специфическое свойство, которое отличает базисы от остальных множеств булевых функций.

Теорема 1.4.7 (Пост). *Система булевых функций полна тогда и только тогда, когда она не содержится полностью ни в одном из классов* T_0, T_1, T_*, $T_\leq$, T_L.

Другими словами, система булевых функций полна тогда и только тогда, когда она содержит

- хотя бы одну функцию, не сохраняющую 0,
- хотя бы одну функцию, не сохраняющую 1,
- хотя бы одну немонотонную функцию,
- хотя бы одну несамодвойственную функцию,
- хотя бы одну нелинейную функцию.

В следующей таблице отмечена принадлежность элементарных булевых функций указанным замкнутым классам.

F_0	T_0	T_1	T_*	$T_\leq$	T_L	Примечания
0	●			●	●	
1		●		●	●	
$\bar{x}$			●		●	
$x \wedge y$	●	●		●		
$x \vee y$	●	●		●		
$x \Rightarrow y$		●				Образует базис с любой $f \notin T_1$.
$x \oplus y$	●				●	
$x \Leftrightarrow y$		●			●	
$x \mid y$						Является базисом.
$x \downarrow y$						Является базисом.
x	●	●	●	●	●	Избыточная функция в любом базисе.

На основе этой таблицы нетрудно построить функционально полные системы булевых функций, включая уже известные базисы, например, $\{ 1, \wedge, \oplus \}$, $\{ \neg, \Rightarrow \}$, $\{ \Rightarrow, 0 \}$ и другие.

2. ПРАКТИЧЕСКИЙ РАЗДЕЛ

2.1. Задачи для самостоятельного решения по теме 1.1

1. Выделив условие и заключение утверждения, сформулируйте его посредством связки «Если ..., то ...»:
   a. «Для того чтобы функция была дифференцируемой в некоторой точке, необходимо, чтобы она была непрерывной в этой точке».
   b. «Для делимости многочлена $f(x)$ на линейный двучлен $(x-a)$ достаточно, чтобы число a было корнем этого многочлена».
   c. «На 5 делятся те целые числа, которые оканчиваются цифрой 0 или цифрой 5».
   d. «Комплексные числа равны, только если равны соответственно их действительные и мнимые части».
   e. «Четность суммы есть необходимое условие четности каждого слагаемого».
   f. «Равенство треугольников есть достаточное условие их равновеликости».
   g. «Для делимости произведения на некоторое число достаточно, чтобы по меньшей мере один из сомножителей делился на это число».
2. Известно, что каждый негамильтонов двусвязный граф содержит тета-подграф. Сформулируйте в виде связки «Если ..., то...» достаточное условие того, что граф гамильтонов.
3. Доказать, что данные формулы являются тавтологиями:
   a. $(p \Rightarrow q) \vee (q \Rightarrow p)$
   b. $p \Rightarrow (q \Rightarrow pq)$
   c. $(p \Rightarrow q) \Rightarrow \big((q \Rightarrow r) \Rightarrow (p \Rightarrow r)\big)$
   d. $(\overline{p} \Rightarrow \overline{q}) \Rightarrow (q \Rightarrow p)$
   e. $(p \Rightarrow q) \Rightarrow \Big(\big(p \Rightarrow (q \Rightarrow r)\big) \Rightarrow (p \Rightarrow r)\Big)$
   f. $(p \Rightarrow q) \Rightarrow \big((p \Rightarrow \overline{q}) \Rightarrow \overline{p}\big)$
   g. $(q \Rightarrow r) \Rightarrow \big((p \vee q) \Rightarrow (p \vee r)\big)$
   h. $(\overline{q} \Rightarrow \overline{p}) \Rightarrow\ ((\overline{q} \Rightarrow\ p) \Rightarrow\ q)$
4. Является ли следующие формулы тавтологиями?
   a. $y\overline{z} \vee \big((x \vee y) \Rightarrow (x \vee z)\big)$
   b. $\overline{x\ \Rightarrow \overline{x}}$

c. $(x\overline{y}) \vee \left((x \Rightarrow \overline{y}) \Rightarrow \overline{x}\right)$

d. $\left((x \Rightarrow yz) \Rightarrow (\overline{y} \Rightarrow \overline{x})\right) \Rightarrow \overline{y}$

e. $\overline{\left((x \vee \overline{x}y) \vee x \vee y\right)}$

f. $(\overline{x} \Rightarrow \overline{y}) \Rightarrow (x \Rightarrow y)$

g. $(xy \vee z) \Rightarrow \left((x \vee y)(x \vee z)\right)$

h. $(x \vee y) \Rightarrow (\overline{x}y \vee x\overline{y})$

5. Является ли тавтологиями следующие утверждения?

   a. «Если дифференцируемая функция непрерывна, то невозможно, чтобы функция была дифференцируема и разрывна».

   b. «Если справедливо, что невырожденная матрица имеет обратную, то справедливо также, что матрица либо вырожденная, либо имеет обратную».

   c. «Если температура и влажность высокие, значит имеет место высокая температура при низком давлении или же и давление и влажность высокие».

1. Доказать эквивалентности:

   a. $a \vee bc = (a \vee b)(a \vee c)$

   b. $a(a \vee b) = a$

   c. $\overline{(a \Rightarrow b)} = a\overline{b}$

   d. $(a \Rightarrow \overline{a}) = \overline{a}$

   e. $(a \vee b)(a \vee c)(b \vee d)(c \vee d) = ad \vee bc$

   f. $a(a \vee c)(b \vee c) = ab \vee ac$

   g. $(a \vee b)(b \vee c)(c \vee a) = ab \vee bc \vee ca$

   h. $(a \vee b)(b \vee c)(c \vee d) = ac \vee bc \vee bd$

   i. $(a \vee b \vee c)(b \vee c \vee d)(c \vee d \vee a) = ab \vee ad \vee bd \vee c$

   j. $ab \vee \left((a \vee b)\left(\overline{a} \vee \overline{b}\right)\right) = a \vee b$

2. Можно ли утверждать, что верны логические следствия?

   a. $(p \Rightarrow q), (q \Rightarrow r) \vdash r$

   b. $(p \Rightarrow q), (p \Rightarrow r), (q \vee r) \vdash p$

   c. $(p \Rightarrow q), (p \Rightarrow r), \overline{pq} \vdash \overline{p}$

   d. $(\overline{p} \vee \overline{q}), (r \vee \overline{q}), \overline{p} \vdash r \vee \overline{p}$

   e. $(p \Rightarrow q), (\overline{q} \Rightarrow \overline{r}), (r \Rightarrow t), (t \vee q) \vdash (p \vee r)$

3. С помощью основной теоремы логического вывода докажите следующие логические следствия:

a. $(a \vee b), (b \Rightarrow c), (a \Rightarrow d) \vdash (c \vee d)$

b. $(a \Rightarrow b), (\overline{c} \vee d), \overline{b \vee d} \vdash (a \Rightarrow \overline{c})$

c. $(\overline{a} \vee b), \left(c \vee \overline{b}\right), a, d \vdash (c \vee d)$

d. $(a \Rightarrow b), \left(\overline{b} \Rightarrow \overline{c}\right), (c \Rightarrow d), (d \vee b) \vdash (a \vee c)$

e. $\big(a \Rightarrow (b \Rightarrow c)\big), (a \Rightarrow b), a \vdash c$

4. [20] Мистер Мак-Грегор, владелец лавки в Лондоне, сообщил в Скотланд-Ярд, что его ограбили. По обвинению владельца лавки были задержаны три подозрительные личности *A*, *B* и *C*. На основании показаний Мак-Грегора, данных под присягой, было установлено, что:

   a. Каждый из подозреваемых был в день ограбления в лавке и никто другой туда не заходил.

   b. Если A виновен, то у него был ровно один сообщник.

   c. Если B невиновен, то C тоже невиновен.

   d. Если C невиновен, то B тоже невиновен.

   e. Если виновны ровно двое подозреваемых, то A – один из них.

   Против кого Скотланд-Ярд выдвинул обвинение?

5. Известно, что если будет холодно, то Андрей наденет тёплую куртку при условии, что рукав будет починен. Известно также, что завтра будет холодно, а рукав не будет починен. Следует ли из этого, что Андрей не наденет тёплую куртку?

6. [20] (*Дело о врунах*.) Три школьника *A*, *B* и *C* вызваны к директору. В беседе с директором *A* утверждает, что *B* врет, *B* утверждает, что *C* врет, а *C* утверждает, что врут оба – *A* и *B*. Какой вывод может сделать директор?

7. [20] (*Дело о рецидивистах*.) Трое рецидивистов *A*, *B* и *C* подозреваются в преступлении. Неопровержимо установлены следующие факты:

   a. Если *A* виновен, а *B* невиновен, то в деле участвовал *C*.

   b. *C* никогда не действует в одиночку.

   c. *A* никогда не ходит на дело вместе с *C*.

   d. Никто, кроме *A*, *B* и *C* в преступлении не замешан, но по крайней мере один из них виновен.

   Можно ли на основании этих фактов выдвинуть обвинение против *A*? Против *B*? Против *C*?

8. Запишите следующие высказывания и их отрицания в виде формул логики предикатов:

a. «Один и только один объект обладает свойством P.»

b. «По крайне мере один объект обладает свойством P.»

c. «Ровно два объекта обладают свойством P.»

d. «По крайней мере три объекта обладают свойством P.»

9. Запишите в виде предиката утверждение:

   a. «Если два объекта обладают свойством P, то они совпадают».

   b. «По крайней мере один студент решил все задачи».

   c. «Каждую задачу решил по крайней мере один студент».

10. [20] Один из афоризмов Кузьмы Пруткова звучит так: «Нет столь великой вещи, которую не превзошла бы величиной еще большая». Запишите этот афоризм в виде предикатной формулы, используя предикат $P(x, y)$, означающий «x больше y».

11. Функция f на множестве A называется *непрерывной в точке* $x_0 \in A$, если

$$(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x \in A)(|x - x_0| \leq \delta \Rightarrow |f(x) - f(x_0)| \leq \varepsilon).$$

Запишите необходимое и достаточное условие того, что функция f не является непрерывной в точке x_0.

12. Число a является пределом последовательности $(a_i)_{i=1}^{\infty}$, если

$$(\forall \varepsilon > 0)(\exists N > 0)(\forall n)(n \geq N \Rightarrow |a_i - a| \leq \varepsilon).$$

Запишите необходимое и достаточное условие того, что число a не является пределом этой последовательности.

13. Приведите предикатную формулу к нормальной форме:

   a. $\big((\forall x)P(x) \Rightarrow (\exists x)Q(x)\big) \Rightarrow (\forall x)P(x)\overline{Q}(x)$.

   b. $(\exists x)\left(\overline{P}(x) \vee Q(x)\right) \vee (\forall x)P(x) \Rightarrow Q(x)$.

   c. $(\exists x)\left(\overline{P}(x) \vee Q(x)\right) \Rightarrow (\forall x)P(x)(\exists x)\overline{Q}(x)$.

   d. $\big((\exists x)P(x) \Rightarrow (\forall x)Q(x)\big)\Big((\forall x)\left(P(x) \Rightarrow \overline{Q}(x)\right)\Big)$.

   e. $\Big((\forall x)P(x) \vee (\exists x)\overline{Q}(x)\Big) \Rightarrow \Big((\exists x)\overline{P}(x) \Rightarrow (\forall x)Q(x)\Big)$.

   f. $\Big((\exists x)\overline{P}(x)(\forall x)Q(x)\Big) \vee \Big((\forall x)P(x) \Rightarrow (\exists x)\overline{Q}(x)\Big)$.

14. Докажите методом математической индукции, что плоскость, разделенная на области любым количеством прямых, может быть раскрашена в черный и белый цвет таким образом, что области, имеющие общую границу, будут раскрашены в разные цвета.

2.2. Задачи для самостоятельного решения по теме 1.2

1. Доказать тождества:
   a. $\overline{A \cup B} = \overline{A} \cap \overline{B}$
   b. $A\backslash(B \cup C) = (A\backslash B) \cap (A\backslash C) = (A\backslash B)\backslash C$
   c. $A\backslash(B \cap C) = (A\backslash B) \cup (A\backslash C)$
   d. $A\backslash(A\backslash B) = A \cap B$
   e. $A\backslash(A \cap B) = A\backslash B$
   f. $A \cap (B\backslash C) = (A \cap B)\backslash(A \cap C) = (A \cap B)\backslash C$
   g. $(A\backslash B)\backslash C = (A\backslash C)\backslash(B\backslash C)$
   h. $A \cup (B\backslash A) = A \cup B$
   i. $A \cap \left(\overline{A} \cup B\right) = A \cap B$
   j. $(A \cup B)\backslash C = (A\backslash C) \cup (B\backslash C)$
   k. $A\backslash(B\backslash C) = (A\backslash B) \cup (A \cap C)$
   l. $(A \cap B) \cup \left(A \cap \overline{B}\right) = A$
   m. $2^{A \cap B} = 2^A \cap 2^B$
2. Доказать:
   a. $A \cup B \subseteq C \Leftrightarrow (A \subseteq C) \wedge (B \subseteq C)$
   b. $A \subseteq B \cap C \Leftrightarrow A \subseteq B \wedge A \subseteq C$
   c. $A \cap B \subseteq C \Leftrightarrow A \subseteq \overline{B} \cup C$
   d. $A \subseteq B \cup C \Leftrightarrow A \cap \overline{B} \subseteq C$
   e. $(A\backslash B) \cup B = A \Leftrightarrow B \subseteq A$
   f. $(A \cap B) \cup C = A \cap (B \cup C) \Leftrightarrow C \subseteq A$
   g. $A \subseteq B \Rightarrow A \cup C \subseteq B \cup C$
   h. $A \subseteq B \Rightarrow (A\backslash C) \subseteq (B\backslash C)$
   i. $A \subseteq B \Rightarrow (C\backslash B) \subseteq (C\backslash A)$
   j. $(A \cup B = A \cap B) \Rightarrow (A = B)$
   k. $\left(A = \overline{B}\right) \Leftrightarrow (A \cap B = \emptyset) \wedge (A \cup B = U)$
3. Доказать тождества:
   a. $(A \cup B) \times C = (A \times C) \cup (B \times C)$
   b. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
   c. $(A \cup B) \times (C \cup D) = (A \times C) \cup (A \times D) \cup (B \times C) \cup (B \times D)$
   d. $(A\backslash B) \times C = (A \times C)\backslash(B \times C)$
   e. $A \times (B\backslash C) = (A \times B)\backslash(A \times C)$

4. Доказать, что если $A \subseteq C$ и $B \subseteq D$, то
$$A \times B = (A \times D) \cap (C \times B).$$
5. Доказать, что если множества A, B, C и D непустые, то
$$(A \subseteq B \wedge C \subseteq D) \Leftrightarrow (A \times C) \subseteq (B \times D).$$
6. Найти D_R, V_R, R^{-1}, $R \circ R$, $R \circ R^{-1}$ и $R^{-1} \circ R$ для отношений
   a. $R = \{ (x, y) \mid (x, y \in \mathbb{N}) \wedge (x \vdots y) \}$ ($x \vdots y$ означает «x делит y»)
   b. $R = \{ (x, y) \mid (x, y \in \mathbb{N}) \wedge (y \vdots x) \}$
   c. $R = \{ (l, m) \mid (l, m - \text{прямые на плоскости}) \wedge (l \perp m) \}$
7. Доказать, что для любых бинарных отношений
   a. $R \cup R = R \cap R = R$
   b. $(R^{-1})^{-1} = R$
   c. $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$
   d. $(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1}$
   e. $\overline{R^{-1}} = \left(\overline{R}\right)^{-1}$
   f. $(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$
8. Доказать, что если $R_1 \subseteq R_2$, то $R_1^{-1} \subseteq R_2^{-1}$.
9. Доказать, что если отношения R_1 и R_2, заданные на множестве A, рефлексивны, то отношения $R_1 \cup R_2$, $R_1 \cap R_2$, R_1^{-1} и $R_1 \circ R_2$ тоже рефлексивны.
10. Доказать, что если отношения R_1 и R_2, заданные на множестве A, антирефлексивны, то отношения $R_1 \cup R_2$, $R_1 \cap R_2$ и R_1^{-1} тоже антирефлексивны. Показать, что композиция антирефлексивных отношений $R_1 \circ R_2$ может не быть антирефлексивной.
11. Доказать, что если отношения R_1 и R_2, заданные на множестве A, симметричны, то отношения $R_1 \cup R_2$, $R_1 \cap R_2$, R_1^{-1} и $R_1 \circ R_1$ тоже симметричны
12. Доказать, что если отношения R_1 и R_2, заданные на множестве A, антисимметричны, то отношения $R_1 \cap R_2$ и R_1^{-1} тоже антисимметричны.
13. Обозначим через I_A *тождественное* отношение на множестве A:
$$I_A = \{ (a, a) \mid a \in A \}.$$
Доказать, что для любых бинарных отношений R_1 и R_2 на множестве A
$$R_1 \cap R_2^{-1} \subseteq I_A \Leftrightarrow R_2 \cap R_1^{-1} \subseteq I_A.$$

14. Доказать, что если отношения R_1 и R_2, заданные на множестве A, антисимметричны, то отношение $R_1 \cup R_2$ антисимметрично тогда и только тогда, когда $R_1 \cap R_2^{-1} \subseteq I_A$.

2.3. Задачи для самостоятельного решения по теме 1.3

1. На вершину горы ведет 7 дорог. Сколькими способами можно подняться на гору и спуститься с нее? Дайте ответ на этот же вопрос, если спуск запрещается по той же дороге, по которой производился подъем.
2. Сколько 4-значных чисел можно составить из цифр 1, 2, 3, 4, 5, если:
   a. каждую из этих цифр можно использовать не более одного раза;
   b. цифры могут повторяться;
   c. цифры могут повторяться, а числа должны быть нечетными.
3. Сколько имеется 5-значных чисел, которые делятся на 5?
4. На одной из боковых сторон треугольника взято n точек на другой – m точек. Каждая из вершин при основании треугольника соединена прямыми с точками, взятыми на противоположной стороне. Сколько точек пересечения этих прямых образуется внутри треугольника? На сколько частей делят треугольник эти прямые?
5. Сколько существует 5-значных чисел, у которых все цифры нечетные?
6. Сколько существует 3-значных чисел, которые записываются с помощью цифр 0, 1, 2, 3, 4, 5 и которые делятся на 3?
7. В селении живут 1500 жителей. Доказать, что по крайней мере двое из них имеют одинаковые инициалы.
8. Сколько разных делителей имеет число $3^5 \times 5^4$?
9. Пусть $p_1, \dots, p_n$ – различные простые числа. Сколько делителей имеет число
$$m = p_1^{\alpha_1} \times \dots \times p_n^{\alpha_n},$$
где $\alpha_1, \dots, \alpha_n$ – некоторые натуральные числа?
10. Пассажир оставил вещи в автоматической камере хранения, а когда вернулся, чтобы их получить, обнаружил, что забыл номер. К счастью, он вспомнил, что в этом пятизначном номере присутствовали комбинации 23 и 57. Какое максимальное количество комбинаций ему придется набрать, чтобы открыть камеру?
11. Прямоугольная матрица размера $m \times n$ содержит только числа 1 и -1, причем произведение элементов каждой строки и каждого столбца равно 1. Сколько существует таких матриц?

12. В турнире принимали участие n шахматистов, и каждые два шахматиста сыграли по одной партии. Сколько было сыграно партий?
13. В скольких точках пересекаются диагонали выпуклого n-угольника, если никакие три диагонали не пересекаются в одной точке?
14. Сколько существует 4-значных чисел, у которых каждая следующая цифра больше предыдущей?
15. Сколько существует 4-значных чисел, у которых каждая следующая цифра меньше предыдущей?
16. Имеется p белых и q черных шаров. Сколькими способами можно выложить в ряд все шары так, чтобы никакие 2 черных шара не лежали рядом?
17. Используя идею шахматного города, доказать равенство (1.3.3) (треугольник Паскаля).
18. Используя идею шахматного города, доказать тождество
$$C_{2n}^{n} = (C_n^0)^2 + \cdots + (C_n^n)^2.$$
19. Сколькими способами можно упорядочить множество $\{1, 2, \dots, 2n\}$ так, чтобы каждое четное число имело четный номер?
20. Сколько существует перестановок из n элементов, в которых данные 2 элемента не стоят рядом?
21. Сколькими способами можно расположить 8 ладей на шахматной доске так, чтобы они не били друг друга?
22. Сколько существует перестановок из n элементов, в которых между двумя данными элементами стоят r элементов?
23. Сколькими способами можно рассадить n гостей за круглым столом?
24. Сколько существует перестановок чисел от 1 до n, в которых каждое число, кратное 2, и каждое число, кратное 3, имело, соответственно, позицию, кратную 2 и 3?
25. Сколько различных слов можно составить, переставляя буквы слова *шиншилла*?
26. С помощью формулы бинома Ньютона докажите равенства:
    a. $\sum_{i=0}^{k} C_n^i C_m^{k-i} = C_{n+m}^k$
    b. $\sum_{m=0}^{n} (-1)^m C_n^m = 0$

c. $\sum_{m=1}^{n} mC_n^m = n2^{n-1}$

d. $\sum_{m=2}^{n} m(m-1)C_n^m = n(n-1)2^{n-2}$

2.4. Задачи для самостоятельного решения по теме 1.4

1. Каково число булевых функций от n переменных, принимающих на противоположных наборах одинаковые значения?
2. Каково число булевых функций от n переменных, принимающих на любой паре соседних наборов противоположные значения?
3. Каково число булевых функций от n переменных, принимающих значение 1 менее, чем на k наборах?
4. По функциям $f(x_1, x_2)$ и $g(x_3, x_4)$, заданным векторно, построить векторное представление функции h:
   a. $f = (1011)$, $g = (1001)$, $h(x_2, x_3, x_4) = f(g(x_3, x_4), x_2)$.
   b. $f = (1101), g = (1001), h(x_1, x_2, x_3, x_4) = f(x_1, x_2) \vee g(x_3, x_4)$.
   c. $f = (1000), g = (0111), h(x_1, x_2, x_3, x_4) = f(x_1, x_2) \wedge g(x_3, x_4)$.
5. Функция $f(x_1, \dots x_n)$ называется *симметрической*, если
$$f(x_1, \dots, x_n) = f(x_{i_1}, \dots, x_{i_n})$$
для любой перестановки $(i_1, \dots, i_n)$. Найти число симметрических функций от n переменных.
6. Построить векторное представление для следующих формул:
   a. $\big(x \Rightarrow (z \oplus \overline{xy})\big) \downarrow \Big(\overline{x} \Rightarrow \big(z \Leftrightarrow (x \vee y)\big)\Big)$
   b. $\overline{xy \Rightarrow z} \Rightarrow y$
   c. $(\overline{xz} \oplus y) \Rightarrow \overline{y}$
   d. $\big((x \vee \overline{y}) \downarrow (x \oplus \overline{y})\big) \mid \big(xy \Rightarrow (\overline{x} \Leftrightarrow y)\big)$
   e. $(x \mid y) \mid (x \mid y)$
   f. $(x \downarrow y) \downarrow (x \downarrow y)$
   g. $(x \vee y) \Rightarrow (x \oplus y \oplus xy)$
   h. $\overline{x \mid y} \vee \big(1 \oplus (x \downarrow y)\big)$
7. Является ли функция g двойственной к функции f, если
   a. $f = x \oplus y,\ g = x \Leftrightarrow y$
   b. $f = x \Rightarrow y,\ g = y \Rightarrow x$

c. $f = (0001\ 1101),\ g = (0100\ 0111)$
d. $f = (0101\ 0011\ 0001\ 1110),\ g = (1000\ 0111\ 0011\ 1101)$

8. Является ли функция самодвойственной?
   a. $(x \oplus y) \vee (x \Leftrightarrow y)$
   b. $\overline{(x \Rightarrow y) \Rightarrow xz} \Rightarrow (y \Rightarrow z)$
   c. (00011101)
   d. (0101001100110101)
9. Построить СДНФ и СКНФ функций из задач 6a-c, 7c, 7d и 8b-d.
10. Минимизировать СДНФ из задачи 9 с помощью метода Квайна.
11. Построить тупиковую ДНФ с помощью геометрического метода для функций
    a. $\overline{xy \Rightarrow z} \Rightarrow y$
    b. $(\overline{xz} \oplus y) \Rightarrow \overline{y}$
    c. $(0111\ 1101)$
    d. $(0111\ 0111)$
12. Построить полином Жегалкина для функций из задач 6a-c и 8a,b.
13. Является ли функция линейной?
    a. $(x_1 \Leftrightarrow x_2) \oplus x_3$
    b. $x_1 x_2 (x_1 \oplus x_2)$
    c. $(x_1 \Rightarrow x_2)(x_2 \Rightarrow x_1) \oplus x_3$
    d. $(1010\ 1010\ 0110\ 1000)$
    e. $(1001\ 0110\ 1001\ 0110)$
    f. $(1001\ 0110\ 0110\ 1001)$
    g. $(0110\ 1001\ 1010\ 0101)$
14. Установить, каким из множеств $T_0 \cup T_1$ и $T_1 \backslash T_0$ принадлежат следующие функции:
    a. $((x \vee y) \Rightarrow (x \mid yz)) \downarrow ((z \Leftrightarrow z) \Rightarrow x)$
    b. $(xy \Rightarrow z) \downarrow ((x \oplus y) \mid (z \Leftrightarrow xy))$
    c. $(x_1 \Rightarrow x_2)(x_3 \Rightarrow x_1) \oplus x_2$
15. Является ли функция монотонной?
    a. $x \Rightarrow (x \Rightarrow y)$
    b. $x \Rightarrow (y \Rightarrow x)$
    c. $xy(x \oplus y)$

d. $xy \oplus yz \oplus zx \oplus z$
e. $(0011\ 0111)$
f. $(0110\ 0111)$
g. $(0001\ 0101\ 1010\ 0111)$
h. $(0000\ 0000\ 1011\ 1111)$

16. Является ли система функций полной?
    a. $\{ x \Rightarrow y,\ \ x \Rightarrow \overline{y}z \}$
    b. $\{ x\overline{y},\ \ \overline{x} \Leftrightarrow yz \}$
    c. $\{ 0,\ \ x \Rightarrow y \}$
    d. $\{ (0110\ 1001),\ \ (1000\ 1101),\ \ (0001\ 1100) \}$

3. РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ

По избранным разделам учебной дисциплины «Дискретная математика и математическая логика» для проверки теоретических знаний в системе автоматического тестирования InsightRunner https://acm.bsu.by/ разработаны тестовые задания.

Тест может включать задания разных видов: вопросы, где нужно выбрать один правильный ответ из предложенных; вопросы, где правильных ответов несколько и требуется отметить множество вариантов; вопросы, где нужно ввести текстовый ответ.

Отвечать на вопросы можно в любом порядке, все ответы автоматически сохраняются. Система ведёт учет времени.

Отличительной особенностью InsightRunner является использование автоматизированных генераторов. Это позволяет создать большую базу вопросов для тестов. Каждый студент получает уникальный набор заданий, тем самым исключается возможность списывания.

Студенты в Образовательной платформе InsightRunner выполняют тестовые задания, преподаватель проводит разбор допущенных ошибок.

В рамках самоконтроля студенты имеют возможность выполнять тестовые задания в удобное для них время из дома/общежития, видеть правильно или нет они ответили, а также ознакомиться с правильными вариантами ответов.

Учебная дисциплина «Дискретная математика и математическая логика» завершается прохождением итогового теста, который, как правило, содержит 20 вопросов по основным разделам дисциплины и рассчитан на 30 минут. При прохождении итогового теста студентам не разрешено пользоваться вспомогательными материалами.

Примеры тестовых заданий

Тест 1. Введение в математическую логику. Логические операции.

Для высказывания «Четность суммы есть необходимое условие четности каждого слагаемого» выберите равносильное ему высказывание:

☒ Если каждое слагаемое чётное, то сумма чётная.

Если сумма чётная, то каждое слагаемое чётное.

Тест 2. Введение в математическую логику. Равносильные формулы.

Для формулы $\overline{A} \vee \overline{B}C$ выберите равносильные ей формулы:

☒ $\overline{A \wedge (\overline{B} \Rightarrow \overline{C})}$

☒ $A \Rightarrow C(\overline{B} \vee \overline{A})$

$(A \vee \overline{B})(\overline{A} \vee C)$
$A \wedge C \vee (A \Rightarrow (B \Rightarrow C))$

Тест 3. Логические операции. Логическое уравнение.

Решите следующее логическое уравнение:

$$\overline{C} \wedge A \wedge (C \Rightarrow \overline{A} \wedge B \wedge \overline{C}) = 1.$$

В качестве ответа выпишите лексикографически минимальный набор значений переменных A, B, C, например 101. Гарантируется, что решение существует.

Ответ: 100

Тест 4. Введение в математическую логику. Логические следствия.

Выберите верные логические следствия.

- ☐ $(p \Rightarrow q), (q \Rightarrow r) \vdash r$
- ☐ $(p \Rightarrow q), (p \Rightarrow r), (q \vee r) \vdash p$
- ☒ $(p \Rightarrow q), (p \Rightarrow r), \overline{qr} \vdash \overline{p}$
- ☐ $(\overline{p} \vee \overline{q}), (r \vee \overline{q}), \overline{p} \vdash r \vee \overline{p}$
- ☐ $(c \Rightarrow (b \vee a)), (a \Rightarrow (c \vee b)), (b \vee a) \vdash ((a \vee b) \Rightarrow c)$

Тест 5. Множества и отношения. Равные множества.

Выберите множества, равные множеству $(C \oplus A) \setminus B$.

- ☒ $(C \cup (B \oplus C)) \oplus (B \cup A)$
- ☒ $((B \cup C) \oplus B) \oplus (A \setminus B)$
- ☐ $(A \cup (B \oplus C)) \setminus (\overline{A} \setminus C)$
- ☐ $\left(\overline{C \oplus \overline{A}} \setminus (C \oplus B)\right) \cap \overline{A}$
- ☐ $\left(((B \oplus C) \oplus B) \setminus A\right) \cup \overline{C}$

Тест 6. Множества и отношения. Декартово произведение множеств.

Пусть имеются следующие множества:

$A = \{3, 4, \ldots, 20\}$
$B = \{19\}$
$C = \{8, 9, \ldots, 15\}$
$D = \{12, 13, \ldots, 19\}$

Найдите $|(A \oplus C) \times (B \cap D)|$.

Ответ: 10

Тест 7. Булевы функции. СДНФ.

Выберите конъюнкции, которые содержатся в совершенной дизъюнктивной нормальной форме функции $f = (y \oplus z) \mid \left(\overline{y \vee (x \mid z)} \Leftrightarrow (y \downarrow z)\right)$:

- ☒ $x\overline{y}z$
- ☒ xyz
- ☒ $x\overline{y}\,\overline{z}$
- ☒ $\overline{x}\,\overline{y}\,\overline{z}$
- ☐ $\overline{x}\,\overline{y}\,z$

Тест 8. Булевы функции. Полином Жегалкина.

Выберите слагаемые, которые содержатся в полиноме Жегалкина для функции $f = \left(x_1 \downarrow (x_3 \oplus x_2)\right) \downarrow \left(x_3 \oplus (\overline{x}_1 \downarrow x_2 x_1)\right)$:

- ☒ 1
- ☐ x_2
- ☒ x_1
- ☒ $x_1 x_2$
- ☒ x_3

Тест 9. Булевы функции. Функционально полные системы функций.

Выберите все полные системы функций.

- ☒ $\{(1100), (01010111)\}$
- ☒ $\{(0010), (10100100)\}$
- ☒ $\{(0110), (11011000)\}$
- ☒ $\{(0110), (11100111)\}$
- ☐ $\{(1001), (10010011)\}$

Тест 10. Комбинаторика. Сочетания.

В скольких точках пересекаются диагонали выпуклого 10-угольника, если никакие три диагонали не пересекаются в одной точке?

- ☐ 1024
- ☐ 340
- ☐ 98
- ☒ 210
- ☐ 212

Тест 11. Комбинаторика. Перестановки и размещения.

Имеется 15 белых и 13 черных шаров. Сколькими способами можно выложить в ряд все шары так, чтобы никакие 2 черных шара не лежали рядом?

- 512
- ☒ 560
- 484
- 617
- 798

Преподаватель, комбинируя категории вопросов, может создавать шаблоны тестов для итоговой проверки теоретических знаний студентов по совокупности разделов учебной дисциплины.

Тест 12. Комбинаторика. Перестановки и размещения.

Сколько существует перестановок из 12 элементов, в которых между двумя данными элементами стоят 3 элемента?

- 206
- ☒ 160
- 98
- 192
- 180

Преподаватель, комбинируя категории вопросов, может создавать шаблоны тестов для итоговой проверки теоретических знаний студентов по совокупности разделов учебной дисциплины.

Образовательная платформа InsightRunner функционирует в рамках учебной дисциплины с 2003 года и доказала свою эффективность на практике. Возможность круглосуточной самостоятельной работы студентов на базе образовательной платформы InsightRunner способствует получению высоких результатов на соревнованиях в области алгоритмизации и спортивного программирования и повышению позиции БГУ в мировых рейтингах.

Результатом внедрения платформы в учебный процесс стала повышенная заинтересованность в практических занятиях по учебной дисциплине «Дискретная математика и математическая логика» как со стороны учащихся, так и со стороны преподавателей [3].

4. ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ

4.1. Рекомендуемая литература

Основная литература

1. Андерсен, Дж. А. Дискретная математика и комбинаторика / Дж. А. Андерсен. – М: Вильямс, 2020. – 960 с.

2. Ерусалимский, Я. М. Дискретная математика. Теория и практикум : учебник / Я. М. Ерусалимский. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2018. – 472 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/212897.

3. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. - 3-е изд., стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2022. – 112 с. – Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/247400.

4. Игнатьев, А. В. Теория графов. Лабораторные работы: учебное пособие для студентов, обучающихся по направлению подготовки «Информационные системы и технологии» / А. В. Игнатьев. – 1-е изд. – СанктПетербург : Лань, 2022 – 64 с. – URL: https://ibooks.ru/bookshelf/354021.

5. Лекции по теории графов : учебное пособие для студ., обуч. по спец. "Математика" и "Прикладная математика" / В. А. Емеличев [и др.]. – Изд. стер. – Москва : URSS : ЛЕНАНД, 2021. – 383 с.

6. Поттосин, Ю. В. Основы дискретной математики и теории алгоритмов : учебно-методическое пособие для специальности 1-40 05 01 "Информационные системы и технологии (по направлениям)" / Ю. В. Поттосин, Т. Г. Пинчук, С. А. Поттосина ; М-во образования Республики Беларусь, БГУИР, Инженерно-экономический факультет, Кафедра экономической информатики. – Минск : БГУИР, 2021. – 121 с.

Дополнительная литература

7. Авдошин, С. М. Дискретная математика. Формально-логические системы и языки / С. М. Авдошин, А. А. Набебин ; [науч. ред. В. А. Захаров]. – Москва : ДМК Пресс, 2018. https://znanium.com/catalog/product/1027772. - 389 с. - URL:

8. Алексеев, В. Е. Графы и алгоритмы. Структуры данных. Модели вычислений / В. Е. Алексеев, В. А. Таланов. – М.: Бином, 2012. – 320 с.

9. Верещагин, Н. К. Лекции по математической логике и теории алгоритмов (в трех частях) / Н. К. Верещагин, А. Х. Шень. – М.: МЦНМО, 2012.

10. Гладкий, А. В. Введение в современную логику. Учебное пособие / А. В. Гладкий. – М.: Либроком, 2016. – 238 с.

11. Глухов, М. М. Математическая логика. Дискретные функции. Теория алгоритмов / М. М. Глухов, А. Б. Шишков. – Спб.: Лань, 2012. – 416 с.

12. Громкович, Ю. Теоретическая информатика. Введение в теорию автоматов, теорию вычислимости, теорию сложности, теорию алгоритмов, рандомизацию, теорию связи и криптографию / Ю. Громкович. – Спб.: БХВ-Петербург, 2010. – 338 с. 12

13. Грэхем, Р. Конкретная математика. Математические основы информатики / Р. Грэхем, Д. Кнут, О. Паташник. – М.: Вильямс, 2016. – 784 с.

14. Гэри, М. Вычислительные машины и труднорешаемые задачи / М. Гэри, Д. Джонсон. – М.: Книга по Требованию, 2012. – 420 с.

15. Емеличев, В. А., Зверович, И. Э., Мельников, О. И и др. Теория графов в задачах и упражнениях. / В. А. Емеличев и др. –Москва: Лаиброком, 2013. – 416 с.

16. Зуев, Ю. А. По океану дискретной математики: учебное пособие в двух частях / Ю. А. Зуев. – М.: Ленанд, 2017.

17. Зюзьков, В. М. Введение в математическую логику : учебное пособие / В. М. Зюзьков. - Изд. 2-е, испр. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2018. - 265 с.- URL: https://e.lanbook.com/book/213008.

18. Игошин, В. И. Теория алгоритмов: учеб. пособие / В. И. Игошин. – М.: ИНФРА-М, 2016. – 318 с.

19. Игошин, В. И. Математическая логика и тория алгоритмов. Сборник задач. Учебное пособие / В. И. Игошин. – М.: Инфра-М, 2017. – 392с.

20. Карпов, Ю.Г. Теория автоматов. / Ю.Г. Карпов. – СПб.: Питер, 2002. – 224 с.

21. Когабаев, Н. Т. Лекции по теории алгоритмов: Учебное пособие / Н. Т. Когабаев. – Новосибирск: НГУ, 2009. – 107 с.

22. Крупский, В.Н. Введение в сложность вычислений / В. Н. Крупский. – М.: Факториал Пресс, 2006. – 128 с.

23. Крупский, В. Н. Теория алгоритмов / В. Н. Крупский, В. Е. Плиско. – М.: Academia, 2009. – 208 с.

24. Кудрявцев, В. Б. Теория автоматов. Учебник / В. Б. Кудрявцев, С. В. Алешин, А. С. Подколзин. – М.: Юрайт, 2017. – 320 с.

25. Марченков, С. С. Конечные автоматы / С. С. Марченков. – М.: Физматлит, 2008. – 56 с.

26. Мозговой, М. В. Классика программирования: алгоритмы, языки, автоматы, компиляторы. Практический подход / М. В. Мозговой. – СПб.: Наука и Техника, 2006. – 320 с.

27. Новиков, Ф. А. Дискретная математика : для бакалавров и магистров : учебник для студ. вузов, обуч. по напр. подготовки "Системный анализ и управление" / Ф. А. Новиков. — 3-е изд. — Санкт-Петербург [и др.] : Питер, 2017. – 493с. –URL: https://ibooks.ru/bookshelf/354021.

28. Папшев, С. В. Дискретная математика. Курс лекций для студентов естественнонаучных направлений подготовки : учебное пособие / С. В. Папшев. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2019. - 189 с. - URL: https://e.lanbook.com/book/206210

29. Пентус, А. Е. Математическая теория формальных языков: Учебное пособие / А. Е. Пентус, М. Р. Пентус. – М.: Бином, 2012. – 247 с.
30. Писарук, Н. Н. Сложность вычислений и криптография / Н. Н. Писарук. – Мн.: БГУ, 1999. – 230 с. 23. Рейуорд-Смит, В. Дж. Теория формальных языков: вводный курс / В. Дж. Рейуорд-Смит. – М.: Радио и связь, 1988. – 128 с. 13
31. Хопкрофт, Дж. Э. Введение в теорию автоматов, языков и вычислений / Дж. Э. Хопкрофт, Р. Мотвани, Дж. Ульман. – М.: Вильямс/Диалектика, 2019. – 528 с.
32. Эндрюс Г. Теория разбиений. / Г. Эндрюс. – М.: Наука, 1982. 256 с.
33. Яблонский, С. В. Введение в дискретную математику. Учебное пособие для вузов. /С. В. Яблонский — 6-е изд.— М.: Высшая школа, 2010. — 38 с.
34. Lewis, H. R. Elements of the theory of computation / H. R. Lewis, C. H. Papadimitriou. – New Jersey: Prentice-Hall, Inc., 1997. – 361 p.

4.2. Электронные ресурсы

1. Образовательный портал БГУ [Электронный ресурс]. – Режим доступа: https://edufpmi.bsu.by/course/view.php?id=96. – Дата доступа: 09.04.2025.
2. Образовательная платформа Insight Runner [Электронный ресурс]. – Режим доступа: https://acm.bsu.by. – Дата доступа: 09.04.2025.
3. Опыт использования образовательной платформы Insight Runner на факультете прикладной математики и информатики Белорусского государственного университета. Роль университетского образования и науки в современном обществе : материалы междунар. науч. конф., Минск, 26–27 февр. 2019 г. / редкол.: А. Д. Король (пред.) [и др.]. – Минск : БГУ, 2019. – С. 263 – 267. Электронный ресурс]. – Режим доступа: https://elib.bsu.by/handle/123456789/231914. – Дата доступа: 09.04.2025.
4. Котов, В.М. Дискретная математика. Специальный курс : пособие для студентов спец. 1-31 03 04 «Информатика» / В.М. Котов, В.А. Мощенский. – Минск: БГУ, 2010. – 115 с. – Режим доступа: https://elib.bsu.by/handle/123456789/4686. – Дата доступа: 05.04.2025.
5. Мощенский, В.А. Избранные главы дискретной математики в утверждениях и упражнениях : пособие для студентов, обучающихся по спец. 1-31 03 04 «Информатика». – Минск : БГУ, 2012. – 168 с. – Режим доступа: https://elib.bsu.by/handle/123456789/53731. – Дата доступа: 05.04.2025.