



Глухов М. М., Шишков А. Б.
Математическая логика. Дискретные функции. Теория алгоритмов: Учебное пособие. 1-е изд.

Рекомендовано УМО вузов России по образованию в области информационной безопасности в качестве учебного пособия для студентов вузов, обучающихся по направлению подготовки (специальности) 090301 — «Компьютерная безопасность» и 090303 — «Информационная безопасность автоматизированных систем»

ISBN 978-5-8114-1344-7

Год выпуска 2012

Тираж 1500 экз.

Формат 12,8×20 см

Переплет: твердый

Страниц 400

Цена 669,90 руб.

Учебное пособие содержит полное изложение материала учебных дисциплин «Математическая логика и теория алгоритмов» и «Дискретные функции» Государственного образовательного стандарта высшего профессионального образования по специальностям «Компьютерная безопасность», «Информационная безопасность автоматизированных систем» и некоторым другим смежным специальностям.

Пособие состоит из трех взаимосвязанных частей, составляющих соответственно основы математической логики, теории дискретных функций и теории алгоритмов.

Предназначено для студентов вузов, обучающихся по специальностям в области информационной безопасности, а также для аспирантов и студентов вузов других технических специальностей, изучающих дискретную математику.

Рецензенты:

В. Б. Алексеев — доктор физико-математических наук, профессор, зав. кафедрой математической кибернетики факультета ВМК Московского государственного университета им. М. И. Ломоносова; *В. П. Язын* — кандидат физико-математических наук, профессор кафедры информационной безопасности Московского государственного технического университета радиотехники, электроники и автоматики.

Предисловие

Данное учебное пособие состоит из трех взаимосвязанных частей, составляющих соответственно основы математической логики, дискретных функций и теории алгоритмов. Пособие содержит систематическое изложение учебного материала по математической логике, теории алгоритмов и дискретным функциям, изучаемого в цикле математических дисциплин по различным специальностям в области информационной безопасности.

Первая часть пособия содержит строгое изложение классического материала по алгебре логики, логике предикатов, исчислениям высказываний и предикатов 1-го порядка (называемого также узким исчислением предикатов) включая доказательства их непротиворечивости и полноты. Изложен также метод резолюций для распознавания истинности некоторых формул узкого исчисления предикатов. Вторая часть посвящена способам задания и изучению свойств булевых функций и функций k -значной логики при $k > 2$. Особое внимание уделяется свойствам функций, играющим важную роль в криптографии, в частности групповой классификации функций, вопросам сравнения произвольных функций с линейными и аффинными функциями, декомпозиции функций. В третьей части излагаются три основных подхода к определению понятия алгоритма, обсуждается связь между ними. Вводятся необходимые понятия о сложности алгоритмов и приводятся примеры нахождения нижних оценок сложности. Особое внимание уделяется вопросам сложности переборных задач. В частности, доказывается известная теорема Кука об NP-полноте проблемы выполнимости булевых функций. Рассматривается также вопрос о сложностной классификации систем булевых уравнений, приводится доказательство результата Шефера о полиномиальности проблемы распознавания совместности систем булевых уравнений, составленных из функций любого одного класса Шефера.

Содержание пособия основано на реализации компетентностного подхода, положенного в основу федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) третьего поколения в области информационной безопасности.

Пособие предназначено для преподавания дисциплины «Математическая логика и теория алгоритмов» для специальностей: 090301 «Компьютерная безопасность»; 090303 «Информационная безопасность автоматизированных систем»; 090305 «Информационно-аналитические системы безопасности».

Материал пособия (в части, касающейся теории дискретных функций) может быть использован в процессе преподавания дисциплины «Дискретная математика» для тех же специальностей.

Несмотря на явную направленность пособия на подготовку специалистов по защите информации, оно может быть использовано также студентами других специальностей при изучении математической логики, теории алгоритмов и дискретной математики. В ходе изложения материала пособия некоторые сравнительно несложные фрагменты доказательств предлагаются в качестве упражнений для самостоятельной работы. Отдельно системы задач и упражнений в пособии не приводятся в связи с тем, что в 2008 г. был издан сборник [75], содержащий задачи и упражнения по всем разделам данного пособия. Кроме того, много задач и упражнений приводится в известных сборниках задач [73, 76]. Материал пособия опробован авторами в ходе преподавания соответствующих учебных дисциплин в Институте криптографии, связи и информатики и отражен во внутривузовских учебных пособиях [12, 13]. В пособии нумерация определений, теорем, утверждений и формул производится в каждой части по главам с указанием номера соответствующей главы.

Глухов М. М., Шишков А. Б.

Математическая логика. Дискретные функции. Теория алгоритмов. Теория информации: Учебное пособие. 1-е изд.

Содержание

[Предисловие 3](#)

[Глава 1. Математическая логика 5](#)

- 1.1. Множества с отношениями и операциями 18
 - Множества и операции над ними 18
 - Отображения множеств 23
 - Отношения на множестве. Отношения эквивалентности и порядка 30
 - Множества с операциями 36
 - Аксиоматическое построение системы натуральных чисел 44
 - Мощность множества. Конечные и бесконечные множества 51
- 1.2. Алгебра высказываний 57
 - Основные логические операции и их свойства 57
 - Формулы алгебры высказываний 61
 - Эквивалентные формулы 65
 - Приведенные формулы и нормальные формы 70
 - Выполнимые и тождественно истинные формулы 74
 - Сокращенные, тупиковые и минимальные ДНФ 76
 - Алгоритм нахождения тупиковых ДНФ по сокращенной ДНФ 82
- 1.3. Исчисление высказываний 86
 - Общее понятие о логическом исчислении 86
 - Язык, аксиомы и правила вывода исчисления высказываний 88
 - Доказуемые формулы исчисления высказываний 89
 - Вспомогательные правила вывода 90
 - Полнота и непротиворечивость исчисления высказываний 95
- 1.4. Алгебра предикатов 102
 - Предикаты и операции над ними 102
 - Формулы алгебры предикатов 107
 - Эквивалентность формул. Основные соотношения эквивалентности 113
 - Приведенные и предваренные формулы 116
- 1.5. Исчисление предикатов 118
 - Язык, аксиомы и правила вывода исчисления предикатов 118
 - Выводимость и доказуемость формул 121
 - Семантика исчисления предикатов 124
 - Понятие о теории моделей 135
 - Проблема разрешимости в логике предикатов 141

[Глава 2. Дискретные функции. 151](#)

- 2.1. Дискретные функции и способы их задания 152
 - Способы задания булевых функций 152
 - Полные системы и замкнутые классы булевых функций 166
 - Функции k -значной логики и способы их задания. Полные системы 173
 - Критерии полноты систем функций k -значной логики 177
 - Полиномиальное представление функций k -значной логики 181
- 2.2. Представление дискретных функций в базисах функциональных пространств 189
 - Базисы линейных функциональных пространств. Базис характеров 190
 - Преобразование Фурье. Коэффициенты Фурье и Уолша–Адамара 193
 - Матричный подход к представлению булевых функций 197
- 2.3. Классификация дискретных функций с помощью групп преобразований 206

Эквивалентность функций. Группы инерции	207
Функции, инвариантные относительно группы	208
Функции с тривиальной группой инерции в аффинной группе	212
Перечисление G-типов. Лемма Бернсайда	213
Инварианты. Нахождение групп инерции и проверка эквивалентности	217
2.4. Вероятностные и комбинаторные свойства и параметры дискретных функций	223
Вероятностная функция булевой функции	224
Линейные приближения (аппроксимации) булевых функций	229
Коэффициент аддитивности дискретных функций	236
2.5. Некоторые специальные классы дискретных функций	243
Корреляционно-иммунные функции	243
k-устойчивые функции	246
Бент-функции	248
Бент-отображения	257
2.6. Декомпозиция булевых функций	264
Простая декомпозиция	266
Разложимые функции	268
Сложные декомпозиции	270
Группы инерции суперпозиции булевых функций в группах Σ_n , S_n , Q_n	279
Глава 3. Теория алгоритмов	283
3.1. Элементы теории алгоритмов	283
Нормальные алгоритмы	286
Принцип нормализации алгоритмов	291
Машины Тьюринга	294
Нумерация слов и арифметизация алгоритмов	299
Рекурсивные функции	305
Примеры алгоритмически неразрешимых проблем	310
3.2. Сложность алгоритмов и вычислений	323
Сложность нормальных алгоритмов, вычисляющих булевы функции	325
Сложности вычислений на машинах Тьюринга	328
Классификации задач по сложности их решения на машинах Тьюринга	334
О сложности классификации систем булевых уравнений	342
Асимптотические оценки сложности алгоритмов	357
Дискретные преобразования Фурье	364
Понятие о вероятностных алгоритмах	368
Приложение Методические рекомендации по организации изучения математической логики, теории алгоритмов, теории дискретных функций	372
Литература	380
