

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Председатель Учебно-методического
объединения вузов Республики Беларусь
по естественнонаучному образованию

_____ В.В. Самохвал

« ____ » _____ 2006 г.

Регистрационный № ТД - ____ /тип.

МЕТОДЫ КОМБИНАТОРНОГО АНАЛИЗА

Учебная программа
для Белорусского государственного университета по специальности

1- 98 01 01- 01 Компьютерная безопасность

**Минск
2006**

Составители:

Е.Н. Орлова – доцент кафедры математического моделирования и анализа данных, кандидат физ.-мат. наук, доцент

Рецензенты:

Кафедра высшей математики №3 Белорусского национального технического университета;

В.И. Берник – главный научный сотрудник отдела комбинаторных моделей и алгоритмов Института Математика НАН Беларуси, доктор физ.-мат. наук, профессор

Рекомендована к утверждению в качестве базовой для БГУ:

Кафедрой математического моделирования и анализа данных Белорусского государственного университета
(протокол №15 от «04» апреля 2006 г.).

Научно-методической комиссией факультета прикладной математики и информатики Белорусского государственного университета
(протокол №__ от «__» _____ 2006г.).

Ученым Советом факультета прикладной математики и информатики
(протокол №5 от «25» апреля 2006 г.).

Научно-методическим Советом Белорусского государственного университета
(протокол №__ от «__» _____ 2006г.).

Согласована

Научно-методическим Советом по компьютерной безопасности УМО вузов Республики Беларусь по естественнонаучному образованию
(протокол №__ от «__» _____ 2006г.).

Ответственный за редакцию: Е.Н. Орлова

Ответственный за выпуск: О.А. Кастрица

Пояснительная записка

Целью курса «Методы комбинаторного анализа» является обучение студентов навыкам исследования теоретических проблем комбинаторного анализа, технике решения задач комбинаторного характера и применению его в криптологии. Этот курс предлагается как общий курс для студентов специальности «Компьютерная безопасность» и других родственных специальностей.

Введение

Предмет теории комбинаторного анализа. Основные понятия и определения. Области применения изучаемой дисциплины. Примеры прикладных задач.

Комбинаторные схемы и объекты

Комбинаторные отношения. Выборки и упорядочения. Разбиения. Множества. Отображения, соответствия, функции, операции, алгебры. Числа, многочлены, операторы. Преобразования. Булевы функции. Цикловое строение. Комбинаторные тождества.

Метод производящих функции

Формальные степенные ряды. Производящие функции: свойства и операции. Специальные числа и специальные функции. Метод дифференциальных уравнений. Метод линейных функционалов. Асимптотические разложения. Числа Каталана. Экспоненциальные производящие функции.

Логические методы

Метод включения и исключения. Системы представителей множеств. Теорема и числа Рамсея. Неравенство Бонферрони. Формулы обращения для частично упорядоченных множеств. Беспорядки. Число булевых функций, существенно зависящих от всех своих переменных. Функции Эйлера и Мебиуса.

Комбинаторные таблицы и схемы

Специальные матрицы. Латинские прямоугольники и квадраты. Системы троек Штейнера и сходные наборы. Блок-схемы. Проблема Ван-дер-Вардена.

Геометрические методы

Графы. Деревья. Циклы подстановок. Графы преобразований. Блоки. Конечные плоскости.

Общая комбинаторная схема и теория Пойа

Группы и эквивалентность отображений. Общая комбинаторная схема. Несимметричные n -базисы. Симметричные n -базисы. Теорема Пойа.

Вероятностные методы в комбинаторном анализе

Вероятностные распределения и случайные величины. Моменты случайных величин. Неотрицательные целочисленные матрицы. Покрытия множеств. Производящие функции и предельные теоремы. Разбиения конечных множеств. Конечные топологии. Разделяющие системы множеств. Случайные подстановки. Случайные размещения. Обобщенная схема размещений. Случайные графы. Гигантские компоненты. Случайное блуждание на прямой и связанные с ним задачи. Производящие функции дискретных распределений и их свойства. Производящие функции моментов. Вероятностные методы решения комбинаторных задач. Методы 1-х и 2-х моментов. Случайные комбинаторные объекты. Получение асимптотических оценок в комбинаторных задачах с помощью вероятностных методов.

Перманенты и трансверсали

Свойства перманентов. Перманенты и трансверсали. Неразложимые и вполне разложимые матрицы. Оценки перманента. Стохастические матрицы. Теорема Биркгофа.

Асимптотические методы

Оценки интервалов по методу Лапласа. Время ожидания коллизии. Комплексный анализ. Формула Коши. Метод перевала. Формула Стирлинга.

Литература.

1. Комбинаторный анализ. Задачи и упражнения./ Под. ред. Рыбникова К.А.. 1982г.
2. В.Н. Сачков. Введение в комбинаторные методы дискретной математики. 1982г.
3. С.К. Ландо. Лекции о производящих функциях. 2002г.