

УДК 519.854(073)

ББК 22.176я73

Ш48

Рецензент: Заслуженный деятель науки Удмуртской Республики,
доктор техн. наук, профессор *В. М. Колодкин*

Шептунов М. В.

Ш48 Дискретная математика для бакалавриата. Учебное пособие
для вузов. – М.: Горячая линия – Телеком, 2017. – 114 с.: ил.

ISBN 978-5-9912-0659-4.

В краткой форме доступно изложены основы дискретной математики. Рассмотрены основы теории множеств, уделено внимание комбинаторному и теоретико-множественному подходам. Рассмотрены элементы математической логики. Изложены основные методы и подходы теории графов. Рассмотрены специальные маршруты в графах и поиск путей. Раскрыты основные вопросы теории кодирования. Наряду с основополагающими понятиями – кодами Грея и Хемминга уделено внимание применению алгоритма RSA в режимах шифрования и электронной цифровой подписи.

Пособие подготовлено в соответствии с разработанными автором рабочими программами Финансового университета (ФГОБУ ВО «Финансовый университет при Правительстве РФ»)

Для студентов, обучающихся по направлениям подготовки бакалавров 10.03.01 – «Информационная безопасность», 09.03.03 – «Прикладная информатика», 38.03.05 – «Бизнес-информатика»

ББК 22.176я73

Учебное издание

Шептунов Максим Валерьевич

Дискретная математика для бакалавриата

Учебное пособие для вузов

Тиражирование книги начато в 2017 г.

Все права защищены.

Любая часть этого издания не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения правообладателя

© ООО «Научно-техническое издательство «Горячая линия – Телеком»

www.techbook.ru

© М. В. Шептунов

Оглавление

Введение	3
1. Множества, отношения и функции	5
1.1. Множества и способы их задания	5
1.1.1. Базовые понятия теории множеств	5
1.1.2. Кортежи и прямое произведение множеств	8
1.1.3. Способы задания множеств и особенности их применения	11
1.1.4. Теоретико-множественный парадокс Рассела и возможности его преодоления	12
1.2. Операции над множествами и диаграммы Эйлера–Венна	13
1.3. Комбинаторный принцип включений и исключений	18
1.3.1. Формулировка принципа включений и исключений в общем случае и для некоторых частных его случаев	18
1.3.2. Доказательство комбинаторного принципа включений и исключений	19
1.4. Отношения	20
1.4.1. Бинарные отношения	20
1.4.2. Отношение эквивалентности	21
1.4.3. Отношение порядка	22
1.4.4. Отношение доминирования	23
1.4.5. Унарные и n -местные отношения	23
1.5. Соответствия	23
1.6. Отображения	25
1.7. Функции	26
1.7.1. Полная и частичная функции	26
1.7.2. Обратная функция	27
1.7.3. Инъективная, сюръективная и биективная функции	27
1.8. Элементы комбинаторного анализа	28
1.8.1. Перестановки, размещения и сочетания	28
1.8.2. Разбиения	29
1.8.3. Взаимосвязь между перестановками с повторениями и отображением	30
1.9. Средневзвешенное по элементам множества	31
1.10. Принцип (метод) математической индукции	32
1.10.1. Формулировка принципа (метода) математической индукции и его доказательство	32
1.10.2. Формулировка принципа (метода) строгой математической индукции	33

1.10.3. Особенности и примеры применения принципа (метода) математической индукции	33
Вопросы для самоконтроля	34
1.11. Решение задач	35
Литература к главе 1	38
2. Элементы математической логики	39
2.1. Основные законы математической логики, булевы функции и таблицы истинности	39
2.1.1. Основные законы математической логики	39
2.1.2. Булевы функции и приоритет логических операций	40
2.1.3. Таблицы истинности	41
2.1.4. Сводная таблица логических функций двух переменных	42
2.2. Логика высказываний и язык математической логики .	43
2.2.1. Простые высказывания	43
2.2.2. Сложные (составные) высказывания	43
2.2.3. Эквивалентные высказывания и замена операций импликации и эквивалентности	43
2.2.4. Упрощение сложных высказываний	44
2.3. Взаимосвязь между языком математической логики и алгеброй множеств	44
2.3.1. Тожества алгебры множеств	44
2.3.2. Язык математической логики и алгебра множеств	45
2.3.3. Доказательства логико-математических выражений на основе диаграмм Эйлера-Венна	45
2.3.4. Доказательства логико-математических выражений путём построения таблицы истинности для левой и правой частей	45
2.3.5. Доказательство логико-математических выражений путём правильных логических рассуждений	46
2.4. Логические сети и контактные схемы	47
2.4.1. Логические сети	47
2.4.2. Релейно-контактные схемы и возможности их использования	47
2.4.3. Анализ и синтез логических сетей с применением функции проводимости	48
2.5. Предикаты	49
2.5.1. Отличие предикатов от высказываний и основные понятия логики предикатов	49
2.5.2. Предикаты и кванторы	50
2.6. Исчисление предикатов (первого порядка)	51
2.6.1. Основные понятия исчисления предикатов	51
2.6.2. Правила вывода в исчислении предикатов (первого порядка)	54
Вопросы для самоконтроля	55

2.7. Решение задач	56
Литература к главе 2	57
3. Элементы теории графов	58
3.1. Основные понятия теории графов	58
3.1.1. Диаграммы графов	58
3.1.2. Типы графов, ориентированные и неориентированные графы	59
3.1.3. Элементы графов; подграф и частичный граф	60
3.1.4. Понятия инцидентности и валентности в теории графов	61
3.1.5. Понятие маршрута, цепи и цикла в графе	61
3.2. Задача о кёнигсберских мостах; эйлеровы и гамильтоновы циклы	62
3.2.1. Задача о кёнигсбергских мостах	62
3.2.2. Понятие уникурсального графа	63
3.2.3. Теорема Эйлера о сумме степеней вершин графа и её доказательство	63
3.2.4. Эйлеровы и гамильтоновы циклы	63
3.3. Деревья	64
3.3.1. Дерево как частный случай графа	64
3.3.2. Применение деревьев в экономике и информатике	65
3.3.3. Применение деревьев в сфере информационной безопасности	66
3.4. Диаметр, радиус и центр графа	66
3.4.1. Понятия диаметра графа и эксцентриситетов	66
3.4.2. Диаметр графа и центр графа	67
3.4.3. Метрические характеристики графов и задачи размещения	67
3.5. Специальные маршруты в графах	67
3.5.1. Латинские свойства путей в графах	67
3.5.2. Метод латинской композиции и его применение	68
3.6. Планарные графы	69
3.6.1. Понятие планарного графа и плоского изображения графа	69
3.6.2. Критерий планарности графа	70
3.6.3. Применение планарных графов	70
3.7. Обходы деревьев и стратегии поиска в глубину и ширину	71
3.7.1. Обходы деревьев	71
3.7.2. Стратегии поиска в глубину и ширину	71
3.7.3. Особенности и основные возможности применения стратегий поиска в глубину и ширину	72
3.8. Матрицы смежности и инцидентий графа	72
3.8.1. Матрица смежности	72

3.8.2. Матрица инцидентов (инцидентности)	73
Вопросы для самоконтроля	73
3.9. Решение задач	74
Литература к главе 3	78
4. Элементы теории кодирования	80
4.1. Двоичное кодирование и коды Грея и Хемминга	80
4.1.1. Позиционные системы счисления и переход от десятичной к двоичной системе и обратно	80
4.1.2. Понятия кодов постоянной и переменной длины и кодов с проверкой чётности	81
4.1.3. Коды Грея и Хемминга	86
4.1.4. Управление доступом в компьютерную систему по матричному принципу как задача о назначениях	89
4.2. Однонаправленные функции и однонаправленные функции с секретом	92
4.2.1. Понятия трудно решаемых задач и стойких шифров ...	92
4.2.2. Однонаправленные функции	94
4.2.3. Однонаправленные функции с секретом	95
4.3. Алгоритм RSA в режиме шифрования	96
4.3.1. Понятие о криптосистеме с открытым ключом	96
4.3.2. Применение алгоритма RSA в режиме шифрования ...	97
4.4. Алгоритм RSA в режиме электронной цифровой подписи	98
4.4.1. Понятие об электронной цифровой подписи	98
4.4.2. Применение алгоритма RSA в режиме электронной цифровой подписи	99
Вопросы для самоконтроля	100
4.5. Решение задач	100
Литература к главе 4	103
Пример выполнения приближенного к типовому варианту контрольной работы с решением	105
Заключение	110