

БАКАЛАВР. АКАДЕМИЧЕСКИЙ КУРС

С. Б. Гашков, А. Б. Фролов

# ДИСКРЕТНАЯ МАТЕМАТИКА

УЧЕБНИК и ПРАКТИКУМ



СООТВЕТСТВУЕТ  
ПРОГРАММАМ  
ВЕДУЩИХ НАУЧНО-  
ОБРАЗОВАТЕЛЬНЫХ  
ШКОЛ

**Юрайт**  
Издательство

УМО ВО рекомендует

[biblio-online.ru](http://biblio-online.ru)

С. Б. Гашков, А. Б. Фролов

# ДИСКРЕТНАЯ МАТЕМАТИКА

УЧЕБНИК И ПРАКТИКУМ  
ДЛЯ АКАДЕМИЧЕСКОГО БАКАЛАВРИАТА

*Рекомендовано Учебно–методическим отделом высшего образования  
в качестве учебника для студентов высших учебных заведений,  
обучающихся по естественнонаучным направлениям и специальностям*

Книга доступна в электронной библиотечной системе  
[biblio-online.ru](http://biblio-online.ru)

Москва ■ Юрайт ■ 2016

УДК 51(075.8)  
ББК 22.176я73  
Г24

**Авторы:**

**Гашков Сергей Борисович** — доктор физико-математических наук, профессор кафедры дискретной математики отделения математики механико-математического факультета Московского государственного университета имени М. В. Ломоносова;

**Фролов Александр Борисович** — профессор, доктор технических наук, профессор кафедры математического моделирования Института автоматизации и вычислительной техники Национального исследовательского университета «Московский энергетический институт».

**Рецензенты:**

**Бабаш А. В.** — профессор, доктор физико-математических наук, профессор кафедры информационной безопасности Национального исследовательского университета «Высшая школа экономики»;

**Вагин В. Н.** — профессор, доктор технических наук, профессор кафедры прикладной математики Национального исследовательского университета «Московский энергетический институт».

**Гашков, С. Б.**

Г24 Дискретная математика : учебник и практикум для академического бакалавриата / С. Б. Гашков, А. Б. Фролов. — М. : Издательство Юрайт, 2016. — 423 с. — Серия : Бакалавр. Академический курс.

ISBN 978-5-9916-6382-3

В книге отражены разделы дискретной математики, предусматриваемые учебными программами классических, национальных исследовательских и технических университетов. При соблюдении необходимого уровня доказательности рассматриваются задачи, встречающиеся в инженерной практике, для формализации которых необходимы математические модели дискретной математики — теоретико-множественные, комбинаторно-логические, автоматные, графовые, функциональные, алгебраические и др. Существенное внимание уделено принципам построения алгоритмов решения задач дискретной математики на базе известных моделей вычислений (рекурсия, ветвления и ограничения и т.п.) и оценкам их сложности в контексте общей теории сложности алгоритмов. По каждому разделу даны задачи и теоретические упражнения.

Соответствует актуальным требованиям Федерального государственного образовательного стандарта высшего образования.

*Для студентов, слушателей факультетов повышения квалификации, специалистов, преподавателей и программистов, использующих методы дискретной математики.*

УДК 51(075.8)  
ББК 22.176я73



*Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав. Правовую поддержку издательства обеспечивает юридическая компания «Дельфи».*

ISBN 978-5-9916-6382-3

© Гашков С. Б., Фролов А. Б., 2016  
© ООО «Издательство Юрайт», 2016

## Оглавление

<b>Предисловие</b> .....	<b>7</b>
<b>Глава 1. Множества и отношения</b> .....	<b>11</b>
1.1. Множества и булеаны .....	11
1.2. Отношения .....	15
1.2.1. Соответствия .....	16
1.2.2. Гомоморфизм и изоморфизм .....	18
1.2.3. Однородные бинарные отношения .....	19
<i>Задачи</i> .....	21
<b>Глава 2. Функции алгебры логики</b> .....	<b>22</b>
2.1. Основные определения.....	22
2.2. Разложение булевых функций по переменным .....	28
2.3. Теорема о полноте .....	33
2.4. Минимизация булевых функций.....	38
2.5. Геометрическая интерпретация дизъюнктивной нормальной формы .....	43
2.6. Минимизация систем функций алгебры логики.....	48
<i>Задачи</i> .....	52
<b>Глава 3. Алгебры высказываний, предикатов и множеств</b> .....	<b>54</b>
3.1. Алгебра высказываний.....	54
3.2. Алгебра предикатов .....	58
3.3. Алгебра множеств .....	60
<i>Задачи</i> .....	61
<b>Глава 4. Отношения эквивалентности и частичного порядка</b> .....	<b>62</b>
4.1. Отношения эквивалентности .....	62
4.2. Ядерная эквивалентность и каноническое разложение.....	64
4.3. Отношения частичного порядка.....	65
4.4. Многокритериальная оптимизация .....	68
4.5. Решетки .....	69
4.6. Булевы решетки .....	70
<i>Задачи</i> .....	73
<b>Глава 5. Комбинаторика</b> .....	<b>74</b>
5.1. Основные принципы комбинаторики .....	74
5.2. Разбиения, сочетания с повторениями и биномиальные коэффициенты ...	79
5.3. Формула включения-исключения и числа Стирлинга .....	80
5.4. Числа Фибоначчи .....	87
5.5. Рекуррентные последовательности.....	89
5.6. Производящие функции .....	99

5.7. Числа Стирлинга и взаимно-обратные преобразования .....	102
5.8. Задача Эйлера о размене монет и разбиение чисел на слагаемые .....	106
5.9. Числа Каталана.....	112
5.10. Линейные рекуррентные последовательности и производящие функции .....	115
5.11. Шары в ящиках: 12 вариантов задачи .....	123
5.12. Статистики перестановок.....	125
5.13. Производящие функции множеств и языков .....	128
5.14. Формула обращения Мёбиуса.....	131
<i>Задачи</i> .....	133
<b>Глава 6. Графы .....</b>	<b>137</b>
6.1. Основные понятия .....	137
6.2. Операции над графами. Подграфы.....	143
6.3. Фундаментальные циклы и разрезы графа .....	146
6.4. Обходы графа и орграфа .....	150
6.5. Связность графов и орграфов .....	156
6.6. Множества внешней и внутренней устойчивости .....	161
6.7. Раскраска графов .....	164
6.8. Паросочетания в двудольных графах .....	169
6.9. Плоские графы. Критерии планарности графа.....	173
6.10. Потоки в сетях.....	177
<i>Задачи</i> .....	183
<b>Глава 7. Логика предикатов .....</b>	<b>186</b>
7.1. Формулы логики предикатов.....	186
7.2. Преобразование предикатов .....	190
7.3. Эквивалентные преобразования формул.....	192
7.4. Общезначимые и противоречивые формулы .....	196
7.5. Логические следствия .....	200
<i>Задачи</i> .....	201
<b>Глава 8. Логические схемы.....</b>	<b>203</b>
8.1. Схемы из функциональных элементов и логические схемы .....	203
8.2. Сложность схемы. Минимальные схемы .....	209
8.3. Некоторые элементарные методы синтеза .....	212
8.4. Функция Шеннона. Оценки Шеннона – Лупанова .....	214
8.5. Синтез схем методом каскадов .....	219
8.6. Декомпозиционные методы синтеза.....	221
8.6.1. Понятие декомпозиции .....	221
8.6.2. Использование нетривиальной декомпозиции.....	224
8.6.3. Использование программируемых логических матриц.....	228
8.7. Контактные схемы.....	231
8.8. Тестирование логических схем.....	237
<i>Задачи</i> .....	240
<b>Глава 9. Конечные автоматы .....</b>	<b>242</b>
9.1. Основные понятия .....	242

9.2. Эквивалентность автоматов .....	248
9.3. Изоморфизм автоматов .....	251
9.4. Минимизация автоматов .....	252
9.5. Регулярные события и регулярные выражения .....	256
9.6. Регулярность событий, представимых автоматами .....	257
9.7. Представление регулярного события автоматом .....	259
9.8. Схемы с обратной связью .....	263
<i>Задачи</i> .....	267
<b>Глава 10. Теория алгоритмов и вычислимых функций .....</b>	<b>269</b>
10.1. Машины Тьюринга .....	269
10.2. Тьюрингово программирование и тьюринговы диаграммы .....	274
10.3. Алгоритмически неразрешимые проблемы .....	276
10.4. Вычисления на абакe .....	279
10.5. Рекурсивные функции .....	281
10.6. Универсальные функции .....	285
10.7. Разрешимые и перечислимые множества и предикаты .....	287
10.8. Формальные системы и алгоритмы Маркова .....	289
10.8.1. Формальные системы .....	289
10.8.2. Нормальные алгоритмы Маркова .....	295
<i>Задачи</i> .....	297
<b>Глава 11. NP-полные задачи .....</b>	<b>299</b>
11.1. Схемы, предикаты и конъюнктивные нормальные формы .....	299
11.2. Моделирование машин Тьюринга булевыми схемами .....	303
11.3. Классы <i>P</i> и <i>NP</i> . Теорема Кука .....	307
11.4. NP-полные задачи .....	310
11.5. Частные случаи NP-полных задач .....	318
11.6. Алгоритмы для точного решения некоторых NP-полных задач .....	325
11.6.1. Динамическое программирование .....	326
11.6.2. Псевдополиномиальные алгоритмы .....	328
11.6.3. Метод ветвей и границ .....	329
11.7. Приближенные алгоритмы решения NP-полных задач .....	331
11.7.1. Жадные алгоритмы .....	331
11.7.2. Полиномиальные алгоритмы с ограниченной погрешностью .....	335
11.7.3. Алгоритмы локальной минимизации .....	339
<i>Задачи</i> .....	341
<b>Глава 12. Конечные поля и эллиптические кривые .....</b>	<b>346</b>
12.1. Группы, кольца, поля и многочлены .....	346
12.2. Конечные поля .....	359
12.2.1. Мультипликативная группа поля .....	361
12.2.2. Подполя и расширения .....	362
12.2.3. Неприводимые и примитивные многочлены .....	366
12.3. Эллиптические кривые .....	369
<i>Задачи</i> .....	378

<b>Глава 13. Теория кодов, исправляющих ошибки .....</b>	<b>379</b>
13.1. Основные понятия .....	379
13.1.1. Двоичные коды .....	379
13.1.2. $q$ -Ичные коды и границы сферической упаковки .....	382
13.1.3. Линейные коды. Порождающие и проверочные матрицы .....	385
13.2. Коды Хемминга .....	388
13.2.1. Коды Хемминга как циклические коды .....	390
13.2.2. $q$ -Ичные коды Хемминга .....	395
13.3. Коды Рида – Соломона .....	396
13.4. Коды Боуза – Чоудхури – Хоквингема .....	399
13.5. Матричное определение кодов Боуза – Чоудхури – Хоквингема и Рида – Соломона .....	401
13.6. Исправление двух ошибок .....	404
13.7. Определение позиций ошибок в общем случае методом Питерсона .....	404
<i>Задачи</i> .....	408
<b>Глава 14. Криптографические приложения .....</b>	<b>410</b>
14.1. Линейная рекуррентная последовательность и ее характеристический многочлен .....	410
14.1.1. Основные понятия .....	410
14.1.2. Автоматная интерпретация линейной рекуррентной последовательности .....	411
14.1.3. Статистические свойства линейной рекуррентной последовательности .....	413
14.1.4. След элемента конечного поля .....	414
14.1.5. Формула общего члена линейной рекуррентной последовательности .....	415
14.2. Электронная цифровая подпись .....	417
14.2.1. Понятие, назначение и свойства цифровой подписи .....	417
14.2.2. О российском стандарте цифровой подписи 2012 года .....	419
<i>Задачи</i> .....	420
<b>Литература .....</b>	<b>422</b>