

# ПРОГРАММА КУРСА "ТЕОРИЯ КОДИРОВАНИЯ" ММФ НГУ (1 год магистратуры, 2 семестр)

к.ф.-м.н., профессор Ф. И. Соловьева

Передача информации, основная проблема теории информации. Методы кодирования и защиты информации. Блочное кодирование. Канал связи, типы каналов связи. Дискретные каналы без шума и с шумом.

1. Модель канала связи. Вероятность ошибки декодирования. Стандартное расположение, синдром, его свойства. Теорема Шеннона для двоичного симметричного канала связи (без доказательства).

2. Поля Галуа, их свойства. Теорема о ненулевых элементах поля Галуа.

3. Линейные коды. Кодирование и декодирование. Общие свойства линейных кодов. Теорема о связи проверочной и порождающей матриц. Теорема Глаголева.

4. Границы объема кода: граница Синглтона, граница Хэмминга, граница Варшавова-Гилберта, граница Плоткина. Коды Хэмминга над  $GF(q)$ , способы задания, кодирование, декодирование, единственность.

5. Методы построения новых кодов из заданных. Комбинирование кодов. Теорема Плоткина. Коды с малыми расстояниями (коды Хэммилляйна, использование метода включения и исключения).

6. Совершенные коды. Конструкция Васильева. Теорема о существовании совершенных кодов. Оценки числа совершенных кодов. Общие свойства совершенных кодов, теоремы Шапиро и Злотника.

7. Циклические коды. Кольцо многочленов над полем Галуа. Определение циклического кода. Порождающий многочлен циклического кода, его свойства, теорема о порождающем многочлене. Теорема о необходимом и достаточном условии существования циклического кода с заданным порождающим многочленом. Порождающая матрица циклического кода. Кодирование и декодирование циклических кодов. Проверочный многочлен. Теорема о проверочной матрице циклического кода. Минимальный многочлен, его свойства. Теорема о границе Боуза. Критерий принадлежности многочлена циклическому коду. Число циклических кодов длины  $n$  над полем Галуа  $GF(p^m)$ .

8. Коды Боуза-Чоудхури-Хоквингема (БЧХ-коды) над полем Галуа  $GF(p^m)$ . Кодирование, декодирование. Двоичные коды БЧХ. Циклическое представление кодов Хэмминга. Двоичные коды БЧХ с расстоянием 5. Коды Рида-Соломона.

9. Коды Рида-Маллера, кодирование, свойства.

10. Методы построения кодов (продолжение). Свитчинговые методы построения кодов (основная идея, коды с параметрами кодов Рида-Маллера, коды Моллера). Каскадные методы построения кодов (основная идея, коды Соловьевой, коды Фелпса, обобщенный каскадный метод Зиновьева).

## ЛИТЕРАТУРА

1. Мак-Вильямс Ф.Дж.А., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. - М.: Связь, 1979. - 744 с.
2. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ. - М.: Мир, 1976. - 594 с.
3. Берлекэмп Е. Р. Алгебраическая теория кодирования: Пер. с англ. - М.: Мир, 1971. - 477 с.
4. Блейхут Р. Теория и практика кодов, контролируемых ошибки: Пер. с англ. - М.: Мир, 1986. - 576 с.
5. Галлагер Р. Г. Теория информации и надежная связь: М.: Сов. радио, 1974.
6. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования: Пер. с япон. - М.: Мир, 1978. - 576 с.
7. Колесник В. Д., Полтырев Г. Ш. Курс теории информации. М.: Наука, 1982. 416 с.
8. Конвей Дж.Н., Слоэн Н.Дж.А. Упаковки шаров, решетки и группы: пер. с англ. - М.: Мир, 1990, - I, II т.
9. Шеннон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963.
10. Шоломов Л.А. Основы теории дискретных логических и вычислительных устройств, - М.: Наука, 1980. - 399 с.
11. Фано Р. М. Передача информации. Статистическая теория связи. М.: Мир, 1965.
12. Handbook on coding theory, Amsterdam: North-Holland, 1998.
13. Соловьева Ф.И., Введение в теорию кодирования, учебное пособие, изд-во НГУ, Новосибирск, 2006 г.
14. Solov'eva F.I., On perfect codes and related topics, Lecture Notes, Pohang University of Science and Technology (POSTECH), Korea, 2004, 80 pp.

---

Сайт "Теория кодирования в Новосибирском государственном университете" по адресу <http://www.codingtheory.gorodok.net>.

Профессор  
кафедры теоретической кибернетики  
ММФ НГУ

Ф.И. Соловьева

30.01.2008