

ПРОГРАММА ЭКЗАМЕНА
по спецкурсу "Циклические коды" (2006-2007 у.г.)

1. Оператор циклического сдвига. Две леммы о действии этого оператора. Циклические подпространства, пример построения циклического подпространства. Критерий цикличности подпространства. Первое определение циклического кода.
2. Идеалы в кольце многочленов одной переменной. Примеры. Теорема о том, что $F_q[x]$ является кольцом главных идеалов. Построение факторкольца кольца многочленов, выбор представителей факторклассов.
3. Кольцевой гомоморфизм, естественный гомоморфизм. Делимость идеалов. Теорема о связи между идеалами при естественном гомоморфизме. Лемма о связи между делителями многочлена $f(x)$ и идеалами, делящими $(f(x))$. Описание всех идеалов в факторкольцах. Примеры.
4. Представление факторкольца как векторного пространства. Преобразование Лорана. Оператор умножения на x , действующий в факторкольце, образ этого оператора после преобразования Лорана. Лемма о свойствах преобразования Лорана. Второе определение циклического кода. Способ вычисления количества циклических кодов фиксированной длины над заданным полем.
5. Порождающий и проверочный многочлены циклического кода. Теорема о порождающей матрице циклического кода. Теорема о проверочной матрице циклического кода.
6. Теорема о дуальном коде циклического кода. Возвратный многочлен, обратный код. Теорема об обратном коде. Соотношения между делителями и корнями многочлена и возвратного к нему.
7. Комбинаторная эквивалентность кодов. Лемма о комбинаторной эквивалентности двух кодов. Группа автоморфизмов кода, примеры. Лемма о группе автоморфизмов двоичных кодов. Теорема о связи групп автоморфизмов кода и дуального кода. Лемма о некоторых подгруппах группы автоморфизмов циклического кода.
8. Кодирование циклических кодов в векторной, полиномиальной и систематической формах. Синдромный многочлен. Теорема о синдромном многочлене. Максимальное количество синдромных многочленов МДР-кода. Простейший декодер циклического кода. Пример декодирования.
9. Теорема и декодер Меггитта. Пример. Декодер с выявлением ошибок. Пример.
10. Укороченные циклические коды. Пример укорочения кода Хэмминга. Кодирование укороченных кодов. Псевдоциклические коды. Две теоремы о совпадении классов укороченных циклических и псевдоциклических кодов. Декодирование укороченных циклических кодов.
11. Минимальный многочлен. Теорема о минимальном многочлене. Свойства минимального многочлена. Сопряженные элементы. Теорема о корнях минимального многочлена. Пример.
12. Нули и ненули циклического кода. Теорема о нулях кодовых слов. Третье определение циклического кода. Построение порождающего многочлена по нулям кода, определение длины циклического кода. Теорема о проверочной матрице циклического кода.

13. Циклические коды Хэмминга. Два типа обобщенных коды Хэмминга. Теорема о коде Хэмминга. Пример построения обобщенных кодов Хэмминга.
14. Граница БЧХ. Конструктивное расстояние циклического кода. Примеры вычисления конструктивного расстояния, (код Хэмминга, симплексный код). Обобщение границы БЧХ.
15. Коды БЧХ, их свойства. Примитивные коды БЧХ, коды БЧХ в узком смысле. Расстояние Боуза. Примеры. Верхняя оценка минимального расстояния кода БЧХ. Асимптотически хорошие семейства кодов.
16. Декодирование кодов БЧХ: синдромный многочлен, многочлен локаторов ошибок, лемма о матрице синдромов, определение количества произошедших в канале ошибок. Принципиальный алгоритм Питерсона-Горенштейна-Цирлера декодирования кодов БЧХ.
17. Классические коды Рида-Соломона. Теорема о параметрах КРС-кодов. Теорема о цикличности КРС-кодов. Алгоритм декодирования КРС-кодов (описание PGZ-алгоритма).
18. Коды Рида-Соломона типа 1, типа 2, типа 3. Лемма о параметрах РС-кодов. Теорема о цикличности РС-кодов типа 1. Вопросы цикличности РС-кодов типа 2, типа 3. Подгруппы автоморфизмов РС-кодов. Коды, дуальные к РС-кодам.
19. Декодирование РС-кодов методом Берлекэмпа-Велча. Теорема Берлекэмпа-Велча.
20. Понятие об алгоритме Берлекэмпа-Мессис: предназначение, идея, основные шаги.
21. Понятие о квадратично-вычетных кодах; конструкция, параметры, идемпотенты, декодирование.
22. Понятие о каскадных кодах и кодах Юстесена: конструкция, параметры.
23. Понятие о кодах Гоппы: конструкция, параметры.
24. Понятие о CRC-кодах: конструкция, параметры.