

Базовый курс “Дискретная математика”
ФКН НИУ ВШЭ, 1-й курс, модули 1-3,
лекторы М.Н. Вялый и В.В. Подольский

В курсе будет рассказано об основных понятиях, методах и приемах дискретной математики, а также будет дано базовое представление о том, как эти знания могут применяться в Computer Science.

Примерная программа курса

Основные темы

Математическая индукция. Формулировка, примеры рассуждений. Коды Грея, теорема Холла о представителях.

Множества и логика. Операции с множествами. Логические связки, таблицы истинности. Дизъюнктивная нормальная форма, полиномы Жегалкина. Формула включений и исключений.

Комбинаторика. Подсчет вариантов. Число подмножеств, число n -битовых слов, взаимно-однозначное соответствие. Рекуррентные формулы. Перестановки. Бином Ньютона, треугольник Паскаля. Числа Каталана.

Отношения и их графы. Бинарные отношения и двудольные графы. Отношения эквивалентности, классы. Неориентированные графы. Функции, инъекции, сюръекции, биекции. Образы и прообразы. Перестановки, разложение в циклы, транспозиции, порядок перестановки.

Упорядоченные множества. Частичный порядок, примеры. Изоморфизм упорядоченных множеств. Методы доказательства неизоморфности. Линейный порядок. Фундированные множества и индукция. Цепи и антицепи.

Мощность множеств. Мощность множества, конечная и бесконечная мощность. Счетные множества, счетность множества целых и рациональных чисел. Несчетные множества. Континуальные множества. Несчетность континуальных множеств.

Графы: начальные сведения. Ориентированные и неориентированные графы. Степени вершин. Пути. Связные компоненты. Циклы. Деревья. Число вершин и рёбер в дереве. Эйлеров цикл, критерий его существования для ориентированных и неориентированных графов. Теоремы рамсеевского типа для конечных и бесконечных графов.

Вероятность: первые шаги. Конечное вероятностное пространство, события, формула сложения вероятностей. Комбинаторные формулы и вероятность. Вероятностные доказательства существования (оценка сверху вероятности нарушения одного из требований с помощью union bound). Математическое ожидание и его линейность. Условные вероятности, теорема Байеса, независимые события.

Основы теории чисел. Делимость, делимость с остатком. НОД и НОК. Алгоритм Евклида. Обратный ход алгоритма Евклида и диофантовы уравнения. Основная теорема арифметики.

Теория чисел, продолжение. Функция Эйлера. Малая теорема Ферма и теорема Эйлера. Китайская теорема об остатках.

Сложность алгоритмов: разрешающие деревья. Задача об отгадывании числа: алгоритм как разрешающее дерево. Двоичный поиск. On-line и off-line алгоритмы. Сложность алгоритма, верхние и нижние оценки. Верхние и нижние оценки для сортировки. Adversary arguments для нижних оценок.

Выполнимость булевых формул. Конъюнктивная нормальная форма, задача о выполнимости. Редукция произвольной формулы к 3-КНФ. Исчисление резолюций, теорема о полноте. Алгоритм проверки выполнимости для 2-КНФ. Во всякой 3-КНФ можно выполнить 7/8 условий (вероятностное доказательство).

Схемы из функциональных элементов. Схемы и вычисляемые ими булевы функции, полнота. Размер и глубина схемы. Схемы для сложения и умножения чисел. Большинство функций имеют экспоненциальную сложность.

Коды с исправлением ошибок. Булев куб и расстояние Хемминга. Исправление ошибок и кодовое расстояние. Отгадывание числа с неверными ответами. Верхняя оценка для числа кодовых слов. Код Хемминга.

Вычислимость и перечислимость. Алгоритмы со входом и выходом. Вычислимые функции. Перечислимые и разрешимые множества. Теорема Поста. Рефлексия: возможность пошагового выполнения и универсальный интерпретатор. Универсальная функция, перечислимое неразрешимое множество, неразрешимость проблемы останова.

Машины Тьюринга. Машины Тьюринга, примеры. Тезис Черча-Тьюринга. Лемма об очистке мусора. Многоленточные машины Тьюринга. Универсальная машина Тьюринга. Машины Тьюринга без возможности записи и конечные автоматы. Машины Тьюринга, изменяющие значение каждой ячейки не более одного раза.

Дополнительные темы

Конкретные неразрешимые задачи. Системы Туэ. Проблема выводимости в данной системе Туэ. Полугруппы. Проблема распознавания равенства в полугруппе.

Неподвижная точка. Программа, печатающая свой текст. Обобщение: каков бы ни был преобразователь программ, есть неподвижная точка.

Независимость от выбора языков программирования (если есть взаимная трансляция).

Формулы первого порядка. Примеры формул со свободными переменными и без, их интуитивный смысл. Сигнатура, интерпретация, формула, параметры. Выразимые предикаты. Примеры выразимости. Доказательство невыразимости с помощью автоморфизмов. Доказательство невыразимости с помощью элиминации кванторов. Изоморфизм и элементарная эквивалентность интерпретаций.

Игры и стратегии. Конечные игры с полной информацией. Цена игры, теорема Цермело. Доказательства существования стратегии. Игра Ним и игры Шпрага – Гранди.

Линейное программирование. Линейные (однородные) равенства. Семантическое и синтаксическое следование, их эквивалентность. Совместные и несовместные системы линейных неоднородных равенств: если система несовместна, то можно вывести $0 = 1$ как линейную комбинацию. Совместные и несовместные системы линейных неоднородных неравенств: если система несовместна, то можно вывести $0 \geq 1$. Неотрицательная линейная оболочка конечного множества векторов есть пересечение конечного числа полупространств. В любой матрице есть либо нетривиальная неотрицательная линейная комбинация строк, в которой все координаты неотрицательны, либо нетривиальная неотрицательная линейная комбинация столбцов, в которой все координаты неположительны.

Игры с нулевой суммой. Игра в орлянку и в каком смысле она честная (вероятностные стратегии). Примеры игр. Цена игры. Теорема фон Неймана о существовании цены игры.