Билеты по дискретной математике, 3 модуль

Таисия Чегодаева, ПАДИИ, 1 курс

28 March 2023

1 Отношение равномощности множеств. Разные определения бесконечного множества. Примеры.

Определение:
Множества называются *равномощными*, если между ними можно установить взаимно однозначное соответствие (т.е. биекцию).
Отношение равномощности - отношение эквивалентности.

2 Счётные множества. Теорема о свойствах счетных множеств (подмножества счетных множеств, минимальность среди бесконечных, нбчс объединение нбчс множеств- нбчс).

Определение:
Множество называется счетным, если оно равномощно $\mathbb{N}$.

Теорема:
1. Подмножество счетного множества конечно или счетно.
2. Всякое бесконечное множество содержит счетное подмножество.
3. Объединение конечного или счетного числа конечных или счетных множеств конечно или счетно.

Доказательство:
1. Пусть B - подмножество счетного множества A. $A = a_1, a_2, ...$. Удалим из A такие элементы, которые не принадлежат B. Тогда оставшиеся элементы образуют либо конечную последовательность (B - конечное), либо бесконечную последовательность (B - счетное).
2. Пусть A - бесконечное множество. Тогда выберем $b_1, b_2, ..., b_n, ...$. Занумеруем их в порядке выбора. Тогда эти элементы будут составлять счетное

множество B.
3. Пусть $A_1, A_2, ..., A_n, ...$ - множество счетных подмножеств. Тогда расположим их элементы друг под другом, получим таблицу. Пройдем через диагонали по всей таблице, получим счетное множество.

3 Счетность множества $\mathbb{Q}$.

Рациональные числа представляются дробями, где числитель и знаменатель - целые числа. Множество дробей с определенным знаменателем счетно, значит, $\mathbb{Q}$ - объединение таких множеств, т.е. $\mathbb{Q}$ - счетное.

4 Теорема об объединении счетного и бесконечного множеств.

Теорема:
Если множество A бесконечно, а множество B конечно или счетно, то $A \cup B$ равномощно A.

Доказательство:
Выделим в A счетное подмножество P, оставщееся множество обозначим за Q. $B + P$ и P счетные, значит, $B + P + Q$ равномощно $P + Q$.
В данном доказательстве $+$ - объединение непересекающихся множеств.

5 Равномощность единичного отрезка и множества бесконечных битовых последовательностей.

Заметим, что любое число из $[0, 1]$ может быть записано в виде бесконечной двоичной дроби: первый знак дроби равен 0, если $x \in [0, \frac{1}{2})$, в противном случае первый знак дроби равен 1. И так далее можно построить бесконечную двоичную дробь.

6 Равномощность квадрата и отрезка. Схема построения биекции.

Заметим, что паре последовательностей для координаты (x, y) можно сопоставить последовательность чередующихся знаков $x_0y_0x_1y_1...$. Значит, нашлось взаимно однозначное соответствие.

7 Теорема Кантора-Бернштейна.

Теорема:
Если множество A равномощно некоторому подмножеству множества B, а множество B равномощно некоторому подмножеству множества A, то A и B равномощны.

Доказательство:
пусть A Равномощно подмножеству B_1 множества B, B равномощно подмножеству A_1 множества A. Тогда при биекции между B и A_1 $B_1 \in B$ переходит в $A_2 \in A_1$. При этом множества B_1, A, A_2 равномощны
ДУШНОЕ ДОКАЗАТЕЛЬСТВО

8 Теорема Кантора в формулировке несчетности множества бесконечных битовых последовательностей.

Теорема:
Множество бесконечных последовательностей из нулей и единиц несчетно.

Доказательство:
предположим, что это множество счетное. Тогда занумеруем все последовательности из 0 и 1 и составим таблицу из этих последовательностей.
Рассмотрим последовательность, состоящую из элементов, находящихся на диагонали таблицы: пусть $\beta_i = 1 - \alpha_i$, где i - номер строчки и столбца в таблице. Тогда β отличается от всех остальных последовательностей в i позиции, значит, отсутствует в таблице. Противоречие.

9 Парадокс Кантора. Общая формулировка: теорема Кантора о неравномощности X и 2^X.

Теорема:

$$X \neq 2^X$$

Доказательство:
абоба

Парадокс Рассела:

10 ZFC. Аксиомы о равенстве и существовании множеств. Примеры применения.

11 ZFC. Аксиомы об образовании множеств. Примеры применения.

12 ZFC. Аксиомы регулярности и выбора. Примеры применения. Примеры необходимости использования аксиомы выбора.

13 Операции над мощностями.

1. $|A| + |B| = |A \cup B|$, если $A \cap B = \varnothing$.
2. $|A| \cdot |B| = |A \times B|$.
3. $f : B \longrightarrow A$. $|f| = |A|^{|}B|$.
4. Существуют коммутативность, ассоциативность или дистрибутивность относительно сложения и умножения.
5. $a^{b+c} = a^b \times a^c$.
6. $(ab)^c = a^c \times b^c$.
7. $(a^b)^c = a^{b \times c}$.

14 Теорема Кенига о равномощном элементе конечного разбиения бесконечного множества.

Теорема:
Если множество $A_1 \times A_2 \times ... \times A_n$ разбито на непересекающиеся части $B_1, B_2, ..., B_n$, то найдется такое i, что мощность B_i не меньше мощности A_i.

Доказательство:

15 Отношения эквивалентности, частичного и линейного порядка. Строгие и нестрогие порядки.

Определение:
Бинарное отношение R на множестве X называется *отношением эквивалентности*, если выполняется следующее:

1. $xRx \ \forall x \in X$.
2. $xRy \Longrightarrow yRx \ \forall x, y \in X$.
3. $xRy, yRz \Longrightarrow xRz \ \forall x, y, z \in X$.

Определение:
Бинарное отношение $\leq$ на множестве X называется *отношением частичного порядка*, если выполняется следующее:
1. $x \leq x \ \forall x \in X$.
2. $x \leq y, y \leq x \Longrightarrow y = x \ \forall x, y \in X$.
3. $x \leq y, y \leq z \Longrightarrow x \leq z \ \forall x, y, z \in X$.

Определение:
Частично упорядоченное множество (ЧУМ) - множество с заданным на нем частичным порядком.

Определение:
Два элемента множества сравнимы, если $x \leq y$ или $y \leq x$.

Определение:
Бинарное отношение $\leq$ на множестве X называется *отношением линейного порядка*, если кроме условий для частичного порядка выполняется, что любые два элемента из X сравнимы.

Определение:
$<$ - отношение строгого порядка.
$\leq$ - отношение нестрогого порядка.

16 Операции над ЧУМ. Наибольшие и максимальные, наименьшие и минимальные элементы ЧУМ.

Определение:
Элемент ЧУМа называется *наибольшим*, если он больше любого другого элемента.
Элемент ЧУМа называется *наименьшим*, если он меньше любого другого элемента.
Элемент ЧУМа называется *максимальным*, если не существует большего элемента.
Элемент ЧУМа называется *минимальным*, если не существует меньшего элемента.

Операции над ЧУМ:
1.

17 Изоморфизмы. Теорема об изоморфности для конечных множеств.

Определение:
Два ЧУМа называются *изоморфными*, если между ними существует взаимно однозначное соответствие, сохраняющее порядок (изоморфизм).

Теорема:
Конечные линейно упорядоченные множества из одинакового числа элементов изоморфны.

Доказательство:

18 Примеры неизоморфных равномощных множеств.

1. $[0, 1]$ не изоморфно $\mathbb{R}$.
2. $\mathbb{Z}$ не изоморфно $\mathbb{Q}$.

19 Плотные множества. Теорема об изоморфности счетных плотных множеств.

Определение:
Линейно упорядоченное множество называется *плотным*, если в нем нет соседних элементов (т.е. между любыми двумя элементами существует третий).

Теорема:
Любые два счетных плотных линейно упорядоченных множества без наибольших и наименьших элементов изоморфны.

Доказательство:
Пусть X, Y - данные множества. Будем строить изоморфизм по шагам: на каждом шаге выбираем какой-то элемент из X, находим его местоположение относительно других элементов в X, затем выбираем элемент из Y, находящийся в том же положении. Так выбрать можно, т.к. множества плотные и без наибольших/наименьших элементов.
Почему изоморфизм корректен? Пронумеруем X и Y, будем выбирать неохваченный элемент с наименьшим номером (на нечетных шагах - из X, на четных - из Y).

20 Теорема об изоморфности счетного множества и подмножества $\mathbb{Q}$

Теорема:
Всякое счетное линейно упорядоченное множество изоморфно некоторому подмножеству множества $\mathbb{Q}$.

Доказательство:
Аналогично предыдущему билету.

21 Теорема о допустимости индукции (эквивалентность трех свойств). Фундированные множества.

Теорема:
Следующие три свойства ЧУМа X равносильны:
1. Любое непустое подмножество X имеет минимальный элемент.
2. Не существует бесконечной строго убывающей последовательности элементов множества X.
3. Для множества X верен принцип индукции:если при каждом $x \in X$ из истинности $A(y)$ для всех $y < x$ следует истинность $A(x)$, то свойство $A(x)$ верно для всех x.

Доказательство:
ляляля

Определение:
Множества, обладающие этими тремя свойствами - *фундированные.*

22 Теорема о произведении фундированных множеств.

Теорема:
A, B - фундированные ЧУМы. Тогда

$$A \times B =< a_1, b_1 >\leq< a_2, b_2 >\Longleftrightarrow [(b_1 < b_2) \; or \; (b_1 = b_2 \; and \; a_1 \leq a_2)]$$

Доказательство:

23 Вполне упорядоченные множества. Примеры.

Определение:
Вполне упорядоченные множества - фундированные линейно упорядоченные множества.

Примеры:

24 Теорема Цермело. Цели и следствия.

Теорема:
Всякое множество может быть вполне упорядочено.

Теорема:
Из любых двух множеств одно равномощно подмножеству другого.

Цели:

25 Лемма Цорна. Цели и следствия. Теорема о продолжении частичного порядка до линейного.

Теорема:
Пусть Z - ЧУМ, в котором всякая цепь имеет верхнюю границу. Тогда в Z есть максимальный элемент.

Цели:
ляляля

Теорема:
Всякий частичный порядок может быть продолжен до линейного.

Доказательство:
лд

26 Высказывания. Логические связки. Пропозициональные формулы. Теорема об однозначности разбора.

Определение:
Логическая связка - логический символ, соединяющий между собой высказывания.

Определение:
Пропозициональная переменная - элементарное высказывание.

Определение:
Пропозициональная формула - формула, построенная следующим образом:
1. Любая пропозициональная переменная - формула.
2. Если A - пропозициональная формула, то $\overline{A}$ - тоже пропозициональная формула.
3. Если A, B - пропозициональные формулы, то $A \wedge B, A \vee B, A \longrightarrow B$ - пропозициональные формулы.

Теорема:
Пропозициональная формула, не являющаяся переменной, может быть представлена ровно в одном из четырех видов: $(A \wedge B), (A \vee B), (A \longrightarrow B)$ и $\overline{A}$, где A, B - некоторые формулы, причем A и B восстанавливаются однозначно.

Доказательство:

27 Булевы функции. Теорема о выразимости булевой функции в КНФ и ДНФ.

Определение:
$\varphi : \mathbb{B}^n \longrightarrow \mathbb{B}$. φ - булева функция n аргументов.

Теорема:
Всякая булева функция может быть в конъюнктивной нормальной форме или дизъюнктивной нормальной форме.

Доказательство:

28 Полиномы Жегалкина. Теорема о полиномах Жегалкина (выразимость булевых формул).

Определение:
Моном - конъюнкция любого набора переменных или константа 1.
Полином Жегалкина - сумма мономов, взятая по модулю 2.

Теорема:
Всякая булева функция представляется полиномом Жегалкина.

Доказательство:

29 Критерий Поста.

Критерий Поста:
Набор булевых функций является полным тогда и только тогда, когда он не содержится целиком ни в одном из следующих классов функций:
1. Монотонные функции (не убывают по каждому из своих аргументов)
2. Линейные функции (представимы многочленом, в котором все мономы содержат не более 1 переменной)
3. Функции, сохраняющие 0: $f(0, 0, ..., 0) = 0$
4. Функции, сохраняющие 1: $f(1, 1, ..., 1) = 1$
5. Самодвойственные функции: $f(1-p_1, 1-p_2, ..., 1-p_n) = 1-f(p_1, p_2, ..., p_n))$.

Доказательство:

30 Схемы из функциональных элементов. Сложность схемы. Теорема о линейной зависимости размеров схем.

Определение:
Сложность булевой функции f - $size_B(f)$ - минимальный размер схемы из B-элементов, вычисляющей функцию f.

Теорема:
Всякая булева функция представляется полиномом Жегалкина.

31 Теоремы о схемах для операции сравнения.

Теорема:
Пусть B - полный набор булевых функций. Существует такая константа C, что $size_B(Comp_n) \leq C \cdot n$.

Доказательство: Дополним число бит в каждом из бит до степени двойки нулями слева.
Будем строить схему с $2n$ входами (по n бит для кждого числа) и 2 выходами, где результат 10 - $x = y$, 01 - $x < y$, 00 - $x > y$. Рекурсивно соберем схему:

$$T(2n) \leq 2 \cdot T(n) + c \Longrightarrow T(2^k) \leq c' \cdot 2^k$$

где c, c' - некоторые константы.

32 Теоремы о схемах для сложения.

Теорема:
Существует схема размера $O(n)$, осуществляющая сложение двух n-битовых чисел.

Доказательство:
Складываем числа в столбик: заметим, что каждый из битов переноса или результата определяется тремя другими битами (бит результата равен сумме битов чисел и бита переноса, взятой по модулю 2, а бит переноса равен 1, если . Значит, составить такую схему можно.

Теорема:
Существует схема размера $O(n)$ и глубины $O(\log n)$, осуществляющая сложение двух n-битовых чисел.

Доказательство:
Заметим, что вычисление битов переноса равносильно сравнению. Дальше полуочев. За k шагов до конца мы знаем результаты сравнения всех суффиксов, длины которых кратны 2^k.

33 Теоремы о схемах для умножения.

Теорема:
Существует схема размера $O(n^2)$ и глубины $O(\log n)$, осуществляющая умножение двух n-битовых чисел.

Доказательство:
kzkzkzk

Теорема:
Существует схема размера $O(n^{\log_2 3})$ и глубины $O(\log^2 n)$, осуществляющая умножение двух n-битовых чисел.

Доказательство:

34 Аксиомы исчисления высказываний. Логический вывод.

35 Теорема о корректности ИВ.

36 Теорема о полноте ИВ: схема доказательства и лемма о тавтологии (X->X).

37 Лемма о дедукции.

38 Лемма о разборе случаев для для логических связок.