

Механико-математический факультет МГУ

Программа курса «Дискретная математика», 4 курс, 1 поток,
лектор — профессор Ю. В. Таранников, 2025/2026 уч. год, осенний семестр

1. Комбинаторные схемы размещения. Двоичная энтропия. Выражение биномиальных коэффициентов через энтропию. Энтропийное неравенство. Неравенство Чернова.
2. Производящие функции. Производящие функции множеств. Линейные рекуррентные последовательности. Перечисление правильных скобочных структур. Числа Каталана.
3. Функция Мебиуса. Формула обращения Мебиуса. Перечисление циклических последовательностей. Число неприводимых многочленов над полем \mathbf{F}_q .
4. Групповая эквивалентность на множестве. Орбиты, эквивалентные элементы, группы инерции, их свойства. Лемма Бернсайда. Цикловой индекс группы. Теорема Пойа.
5. Предшествование наборов. Частично упорядоченное множество (ЧУМ). Проверка свойств ЧУМ для \mathbf{F}_2^n . Эквивалентность системе подмножеств. Пример полного порядка. Пример ЧУМ: делимость на натуральных числах. Локально конечные частично упорядоченные множества, формула обращения Мебиуса для них. Функция Мебиуса для частичного порядка на двоичных наборах. Булевы функции и их полиномы. Связь числовой нормальной формы с полиномом Жегалкина. Теорема Мак-Элиса. Зависимость веса от алгебраической степени.
6. Чувствительность булевой функции. Теорема Симона–Вегенера. Блочная чувствительность. Сертификационная сложность.
7. CREW PRAM. Теорема Кука–Дворк–Рейщука о нижней оценке времени вычисления булевой функции в модели CREW PRAM в зависимости от чувствительности функции.
8. Булевы деревья решений. Детерминированная модель. Связь сертифицированной сложности и глубины дерева решений. Сложность CREW PRAM. Метод «удвоения указателя». CROW PRAM. Связь глубины дерева решений булевой функции и ее действительной степени.
9. Симметризация многочленов. Неравенство братьев Марковых (без доказательства). Следствия из неравенства братьев Марковых для $k = 1$. Соотношение между блочной чувствительностью и действительной степенью. Теорема Коши о чередовании корней (без доказательства). Эрмитовы матрицы. Теорема Коши о чередовании собственных значений.
10. Коэффициенты Уолша булевых функций. Доказательство гипотезы чувствительности. Сведение Гоцмана и Линиала.
11. Алфавитное кодирование. Коды с однозначным декодированием. Префиксные, суффиксные коды. Неравенство Макмиллана. Существование префиксного кода с параметрами, удовлетворяющими неравенству Макмиллана. Явное задание префиксного кода с параметрами, удовлетворяющими неравенству Макмиллана.
12. Оптимальные коды. Существование оптимальных префиксных кодов. Оценки стоимости оп-

тимального кода через энтропию. Свойства оптимальных префиксных кодов. Лемма о редукции. Алгоритм Хаффмана построения q -ичного оптимального кода.

13. Передача информации по каналу связи. Помехи, ошибки. Расстояние Хэмминга. Кодовое расстояние. Обнаружение и корректирование ошибок. Линейный код. Порождающая матрица. Кодирование и декодирование с помощью порождающей матрицы. Двойственный код. Проверочная матрица. Синдром. Кодовое расстояние линейного кода. Связь кодового расстояния со свойствами столбцов проверочной матрицы. Вектор ошибок. Исправление небольшого числа ошибок. Линейные коды с кодовым расстоянием 1 и 2. Линейные коды с кодовым расстоянием 3. Двоичный код Хэмминга. Кодирование, исправление ошибок и декодирование с помощью двоичного кода Хэмминга. Проблема верхних оценок мощности кодов. Оценка Хэмминга (граница сферической упаковки). Достижимость оценки Хэмминга на коде Хэмминга. Совершенные коды. Оценка Синглтона.

14. Оценка Гильберта (сферическая нижняя оценка). Оценка Варшамова. Скорость кода. Асимптотические оценки скорости кода, их сравнение. Асимптотическая оценка Варшамова–Гильберта для скорости кода. Код Рида–Маллера, его кодовое расстояние. Дуальный код к коду Рида–Маллера. Мажоритарное декодирование кодов Рида–Маллера.

15. Матрица Вандермонда, ее невырожденность. Коды Рида–Соломона трех типов, их параметры. Достижимость оценки Синглтона на кодах Рида–Соломона. Подполе и расширение поля. Коды Боуза–Чоудхури–Хоквингема (БЧХ), их проверочная матрица, оценки кодового расстояния и размерности. Коды Хэмминга и Рида–Соломона первого типа как частные случаи кода БЧХ. Алгоритм декодирования Питерсона–Горенштейна–Цирлера для кодов БЧХ.