Лекции по дискретной математике, Пилотный поток, 2016-2017

1 Математическая индукция

- Примеры рассуждений: двухцветная раскраска, наличие треугольника.
- Равенства: $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$, $1 + 2 + 4 + 8 + \ldots + 2^{n-1} = 2^n - 1$.
- Неравенства: $(1 + h)^n \geq 1 + hn$ (при $1 + h \geq 0$);
  $1 + 1/4 + 1/9 + \ldots + 1/n^2 < 2$ (усиление утверждения для индукции).
- Двоичная система: гирями в $1, 2, 4, \ldots, 2^{n-1}$ можно уравновесить любой груз от 0 до $2^n - 1$ единственным образом.
- Исключение переменных: система из менее чем n линейных однородных уравнений относительно $x_1, \ldots, x_n$ имеет ненулевое решение.
- Слова длины n, коды Грея.
- Индуктивное доказательство теоремы Холла о представителях.

2 Комбинаторика

- Формулы суммы и произведения при подсчёте вариантов.
- Сумма множеств и декартово произведение.
- Число подмножеств, число n-битовых слов, взаимно однозначное соответствие.
- Рекуррентные формулы: число путей, число слов без двух нулей подряд.

- Перестановки.
- Число подмножеств данного размера, треугольник Паскаля.
- Формула для чисел сочетаний. Бином Ньютона.
- Числа Каталана.

3 Множества и логика

- Обозначения: $x \in A$, $A \cap B$, $A \cup B$, $A \setminus B$, $A \subset B$, $A = B$.
- Тождества. Доказательство $(A \cap B) \setminus C = (A \setminus C) \cap B$, иллюстрация на картинке и почему эту картинку можно считать доказательством (разбор случаев).
- Логические связки и операции с множествами, таблицы истинности, выражение одних через другие, законы де Моргана.
- Полнота: доказательство с дизъюнктивной нормальной формой и с полиномом Жегалкина.
- Формула включений и исключений для двух и трёх множеств.
- Общая формула: доказательство по индукции и с индикаторами.

4 Отношения и их графы

- Бинарные отношения и двудольные графы.
- Отношения эквивалентности, классы.
- Неориентированные графы. Связные компоненты.
- Функции, инъекции, сюръекции, биекции.
- Образы и прообразы.
- Композиция отношений и функций.
- Перестановки, разложение в циклы, транспозиции, порядок перестановки.

5 Мощность множеств

- Мощность множества, конечная и бесконечная мощность.
- Счетные множества; замкнутость относительно счетного объединения; счетность множества целых и рациональных чисел.
- Несчетные множества. Континуальные множества: действительная прямая, интервал, отрезок, бесконечные двоичные последовательности. Несчетность континуальных множеств.

6 Упорядоченные множества

- Частичный порядок. Примеры: сумма и произведение, лексикографический порядок, покоординатный порядок на словах.
- Изоморфизм упорядоченных множеств. Почему не изоморфны: минимальные и максимальные элементы, плотность.
- Линейный порядок, единственность на конечном множестве.
- Фундированные множества и индукция.
- Цепи и антицепи.

7 Графы: начальные сведения

- Ориентированные и неориентированные графы. Степени вершин. Сумма степеней.
- Пути. Связные компоненты. В связном графе с n вершинами не менее $n-1$ рёбер.
- 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.

8 Графы: продолжение

- Клики и независимые множества; вершинные покрытия.
- Теорема Холла.
-

9 Вероятность: первые шаги

- Мотивировка: равновозможность, вероятность как доля, частота.
- 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.
- Закон больших чисел для бернуллиевского распределения: доказательство со сравнением мер.

10 Основы теории чисел

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

11 Теория чисел, продолжение

- Функция Эйлера.
- Малая теорема Ферма и теорема Эйлера.
- Китайская теорема об остатках.

12 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 (мощностные).
- Adversary arguments для нижних оценок (пример).
- Порядковые статистики: линейный алгоритм.

13 Схемы из функциональных элементов

- Схемы и представляемые ими булевы функции. Полнота.
- Размер и глубина схемы.
- Сложение чисел: схема линейного размера.
- Умножение чисел: схема квадратичного размера.
- Большинство функций имеют экспоненциальную сложность.
- Быстрые вычисления: сложение с линейным размером и логарифмической глубиной.
- Субквадратичное умножение: трюк Карацубы.

14 Вычислимость и перечислимость

- Алгоритмы со входом и выходом. Вычислимые функции. Существование невычислимой функции.
- Перечислимые и разрешимые множества. Варианты определений, теорема Поста, вычислимость функции и перечислимость графика.
- Рефлексия: возможность пошагового выполнения и универсальный интерпретатор.
- Универсальная функция, перечислимое неразрешимое множество, неразрешимость проблемы остановки, неотделимые множества.

15 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.

16 Конкретные неразрешимые задачи

- Системы Туэ. Проблема выводимости в данной системе Туэ.
- Полугруппы. Проблема распознавания равенства в полугруппе.

17 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)
- Доказательство для специального языка программирования с системными вызовами « текст программы» и « выполнить».
- Доказательство с диагональной конструкцией: $A(p) =$ « программа, которая делает не то, что $p(p)$».