УТВЕРЖДАЮ:
Зав. кафедрой_____
ВМ и УМФ
Мартышко П.С.

ПРОГРАММА
экзамена по курсу
Дискретная математика
2008/2009 учебный год

4.2 Содержание разделов дисциплины

4.2.1 Основные понятия теории множеств. Отношения и операции.

Множество. Обозначения. Способы задания. Мощность. Подмножество и надмножество. Операции над множествами: объединение, пересечение, разность, дополнение. Декартово произведение.

Отношения (бинарные) между множествами, отображения, свойства. Отношения на множестве, свойства: рефлексивность, симметричность, транзитивность, дихотомия. Отношение эквивалентности. Отношение порядка. Диаграммы Хассе. Максимальный и минимальный элементы.

4.2.2 Комбинаторика

Перестановки и подстановки. Сочетания. Размещения. Формулы для подсчета. Применение для решения задач на конечные множества.

4.2.3 Элементы теории чисел. Модульная арифметика

Целые числа, делимость. Отношение сравнения. Его свойства. Алгоритм Евклида: прямой и обратный ход. Классы вычетов, свойства. Решение задач с использованием свойств сравнений. Кольцо классов вычетов по модулю: построение и доказательство аксиом. Примеры. Модульная арифметика. Малая теорема Ферма. Китайская теорема об остатках. Понятие о криптографии. Открытый ключ, метод RSA.

4.2.4 Алгебраические структуры

Понятие алгебраической операции на множестве. Таблица Кэли. Свойства операции. Определение и простейшие свойства группы. Абелева группа. Циклическая группа. Изоморфизм. Примеры групп: аддитивная группа комплексных чисел, аддитивная группа вещественных чисел, мультипликативные группы. Группа преобразований симметрии. Группа подстановок: некоммутативность, порядок группы, изоморфизм группе симметрии правильного треугольника. Подгруппы: определение, примеры, смежные классы по подгруппе, теорема Лагранжа. Порядок элемента делит порядок группы. Нормальный делитель. Фактор-группа.

Алгебры с двумя операциями. Кольца и поля. Определение и простейшие свойства кольца: единственность обратного элемента, группа обратимых элементов, примеры, $Z \subset Q \subset R \subset C$. Кольцо многочленов $C[x]$, кольцо квадратных матриц. Поле: определение, примеры. Характеристика, мультипликативная группа, примитивный элемент. Изоморфизм конечных полей одного порядка. Теоремыы об отсутствии делителей нуля, о поле классов вычетов простого модуля. Подполе. Поля Галуа.

4.2.5 Конечные поля

Конечные поля и многочлены. Кольцо многочленов над конечным полем. Деление с остатком. Классы вычетов по модулю. Порядок кольца классов вычетов по модулю многочлена. Поле классов вычетов по модулю неприводимого многочлена. Расширение простого поля. Полиномиальное описание конечных полей. Свойства конечных полей. Т. о порядке конечного поля (б/д). $(a+b)^p=a^p+b^p$. $F_q\backslash\{0\}$- циклическая группа. $x^{q-1}-1=(x-a_1)(x-a_2)\ldots(x-a_{q-1})$. НОД многочленов. Алгоритм Евклида для многочленов. Минимальный многочлен. Векторное пространство над конечным полем. Определение. Базис и размерность. Примеры. Число элементов.

4.2.6 Векторное пространство над конечным полем. Линейные коды

Помехоустойчивое кодирование. Блоковые коды. Основная терминология. Разреженность кода. Расстояние по Хеммингу. Его свойства. Неравенство Хемминга. Исправление и обнаружение ошибок. Т. о расстоянии и ошибках. Примеры кодов и их характеристики.

Линейные коды. Определение, порождающая и проверочные матрицы. Т. о связи матриц. Эквивалентные коды. Т. об эквивалентных кодах. Систематический код. Нахождение проверочной матрицы.

Разреженность линейного кода. Вес Хемминга. Т. о столбцах проверочной матрицы. Неравенство Синглтона.

Декодирование. Лидеры. Таблица декодирования. Синдромное декодирование. Коды Хемминга и связанные с ними. Определение. Т. об исправляющих свойствах. Декодирование кода Хемминга.

4.2.7 Многочлены над конечными полями. Циклические коды

Циклические коды. Полиномиальное описание кода. Т. о полиномиальных кодах. Порождающие многочлены. Свойства порождающего многочлена. Проверочный многочлен. Дуальные коды. Синдромный многочлен. Систематический код и его порождающая и проверочная матрицы.

Декодирование циклических кодов. Свойства синдромного многочлена. Локаторы ошибок, построение и решение уравнения для локаторов.

Минимальный многочлен, сопряженные элементы, циклотомические классы. Разложение многочлена (x^n-1) на неприводимые.

Теорема БЧХ, построение кода с заданными свойствами. Код Рида-Соломона: два определения, их эквивалентность. Примеры применимости кода Рида-Соломона.

4.2.7 Элементы теории графов

Графы. Основная терминология. Граф. Вершина, ребро, дуга. Неориентированный граф, ориентированный граф (орграф). Кратные ребра (дуги). Петли. Смежные вершины, смежные дуги. Степень вершины. Инцидентные ребро и вершина, дуга и вершина. Укладка графа. Плоский граф.

Лемма о рукопожатиях. Лемма о числе вершин с нечетной степенью.

Описание графов для ЭВМ: матрица смежности, матрица инцидентности. Список смежности. Изоморфизм графов.

Задача о минимальном остове связанного графа и ее применение. Связность как бинарное отношение, компоненты связности. Дерево, остов. Алгоритмы решения задачи о минимальном остове. Понятие о сложности алгоритма.

Обход графа. Длина маршрута, расстояние между вершинами. Задача о крат-

чайшем пути в связном графе. Постановка задачи и примеры.Задача о кратчайшем пути в связном графе. Алгоритм Дейкстры и его программная реализация. Применения.

Двудольные графы. Паросочетание. Задача о построении максимального паросочетания. Чередующиеся цепи, алгоритм расширяющейся цепи.

Транспортная сеть. Пропускная способность и поток. Насыщенные дуги и пути. Алгоритм Форда-Фолкерсона.

4.2.8 Сжатие информации.

Алфавитное кодирование. Эффективное кодирование: Фано и Хаффмана. Префиксные коды. Примеры построения дерева кода (Н-дерева). Адаптивные методы

Алгоритм Зива-Лемпеля и его реализации. Архивация файлов. Сжатие с потерей и без потерь.

ЛИТЕРАТУРА

1. Новиков Дискретная математика.
2. Яблонский С.С. Введение в дискретную математику.
3. См. сайт yourtutor.narod.ru