ПРОГРАММА

курса **«Дискретная математика»**

механико-математический факультет МГУ, 4-й курс, 7-й семестр, 1-й поток,
2021/2022 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 Z. Функции, удовлетворяющие условию $\langle 0^\infty \rangle$. Свойства функций $x \vee yz$ и $d_p(x_1, \ldots, x_p)$, $p \geq 2$. 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. Дескриптивные 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 включений-исключений, ее варианты и примеры применения. Формула для функции Эйлера. Неравенства Бонферрони.

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. 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. 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 Брёйна. Последовательность де Брёйна.

Кодирование

14. Побуквенное (алфавитное) кодирование. Разделимые коды. Префиксные коды. Кодовые деревья. Теорема Маркова о проверке взаимной однозначности алфавитного кодирования (графовый алгоритм). 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 p-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 p-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 Варшамова — Гилберта. Код Хэмминга и его свойства. Алгоритм декодирования кода Хэмминга. Расширенный код Хемминга и его свойства. Обобщенный код Хэмминга и его свойства Алгоритм декодирования обобщенного кода Хэмминга.

18. Коды Рида — Маллера и их свойства. Мажоритарный алгоритм декодирования.

19. Двоичные коды БЧХ (коды Боуза — Чоудхури — Хоквингема). Построение кодов БЧХ, исправляющих t ошибок. Параметры кодов БЧХ. Алгоритм декодирования для кодов БЧХ, исправляющих две ошибки. Общая схема декодирования кода БЧХ. Алгоритм Питерсона — Горенстейна — Цирлера.

Сложность схемных вычислений

20. Схемы вычислений. Схемы из функциональных элементов. Сложность схемных вычислений. Функция Шеннона. Асимптотика роста сложности для задачи возведения в степень. Асимптотика роста сложности для задачи сборки двоичных слов схемами конкатенации.

21. Мощностной метод доказательства нижних оценок в произвольном конечном полном базисе. Метод Шеннона. Порядок роста функции Шеннона в произвольном конечном полном базисе.

22. Асимптотически наилучший метод Лупанова синтеза схем в базисе $\{x \vee y, x\&y, \overline{x}\}$. Асимптотика функции Шеннона в этом базисе.

23. Принцип локального кодирования. Реализация симметрических функций. Реализация самодвойственных функций. Вычисление булевой функции на r последовательных наборах.

24. Реализация функций из инвариантных классов Яблонского. Теорема Яблонского о невозможности элиминации перебора при построении последовательности самых сложных функций.

Дополнительная к лекциям литература

1. Дискретная математика и математические вопросы кибернетики. Том I. / Под общ. ред. С. В. Яблонского и О. Б. Лупанова. — М.: Наука, 1974. — 312 с.
2. *Яблонский С. В.* Введение в дискретную математику. — М.: Наука, 1986. — 384 с.
3. *Гаврилов Г. П., Сапоженко А. А.* Задачи и упражнения по дискретной математике. — М.: Физматлит, 2004. — 424 с.
4. *Яблонский С. В.* Элементы математической кибернетики. — М.: Высшая школа, 2007. — 188 с.
5. Конспект лекций О. Б. Лупанова по курсу «Введение в математическую логику» / Отв. ред. А. Б. Угольников. — М.: Изд-во ЦПИ при мех.-матем. ф-те МГУ им. М. В. Ломоносова, 2007. — 192 с.
6. *Чашкин А. В.* Дискретная математика. — М.: Изд. дом «Академия», 2012. —352 с.
7. *Угольников А. Б.* Классы Поста. — М.: Изд.-во ЦПИ при механико-математическом факультете МГУ им. М. В. Ломоносова, 2008. — 64 с.
8. *Холл М.* Комбинаторика. — М.: Мир, 1970. — 424 с.
9. *Кнут Д., Грехем Р., Паташник О.* Конкретная математика. Основание информатики. — М.: Мир, 1998. — 703 с.
10. *МакВильмс Ф. Дж., Слоэн Н. Дж.* Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.
11. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. — М.: Мир, 1976. — 596 с.
12. *Сидельников В. М.* Теория кодирования. — М.: Физматлит, 2008. — 324 с.
13. *Лупанов О. Б.* Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ им. М. В. Ломоносова, 1984. — 138 с.