

ПРОГРАММА

курса «Дискретная математика»

механико-математический факультет МГУ, 4-й курс, 7-й семестр, 1-й поток,
2013/2014 уч. год (лектор — проф. В. В. Кочергин)

Функции алгебры логики

1. Функции алгебры логики. Равенство функций. Задание функций таблицами. Существенные и несущественные переменные. Формулы. Представление функций формулами. Операция суперпозиции. Замкнутые классы относительно операции суперпозиции (классы Поста). Операция введения несущественной переменной. Замкнутые классы относительно операций суперпозиции и введения несущественной переменной (замкнутые классы). Свойства замкнутых классов. Примеры классов Поста, не являющихся замкнутыми.
2. Полные системы функций. Примеры полных систем. Полиномы Жегалкина. Представление булевых функций полиномами. Линейные функции. Лемма о нелинейной функции. Классы конъюнкций и дизъюнкций. Монотонные функции. Свойства монотонных функций. Лемма о немонотонной функции. Лемма о порождении функций $x \vee y$ и xy . Теорема о конечной порожденности замкнутых классов, содержащих константы 0 и 1. Замкнутые классы, содержащие константы 0 и 1.
3. Лемма "со звездочкой". Функции, удовлетворяющие условию $\langle 0^\infty \rangle$. Свойства функций $x \vee yz$ и $d_p(x_1, \dots, x_p)$, $p \geq 2$. Основная лемма о порождении монотонных функций. Лемма о порождении монотонной функции f системой функций $\{x \vee yz, d_{p(f)}\}$. Теорема о конечной порожденности замкнутых классов монотонных функций, содержащих константу 1. Замкнутые классы монотонных функций, содержащих константу 1. Принцип двойственности. Лемма о порождении импликации. Лемма о монотонной функции. Теорема о конечной порожденности замкнутых классов, содержащих константу 1. Замкнутые классы, содержащие константу 1.
4. Самодвойственные функции. Лемма о несамодвойственной функции. Функции, сохраняющие константы. Теорема о конечной порожденности замкнутых классов, не содержащих констант 0 и 1. Теорема Поста о конечной порожденности всех замкнутых классов булевых функций. Необходимые и достаточные условия порождения констант системами булевых функций.
5. Особенности k -значных логик ($k \geq 3$). Пример Мучника замкнутого класса со счетным базисом. Построение континуального семейства замкнутых классов функций k -значной логики ($k \geq 3$).
6. Алгебраическое определение оператора замыкания. Инвариантные классы Яблонского. Характеристика инвариантного класса. Deskриптивные и метрические свойства инвариантных классов. Континуальность числа инвариантных классов. Пример инвариантного класса с характеристикой $1/2$.

Комбинаторика

7. Выборки. Размещения, сочетания, размещения с повторениями, сочетания с повторениями. Биномиальные коэффициенты. Свойства биномиальных коэффициентов, биномиальная теорема. Число монотонных отображений. Формула включения-исключения, ее варианты и примеры применения. Формула для функции Эйлера. Неравенства Бонфферони.
8. Числа Стирлинга 1-го и 2-го рода. Свойства чисел Стирлинга. Рекуррентные формулы для чисел Стирлинга. Комбинаторная интерпретация чисел Стирлинга. Явная формула для чисел Стирлинга 2-го рода. Числа Белла.
9. Формальные степенные ряды, операции над рядами. Кольцо $K[[x]]$ формальных степенных рядов и его свойства; необходимые и достаточные условия существования обратных элементов. Формальная производная, свойства формальной производной.
10. Производящие функции. Примеры применения метода производящих функций для решения комбинаторных задач. Линейные рекуррентные соотношения с постоянными коэффициентами. Теорема о решении линейных рекуррентных соотношений. Числа Фибоначчи.

11. Задача о расстановке скобок. Числа Каталана. Метод траекторий. Арифметическая функция Мёбиуса. Формула обращения Мёбиуса. Перечисление циклических последовательностей. Симметрические функции, элементарные симметрические функции, степенные суммы. Тождества Ньютона (связывающие элементарные симметрические функции и степенные суммы).
12. Конечные поля. Порядок и характеристика поля; свойства конечных полей. Существование примитивного элемента. Поле $GF(p)$. Неприводимые многочлены. Нумератор множества всех нормированных многочленов с коэффициентами из $GF(p)$. Формула для числа I_k^p неприводимых нормированных многочленов степени k с коэффициентами из $GF(p)$. Существование неприводимых многочленов заданной степени, асимптотически точная формула для I_k^p . Построение поля $GF(p^m)$.
13. Эйлеровы циклы в ориентированном графе. Граф де Брейна. Последовательность де Брейна.

Кодирование

14. Побуквенное (алфавитное) кодирование. Разделимые коды. Префиксные коды. Кодовые деревья. Теорема Маркова о проверке взаимной однозначности алфавитного кодирования. Неравенство Крафта — Макмиллана. Полные коды. Критерий полноты для разделимого кода. Критерий полноты для произвольного алфавитного кода. Построение полного (двоичного) кода по заданному префиксному коду.
15. Оптимальные коды (коды с минимальной избыточностью). Свойства оптимальных r -ичных кодов. Верхняя и нижняя оценки стоимости оптимального кода. Метод Шеннона построения кода, близкого к оптимальному. Достаточное условие оптимальности кодов, построенных методом Шеннона. Оптимальность заданного полного префиксного кода для некоторого распределения P . Свойства кодовых деревьев оптимальных префиксных кодов. Теорема о редукции. Алгоритм Хаффмана построения оптимального r -ичного кода.
16. Коды, исправляющие ошибки над полем $GF(p)$. Расстояние Хэмминга. Граница сферической упаковки (граница Хэмминга). Мощностной метод построения кода, исправляющего t ошибок. Верхняя и нижняя оценки мощности максимального кода. Совершенные коды. Примеры совершенных кодов.
17. Линейные коды над $GF(p)$. Порождающие и проверочные матрицы линейных кодов. Двойственные коды. Параметры линейных кодов. Необходимые и достаточные условия существования линейных кодов с заданным минимальным расстоянием. Граница Синглтона. Граница Варшавова — Гилберта. Код Хэмминга и его свойства. Алгоритм декодирования кода Хэмминга. Расширенный код Хэмминга и его свойства. Обобщенный код Хэмминга и его свойства. Алгоритм декодирования обобщенного кода Хэмминга.
18. Двоичные коды БЧХ (коды Боуза — Чоудхури — Хоквингема). Построение кодов БЧХ, исправляющих t ошибок. Параметры кодов БЧХ. Алгоритм декодирования для кодов БЧХ, исправляющих две ошибки. Леммы о значении определителя матрицы M_t (о решении системы уравнений, связывающих степенные суммы и элементарные симметрические функции). Теорема Питерсона. Алгоритм Питерсона декодирования двоичных кодов БЧХ, исправляющих t ошибок.

Схемы из функциональных элементов

19. Схемы из функциональных элементов (СФЭ). Схемы вычислений. Схемная сложность вычислений. Функция Шеннона. Асимптотика роста сложности для задачи возведения в степень. Асимптотика роста сложности для задачи сборки двоичных слов схемами конкатенации.
20. СФЭ в базисе $\{x \vee y, x \& y, \bar{x}\}$. Реализация системы всех конъюнкций длины n и системы всех функций от n переменных. Асимптотически наилучший метод Лупанова синтеза СФЭ. Мощностной метод доказательства нижних оценок. Асимптотика функции Шеннона.
21. Принцип локального кодирования. Реализация симметрических функций. Реализация самодвойственных функций. Вычисление булевой функции на r последовательных наборах. Реализация функций из инвариантных классов Яблонского.
22. Реализация систем из n линейных однородных булевых функций от n переменных в базисе $\{x \oplus y\}$.