Механико-математический факультет МГУ

Программа курса естественно-научного содержания
«Теория кодирования и ее применения в криптографии»,
обязательного для студентов 4 курса направления
«Математические методы защиты информации»,
лектор — доцент Ю. В. Таранников, 2016/2017 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. Вектор ошибок. Исправление небольшого числа ошибок. Кодовое расстояние линейного кода. Связь кодового расстояния со свойствами столбцов проверочной матрицы. 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. Рекуррентные оценки.
5. Оценка Хэмминга (граница сферической упаковки). Достижимость оценки Хэмминга на коде Хэмминга. Совершенные коды.
6. Оценка Синглтона для линейных и нелинейных кодов.
7. Оценка Джонсона. Следствие из нее. Связь между максимальными мощностями кода на всем множестве наборов и на его подмножестве. Оценка Элайеса–Бассалыго.
8. Оценка Плоткина и следствие из нее. Достижимость оценки Плоткина на коде, двойственном к коду Хэмминга.
9. Матрицы Адамара. Делимость порядка матрицы Адамара на 4. Связь матриц Адамара и кодов с большими кодовыми расстояниями. Достижимость оценки Плоткина на кодах, построенных с помощью матрицы Адамара. Эквивалентность матриц Адамара и кодов, на которых достигается равенство в следствии из оценки Плоткина.
10. Кронекерово произведение матриц. Кронекерово произведение матриц Адамара есть матрица Адамара. Матрица Адамара–Сильвестра. Квадратичные вычеты. Символы Лежандра. Построение матриц Адамара с помощью символов Лежандра. Построение матриц Адамара всех порядков до 100, делящихся на 4, кроме 92.
11. Оценка Грайсмера, ее достижимость на коде, двойственном к двоичному коду Хэмминга.
12. Оценка Варшамова–Гильберта.
13. Двоичная энтропия. Выражение биномиальных коэффициентов через энтропию. Скорость кода. Асимптотические оценки скорости кода, получаемые через оценки Хэмминга, Элайеса–Бассалыго и Варшамова–Гильберта, их сравнение между собой.
14. Несуществование совершенных кодов с параметрами $d = 7$, $n > 7$, $n \neq 23$. Расширенный двоичный код Голея, его кодовое расстояние. Двоичный код Голея как совершенный код.
15. Число наборов веса 7 и 8 в двоичном коде Голея. Распределение весов кода. Теорема Шапиро–Злотника.
16. Тождества Мак-Вильямс.
17. Булевы функции. Полином Жегалкина. Код Рида–Маллера, его кодовое расстояние. Дуальный код к коду Рида–Маллера. Связь кода Рида–Маллера первого порядка с матрицей Адамара–Сильвестра.
18. Мажоритарное декодирование кодов Рида–Маллера.
19. Радиус покрытия кода. Радиус покрытия кода Рида–Маллера первого порядка. Его значение для криптографии.

20. Быстрое умножение матрицы Адамара–Сильвестра на столбец.
21. 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.
22. Циклические коды. Представление наборов линейных циклических кодов в виде многочленов. Линейный циклический код как идеал в кольце классов вычетов многочленов. Порождающий многочлен. Проверочный многочлен.
23. Многочлен ошибок. Синдромный многочлен. Кодирование, исправление ошибок и декодирование линейных циклических кодов на языке многочленов.
24. Код Рида–Соломона первого типа как циклический код. Порождающий многочлен кода Рида–Соломона первого типа.
25. 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.
26. 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.
27. Алгоритм декодирования Питерсона–Горенстейна–Цирлера для кодов БЧХ, его трудоемкость.
28. 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.
29. Леммы о длине минимального регистра сдвига.
30. Алгоритм Берлекэмпа–Месси, его трудоемкость.
31. Синдромный многочлен и многочлен значений ошибок для кода БЧХ. Алгоритм Форни нахождения значений ошибок.
32. Открытые системы шифрования на основе кодов, корректирующих ошибки. Системы открытого шифрования Мак-Элиса и Нидеррайтера. Сравнение систем открытого шифрования Мак-Элиса и Нидеррайтера.
33. 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.
34. Ортогональный массив, построенный с помощью кода Рида–Соломона. Конструкция Буша.
35. Рекуррентные соотношения для максимального числа столбцов в ортогональных массивах. Неравенства Буша.
36. Неравенство Рао.
37. Коды аутентификации. Их построение с помощью ортогональных массивов.
38. Дизъюнктные коды. Построение системы разделения ключей с помощью дизъюнктных кодов.
39. Разделяющие коды. Каскадная конструкция дизъюнктных кодов.