Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)»

Рабочая программа дисциплины (модуля)

по дисциплине: Алгебраические коды. Дополнительные главы
по направлению: Прикладные математика и физика
магистерская программа: Телекоммуникационные сети и системы
Физтех-школа радиотехники и компьютерных технологий
Кафедра проблем передачи информации и анализа данных
курс: 1
квалификация: Магистр

Семестры, формы промежуточной аттестации: 1 (Осенний) – Простой зачет
Семестры, формы промежуточной аттестации: 2 (Весенний) – Дифференцированный зачет

Программу составил: **В.Б. Афанасьев, кандидат технических наук, доцент**

Аннотация

В рамках курса студенты знакомятся с базовыми понятиями теории линейных кодов (основные понятия, кодирование и декодирование линейных кодов, границы кодирования, методы построения кодов), а также теории циклических кодов (кольцо многочленов над полем Галуа, определение циклического кода, необходимое и достаточное условие существования циклического кода с порождающим многочленом g(x), кодирование и декодирование циклических кодов, коды Хэмминга, коды Боуза-Чоудхури-Хоквингема (БЧХ-коды), коды Рида-Соломона). Эти классы кодов наиболее часто применяются на практике. Теория линейных кодов самым тесным образом связана с дискретным анализом, теорией групп, теорией Галуа, конечными геометриями, теорией графов, теорией блок-схем, криптографией.

Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 1 (Осенний)

1. Модели: источники, каналы, помехи и сигналы.

   Источники: независимые, с памятью, Марковские. Каналы: общее определение, симметричные, аддитивные, состояния канала с памятью. Помехи: аддитивные, независимые, с памятью. Сигналы: ортогональные и неортогональные.

2. Энтропия. Пропускная способность. Теорема кодирования.

   Определение энтропии, условная энтропия. Информация: собственная, условная, средняя. Пропускная способность канала (системы): общий случай – максимизация взаимной информации, симметричный случай. Теорема кодирования источника. Теорема кодирования канала.

3. Введение в теорию кодирования.

Двоичный симметричный и стирающий каналы. Кодовое расстояние. Исправление и обнаружение ошибок. Исправление стираний. Граница Гилберта (вывод для нелинейного кода). Метод исчерпания. Код Хэмминга. Декодирование и сложность вычислений при декодировании.

4. Теория сравнений. Функция Эйлера. Первообразные корни и индексы.

Определение. Свойства сравнений, полная и приведенная системы вычетов. Теоремы о свойствах систем вычетов. Функция Эйлера. Определение. Мультипликативность и вычисление функции Эйлера. Теоремы Эйлера и Ферма. Первообразные корни и индексы. Показатель, которому принадлежит число по некоторому модулю. Связь сравнимости чисел со сравнимостью их показателей. Показатели чисел по модулю *m*, как делители функции Эйлера. Первообразные корни. Модули, по которым существуют первообразные корни. Число первообразных корней. Индексы. Аналогия между индексами и логарифмами. Основные теоремы об индексах.

5. Группа. Подгруппа. Кольца и поля.

Группа. Определение группы. Единичный и обратный элементы. Порядок группы, порядок элемента группы. Показатель группы. Циклическая группа и порядки ее элементов. Примеры групп. Когда приведенная система вычетов является циклической группой.
Подгруппа. Примеры подгрупп. Смежные классы. Разложение группы по подгруппе. Фактор-группа. Теорема Лагранжа. Нормальные делители. Изоморфизм и гомоморфизм групп.
Кольца и поля. Определение кольца. Делители нуля. Область целостности. Определение поля, характеристика поля. Подполе. Примеры колец и полей. Идеал. Примеры идеалов. Идеалы поля.

6. Поля Галуа. Теоремы о полях Галуа.

Поля Галуа. Определение поля и построение поля по модулю неприводимого многочлена. Расширение поля, степень расширения. Мультипликативная группа поля. Элементы поля, как корни многочлена $X^{q^m} - X$. Теоремы Эйлера и Ферма. Теорема Вильсона. Цикличность мультипликативной группы поля. Аддитивная группа поля. Поле как векторное пространство. Базис поля. Теоремы о полях Галуа. Минимальный многочлен; неприводимость, делимость на минимальный многочлен. Существование минимального многочлена для произвольного элемента поля. Делимость многочлена $X^{q^m} - X$ на неприводимый многочлен над $GF(q)$. Делимость многочлена $X^{q^m} - X$ на многочлен $X^{q^n} - X$. Элементы β и β^q как корни одного и того же многочлена. Сопряженные элементы поля Галуа. Циклотомические классы. Подполе поля $GF(q^m)$. Степени неприводимых делителей многочлена $X^{q^m} - X$. Порядок корней неприводимого многочлена и порядок неприводимого многочлена. Примитивный многочлен. Изоморфизм полей. Автоморфизмы поля Галуа. Группа автоморфизмов (группа Галуа) поля Галуа. Порядок группы Галуа. Связь между подгруппами группы автоморфизмов с подполями поля Галуа.

7. Линейные коды. Операции над кодами.

Определение линейного кода как подпространства. Ортогональные подпространства. Мини-

мальное расстояние и минимальный вес кода. Порождающая и проверочная матрицы кода, их приведённо-ступенчатые формы и связь между ними. Информационные и проверочные символы кода. Связь проверочной матрицы линейного кода с минимальным расстоянием *d*. Удлинение, укорочение линейного кода. Выкалывание. Расширение линейного кода. Пополнение и выбрасывание.

8. Границы параметров кодов. Спектр весов кода.

Границы параметров кодов. Граница Варшамова-Гилберта (вывод для линейных кодов). Границы Синглтона, Хэмминга, Плоткина и Элайса. Другие границы. Оценка сумм биномиальных коэффициентов, асимптотическая форма границ.

9. Кодирование и декодирование линейного кода. Вероятность ошибки декодера.

Кодирование и декодирование линейного кода. Информационный вектор и его умножение на порождающую матрицу. Синдром. Синдромы и смежные классы в разложении пространства по кодовому подпространству. Стандартное расположение, лидеры смежных классов. Совершенные коды.

10. Коды Хэмминга и двойственные им. Коды на матрицах Адамара.

Коды Хэмминга и двойственные кодам Хэмминга. Кодовое расстояние. Коды, построенные на основе матриц Адамара. Мощность и корректирующая способность. Построение матриц Адамара. Матрицы Адамара и граница Плоткина.

11. Коды с мажоритарным декодированием.

Мажоритарное декодирование. Разделенные проверки. Реализация кодового расстояния.

12. Коды Рида-Маллера.

Порождающая матрица. Порядок кода Рида-Маллера. Кодовое расстояние. Кодирование и декодирование. Сложность декодирования.

Семестр: 2 (Весенний)

13. Циклические коды. Коды Боуза-Чоудхури-Хоквингема (коды БЧХ).

Циклические коды. Кольцо $F[x]/(x^n-1)$ многочленов по модулю многочлена x^n-1. Циклическое подпространство, циклический код, как идеал. Порождающий многочлен. Проверочный многочлен. Порождающая и проверочная матрицы циклического кода, их приведённо-ступенчатые формы и связь между ними. Кодирование циклического кода. Задание циклического кода корнями его порождающего многочлена. Длина и число проверочных символов циклического кода.
Коды Боуза-Чоудхури-Хоквингема (коды БЧХ). Определение кода БЧХ. Длина кода. Гарантированное и истинное кодовое расстояние кода БЧХ. Число информационных символов кода БЧХ. Двоичные коды БЧХ. Декодирование двоичного кода БЧХ, исправляющего две ошибки. Общий случай декодирования двоичного кода. Многочлен локаторов ошибок. Алгоритм декодирования Питерсона-Цирлера. Тождества Ньютона.

14. Коды Гоппы

Построение двоичных кодов Гоппы. Коды Гоппы как обобщение кодов БЧХ. Параметры кодов.

15. Коды с максимально достижимым кодовым расстоянием (МДР-коды) - – коды Рида-Соломона.

Информационные совокупности кода. Связь между информационными совокупностями кода и кодовым расстоянием МДР-кода. Дуальный код МДР-кода. Укорочение и выкалывание МДР-кода. Миноры порождающей матрицы. Коды Рида-Соломона. Удлинение кодов Рида-Соломона. Проверочные матрицы удлиненных кодов. Информационный многочлен и компоненты кодового вектора. Декодирование кодов Рида-Соломона. Исправление пачек ошибок.

16. Алгебраическое декодирование. Алгоритм Берлекэмпа-Мэсси. Исправление стираний и ошибок.

Синдром БЧХ кода в области Фурье. Вывод ключевого уравнения. Многочлен локаторов и значений ошибок. Корни и локаторы ошибок. Значения ошибок. Многочлен локаторов стираний и ошибок. Поиск корней многочленов над конечным полем.

17. Каскадные коды. Код произведение. Коды Форни и коды Юстессена.

Матричное представление кодовых слов. Кодирование строк и столбцов. Код произведение. Кодовое расстояние. Сочетания кодов над различными полями: внешние и внутренние коды. Параметры кодов.

18. Обобщенные каскадные коды Зяблова и Зиновьева.

Обобщенный линейный каскадный код (код Зяблова) как сумма кодов произведений. Системы внутренних вложенных кодов. Теорема о кодовом расстоянии. Нелинейные обобщенные каскадные коды Зиновьева. Границы для каскадных кодов.

19. Алгебраическое итеративное декодирование. Алгоритмы Чейза.

Итеративное декодирование линейных обобщенных каскадных кодов. Декодирование с оценкой надежности промежуточного решения.

20. Совместное декодирование циклических кодов в декодировании каскадных кодов.

Перемежение линейных кодов как частный случай кода произведения. Группирование ошибок. Покрывающий вектор ошибок. Построение объединенной системы линейных уравнений. Границы.

21. Методы быстрых вычислений в конечных полях.

Способы ускорения вычислений. Алгоритм Карацубы. Алгоритмы Тоома-Кука. Теоретико-числовые преобразования. Быстрое преобразование Фурье над конечным полем.

22. Быстрые алгоритмы вычислений для линейных кодов.

Быстрое кодирование циклических кодов и быстрое вычисление синдрома. Быстрое решение

ключевого уравнения и исправление ошибок. Асимптотика сложности декодирования.

23. Коды, сигналы и декодирование с мягким решением.

Способы отображения кодовых на последовательности сигналов. Демодуляция с мягким решением. Возможные методы алгебраического декодирования с мягким решением алгоритмы Судана и Кёттера.

Перечень рекомендуемой литературы

Основная литература
1. Сагалович Ю.Л. Введение в алгебраические коды. М.: ИППИ РАН, 2010. – 302 с.
2. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир. 1986. – 576 с.
3. Мак-Вильямс Ф.Дж., Слоэн Н.Дж. Теория кодов, исправляющих ошибки. М.: Связь. 1979. – 744 с.
4. Ван дер Варден Б.Л. Алгебра. М.: Наука. 1976. – 648 с.
5. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир. 1976. – 593 с.
6. Виноградов И.М. Основы теории чисел. М.: Наука, 1972. – 408 с.
7. Бухштаб А.А. Теория чисел. М.: Просвещение, 1966. – 385 с.