Механико-математический факультет МГУ

Программа курса естественно-научного содержания
"Теория кодирования и ее применения в криптографии",
обязательного для студентов 4 курса специализации "Защита информации",
7 семестр, лектор — доцент Ю. В. Таранников, 2013/2014 уч. год.

1. 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 пространстве 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 коде, построенном 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. Двоичный код Голея, его кодовое расстояние. Двоичный код Голея как совершенный код.
15. Число наборов веса 7 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. Определитель Вандермонда, его невырожденность. Коды Рида–Соломона трех типов, их параметры. Достижимость оценки Синглтона на кодах Рида–Соломона. Коды, двойственные к кодам Рида–Соломона второго и третьего типов.

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. 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. Код БЧХ как циклический код. Подполе и расширение поля. 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 шифрования МакЭлиса 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.

Литература.

1. В. М. Сидельников. Теория кодирования. М.: Физматлит, 2008.
2. В. И. Левенштейн. Элементы теории кодирования, в Дискретная математика и математическая кибернетика, т. 1, М.: Издательство "Наука", Главная редакция физико-математической литературы, 1974, с. 207–305.
3. Р. Блейхут. Теория и практика кодов, контролирущих ошибки. М.: Мир, 1986.
4. Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
5. Ю. В. Таранников. Комбинаторные свойства дискретных структур и приложения к криптологии. М.: МЦНМО, 2011.
6. А. В. Чашкин. Дискретная математика. М.: Изд. центр "Академия", 2012.
7. Ю. В. Таранников. Дискретная математика. Семинары, 2004.
8. A. S. Hedayat, N. J. A. Sloane, J. Stufken. Orthogonal arrays. Theory and applications. Springer–Verlag, 1999.
9. V. Pless. Introduction to the theory of error-correcting codes. John Wiley and sons, 1989.
10. D. R. Stinson. Cryptography. Theory and practice. CRC Press, 1995.