Механико-математический факультет МГУ

Программа курса естественно-научного содержания
«Теория кодирования и ее применения в криптографии»,
лектор — доцент Ю. В. Таранников, 2018/2019 уч. год.

1. 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.
2. 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 кодовыми расстояниями 1 и 2.
3. Линейные коды с кодовым расстоянием 3. Двоичный код Хэмминга. Кодирование, исправление ошибок и декодирование с помощью двоичного кода Хэмминга.
4. Проблема верхних оценок мощности кодов.
5. Оценка Хэмминга (граница сферической упаковки). Достижимость оценки Хэмминга на коде Хэмминга. Совершенные коды.
6. Оценка Синглтона для линейных и нелинейных кодов.
7. Оценки Гильберта и Варшамова.
8. Распределение весов кода. Тождества Мак-Вильямс.
9. Матрица Вандермонда, ее невырожденность. Коды Рида–Соломона трех типов, их параметры. Достижимость оценки Синглтона на кодах Рида–Соломона. Коды, двойственные к кодам Рида–Соломона второго и третьего типа.
10. Циклические коды. Представление наборов линейных циклических кодов в виде многочленов. Линейный циклический код как идеал в кольце классов вычетов многочленов. Порождающий многочлен. Проверочный многочлен.
11. Многочлен ошибок. Синдромный многочлен. Кодирование, исправление ошибок и декодирование линейных циклических кодов на языке многочленов.
12. Код Рида–Соломона первого типа как циклический код. Порождающий многочлен кода Рида–Соломона первого типа.
13. 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.
14. Взаимосвязь множества наборов кода БЧХ над $\mathbf{F}_q$ с множеством наборов соответствующего кода Рида–Соломона над $\mathbf{F}_{q^m}$. Код БЧХ как циклический код. Примеры кодов БЧХ. Минимальные многочлены и сопряженные корни. Порождающий многочлен кода БЧХ.
15. Алгоритм декодирования Питерсона–Горенстейна–Цирлера для кодов БЧХ, его трудоемкость.
16. Проблема быстрого решения системы линейных уравнений специального вида при исправлении ошибок в коде БЧХ. Сведение к задаче нахождения регистра сдвига с линейной обратной связью минимальной длины, генерирующего данную последовательность.
17. Леммы о длине минимального регистра сдвига.
18. Алгоритм Берлекэмпа–Месси, его трудоемкость.
19. Синдромный многочлен и многочлен значений ошибок для кода БЧХ. Алгоритм Форни нахождения значений ошибок.
20. Открытые системы шифрования на основе кодов, корректирующих ошибки. Системы открытого шифрования Мак-Элиса и Нидеррайтера. Сравнение систем открытого шифрования Мак-Элиса и Нидеррайтера.
21. Ортогональные массивы. Их параметры. Корреляционно-иммунные функции. Связь силы ортогонального массива, построенного по линейному коду, с кодовым расстоянием дуального кода. Существование ортогональных массивов из выполнения условия границы Варшамова–Гильберта.
22. Ортогональный массив, построенный с помощью кода Рида–Соломона. Конструкция Буша.
23. Неравенство Рао.
24. Коды аутентификации. Их построение с помощью ортогональных массивов.
25. Дизъюнктные коды. Построение системы разделения ключей с помощью дизъюнктных кодов.
26. Разделяющие коды. Каскадная конструкция дизъюнктных кодов.