Дискретная математика. Теормин — I

Содержание

Теория множеств

Множество

Множество - неупорядоченная коллекция различных объектов, именуемых элементами.

Принадлежность элемента множеству

Булевый оператор, который отвечает на запрос «находится ли элемент в множестве»:

- $1 \in \{1, 2, 3\}$
- $\{1, 2\} \in \{\{1, 2\}, \{3, 4\}\}$
- $4 \notin \{1, 2, 3\}$
- $\{1\} \notin \{1, 2, 3\}$
- $2 \notin \{1, \{2\}, 3\}$

Аксиома объёмности

Два множества равны, если у них одинаковые элементы.

$$\forall A, B : [(\forall x : (a \in A \Leftrightarrow b \in B)) \to (A = B)]$$

Урэлементы

Урэлементы – объекты, которые не являются множествами сами по себе, но могут находиться в множестве.

Пустое множество

Множество, внутри которого нет элементов. По ZFC:

$$\exists \emptyset : \forall x : x \notin \emptyset$$

Универсальное множество

Специальное множество, в котором есть все элементы (в т.ч. множества) какого-то принятого универсума.

Но вообще-то говоря, в ZFC, существование универсального множества ведет к противроечию с аксиомой пары.

Отношение подмножества

Множество A является подмножеством B, если все элементы из A также есть в B:

$$A \subseteq B \Longleftrightarrow \forall x : ((x \in A) \to (x \in B))$$

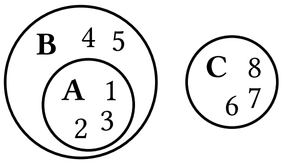
Булеан

Булеан A – множество всех подмножеств A:

$$\mathcal{P}(A) = \{S \mid S \subseteq A\} \qquad |\mathcal{P}(A)| = 2^{|A|}$$

Диаграммы Венна и круги Эйлера

Круги Эйлера – визуальное представление множеств и их отношений (подмножество, пересечение) с помощью замкнутых фигур (обычно кругов):



$A = \{1, 2, 3\}$

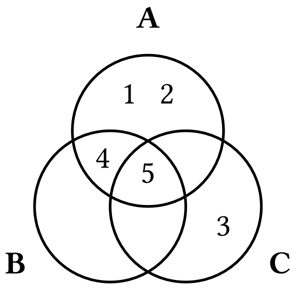
$B = \{1, 2, 3, 4, 5\}$

$C = \{6, 7, 8\}$

$A \subseteq B$

$C \cap B = \emptyset$

Диаграмма Венна – визуальное представление множеств и их отношений с помощью пересекающихся кругов. Каждый круг означает множество, и их пересениеие показывает пересечения:



$A = \{1, 2, 4, 5\}$

$B = \{4, 5\}$

$C = \{3, 5\}$

$A \cap B = \{4, 5\}$

$A \cap B \cap C = \{5\}$

Мощность множества

Для *конечного* множества - количество элементов внутри него.

Для *бесконечного*:
- Счетное - имеющее такую же мощность, что и $\mathbb{N}$, т.е. имеющее биекцию с $\mathbb{N}$.
- Несчетное - если… не счетное, т.е. не имеющее биекцию с $\mathbb{N}$;

Конечные и бесконечные множества

- Конечное - если можно пересчитать его элементы.
- Бесконечное:
  - Счетное ($|A| = |\mathbb{N}|$)
  - Несчетное

Парадокс Рассела

Назовем A *обычным*, если $A \notin A$.

Назовем A *необычным*, если $A \in A$.

Сделаем множество *обычных множеств*:

$$R = \{A \mid A \notin A\}$$

Зададим вопрос: R - обычное?
- Пусть R обычное. Тогда $R \in R$. Тогда R необычное. Противоречие.
- Пусть R необычное. Тогда $R \notin R$. Тогда R необычное. Противоречие.

В любом случае получаем противоречие.

Аксиоматическая теория множеств

ZFC. Все есть множеств, нет урэлементов. 10 аксиом:
1. Множества с одинаковыми элементами равны
2. Существует пустое множество

3. Для любых a, b существует $\{a, b\}$
4. Для любых множеств существует их объединение
5. Для любого множества существует булеан
6. Существует бесконечное множество
7. Для любого мн-ва A и св-ва P существует $\{x \in A \mid P(x)\}$
8. Для любого мн-ва существует образ $F[A]$
9. Для любого непустого мн-ва существует минимальный элемент
10. Для любого семейства непустых мн-в существует функция выбора

Перечислительная форма задания множества

$$A = \{1, 2, 3, ...\}$$

Предикатная форма задания множества

$$A = \{x \mid P(x)\}$$

$P(x)$ - предикат, возвращает true/false

Разбиение множества

P - множество подмножеств A - называется разбиением, если:

1. Все подмножества P непустые
2. Все подмножества P попарно непересекающиеся
3. Объединение всех подмножеств P равно A

Непересекающиеся множества

$$A \cap B = \emptyset$$

Объединение, пересечение, разность и симметрическая разность множеств

- $A \cup B = \{x \mid x \in A \lor x \in B\}$
- $A \cap B = \{x \mid x \in A \land x \in B\}$
- $A \setminus B = \{x \mid x \in A \land x \notin B\}$
- $A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

Дополнение множества

$\overline{A} = U \setminus A$ для некоторого универсума U

Коммутативность, ассоциативность и дистрибутивность операций над множествами

- Коммутативность:
  - $A \cup B = B \cup A$
  - $A \cap B = B \cap A$
- Ассоциативность:
  - $A \cup (B \cup C) = (A \cup B) \cup C$
  - $A \cap (B \cap C) = (A \cap B) \cap C$
- Дистрибутивность:
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Законы де Моргана
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Законы тождества, идемпотентности, поглощения и доминирования
- Тождество:
  - $A = B \Longleftrightarrow \forall x : (x \in A \leftrightarrow x \in B)$
  - $A = B \Longleftrightarrow A \subseteq B \wedge B \subseteq A$
- Идемпотентность:
  - $A \cap A = A$
  - $A \cup A = A$
- Поглощение:
  - $A \cup (A \cap B) = A$
  - $A \cap (A \cup B) = A$
- Доминирование:
  - $A \cap \emptyset = \emptyset$
  - $A \cup U = U$

Бинарные отношения

Упорядоченная пара

$$\langle a, b \rangle \overset{\text{def}}{=} \{\{a\}, \{a, b\}\}$$

Кортеж
Конечная упорядоченная коллекция элементов: $(a_1, a_2, ..., a_n)$

Можно задать рекурсивно:

1. $() = \emptyset$
2. $$\begin{aligned} (a_1, a_2, ..., a_n) &= \langle a_1, (a_2, ..., a_n) \rangle \\ &= \langle a_1, \langle a_2, \langle ..., \langle a_n, \emptyset \rangle ... \rangle \rangle \rangle \end{aligned}$$

Декартово произведение множеств

$$A \times B = \{\langle a, b \rangle \mid a \in A, b \in B\}$$

Бинарное отношение

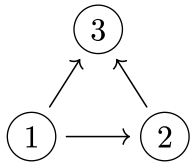
$$R \subseteq A \times B$$

$\langle a, b \rangle \in R$ - «*a относится к b*»

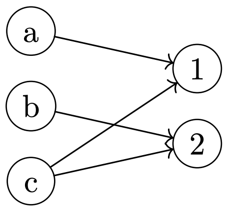
Однородные и неоднородные отношения
- Однородные (гомогенные): $R \subseteq M^2$
- Неоднородные (гетерогенные): $R \subseteq A \times B$

Графическое и матричное представление отношения
Графическое:
1. Для однородных:
   - Направленный граф

- Вершина - элемент M
- $\langle a, b \rangle \in R$ – ребро $a \to b$



2. Для неоднородных:
   - Двудольный граф
   - Левая доля - элементы A
   - Правая доля - элемент B
   - $\langle a, b \rangle \in R$ – ребро $a \to b$



Матричное: бинарная матрица $n \times m$:

$$[\![R]\!]_{ij} = \begin{cases} 1 & a_i \ R \ b_j \\ 0 & a_i \not R \ b_j \end{cases}$$

Пустое, универсальное и тождественное отношения

- Пустое: $\emptyset \subseteq M^2$
- Универсальное: $U_M = M^2$
- Тождественное: $I_M = \{\langle x, x \rangle \mid x \in M\}$

Обратное отношение

$$R^{-1} = \{\langle b, a \rangle \mid a \ R \ b\}$$

Объединение, пересечение, разность и дополнение отношений

- $R \cup S = \{\langle a, b \rangle \mid (a \ R \ b) \lor (a \ S \ b)\}$
- $R \cap S = \{\langle a, b \rangle \mid (a \ R \ b) \land (a \ S \ b)\}$
- $R \setminus S = \{\langle a, b \rangle \mid (a \ R \ b) \land (a \not S \ b)\}$
- $\overline{R} = \{\langle a, b \rangle \mid (a \not R \ b)\}$

Композиция отношений и степени отношения

Для $R \subseteq A \times B$ и $S \subseteq B \times C$:

$$R; S = S \circ R = \{\langle a, c \rangle \mid \exists b : (a \ R \ b) \land (b \ S \ c)\}$$

Для $R \subseteq M^2$:

$$\begin{aligned} &R^0 = I_M \\ &R^1 = R \\ &R^{n+1} = R^n \circ R, \quad n \geq 1 \end{aligned}$$

Рефлексивное, симметрическое и транзитивное замыкания

Замыкание - наименьшее отношение, включающее исходное и удовлетворяющая свойству.

- Рефлексивное: $r(R) = R \cup I_M$
- Симметрическое: $s(R) = R \cup R^{-1}$
- Транзитивное: $t(R)$ - объединение с минимальным мн-вом пар, чтобы новое отношение стало транзитивным

  Или так: $t(r) = R \cup R^2 \cup R^3 \cup \ldots$A (за $O(n^4)$)

Алгоритм Уоршелла (для транзитивного замыкания)

Работает за $O(n^3)$.

Идея в том, чтобы перебрать k-ую вершину и для каждой вершины i и j проверять, есть ли путь $i \to k \to j$.

```
M = relmat(R)
for k = 1...n:
  for i = 1...n:
    for j = 1...n:
      M[i, j] = M[i, j] or (M[i, k] and M[k, j])
```

Рефлексивность, иррефлексивность, корефлексивность

- Рефлексивность: $a\ R\ a$
- Иррефлексивность: $a\ \not R\ a$
- Корефлексивность: $(a\ R\ b) \to (a = b)$

Симметричность, асимметричность, антисимметричность

- Симметричность: $(a\ R\ b) \to (b\ R\ a)$
- Асимметричность: $(a\ R\ b) \to (b\ \not R\ a)$
- Антисимметричность: $(a\ R\ b) \to (b\ \not R\ a)$

Свойство транзитивности

$$(a\ R\ b) \land (b\ R\ c) \to (a\ R\ c)$$

Свойства евклидовости (левая/правая)

- Левая: $(y\ R\ x) \land (z\ R\ x) \to (y\ R\ z)$
- Правая: $(x\ R\ y) \land (x\ R\ z) \to (y\ R\ z)$

Свойство связности

- Semi-connex: $(x \neq y) \to ((x\ R\ y) \lor (y\ R\ x))$
- Connex: $((x\ R\ y) \lor (y\ R\ x))$

Отношения эквивалентности

Отношение эквивалентности

Рефлексивность + симметричность + транзитивность

Класс эквивалентности и фактор-множество

Класс эквивалентности для элемента x - множество всех таких элементов y, что $x\ R\ y$

Фактор-множество - множество всех классов эквивалентности. *Является разбиением.*

Сравнимость по модулю n

Пример отношения эквивалентности.

$x\ R_n\ y \Longleftrightarrow a \equiv b \pmod{n} \Longleftrightarrow n \mid (x - y)$

- Рефлексивность: $n \mid (a - a)$
- Симметричность: $n \mid (a - b) \Longleftrightarrow n \mid (b - a)$
- Транзитивность: $n \mid (b - c) + (c - a)$

Отношения порядка

Частичный порядок и строгий частичный порядок

- Частичный: рефлексивность + антисимметричность + транзитивность
- Строгий: иррефлексивность + антисимметричность + транзитивность

Линейный (полный) порядок и строгий линейный порядок

- Полный: частичный + connex
- Строгий: частичный строгий + semi-connex

Частично упорядоченное множество (poset)

$\langle S, \leq \rangle$ - множество с частичным порядком

Частично упорядоченные множества

Диаграмма Хассе

Визуализация посета:

- Снизу вверх
- Связи $x < y$ без промежуточных $x < z < y$ (x покрывает y)
- Без транзитивных связей

$$\boldsymbol{\langle \mathcal{P}(\{a, b\}), \subseteq \rangle :}$$

$$\begin{tikzcd}
 & \{a, b\} & \\
\{a\} \arrow[ur] & & \{b\} \arrow[ul] \\
 & \emptyset \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Отношение покрытия

Элемент y покрывает x, если между ними нет z:

$$x \lessdot y \Longleftrightarrow \nexists z : x < z < y$$

Сравнимые и несравнимые элементы

- Сравнимые элементы посета: между x и y есть отношение $x\ R\ y$ или $y\ R\ x$.

- Несравнимые элементы посета: нет отношений $x \not R\ y$ и $y \not R\ x$

Цепи и антицепи

- Цепь: подмножество $C \subseteq M$, где каждые два элемента сравнимы.
- Антицепь: подмножество $A \subseteq M$, где любые два элемента не сравнимы.

Минимальные и максимальные элементы

- Минимальный элемент - элемент m, для которого нет элемента меньше:

$$\forall x : (x \leq m) \to (x = m)$$

- Максимальный элемент - элемент m, для которого нет элемента меньше:

$$\forall x : (m \leq x) \to (m = x)$$

Наименьший и наибольший элементы

- Наименьший элемент - элемент g:

$$\forall x : g \leq x$$

- Наибольший элемент - элемент g:

$$\forall x : x \leq g$$

  Покрывает все множество, в отличие от максимального элемента.

Верхняя и нижняя грани

Пусть дан посет $\langle S, \leq \rangle$ и подмножество $C \subseteq S$.

- Верхняя грань - такой $u \in S$, что $\forall x \in C : x \leq u$
- Нижняя грань - такой $u \in S$, что $\forall x \in C : u \leq x$

Может быть несколько.

Инфимум и супремум

- Супремум (join) подмножества C - наименьшая верхняя грань C
- Инфимум (meet) подмножества C - наибольшая нижняя грань C

Если существуют, то всегда единственные.

Обратный (дуальный) порядок

- Дуальный посет для $\langle S, \leq \rangle$ - это посет $\langle S, \geq \rangle$, где $x \geq y \Longleftrightarrow y \leq x$

Теорема Дилворта

В каждом конечном посете, максимальная мощность антицепи равна минимальному количеству цепей, которые покроют все множество

Решётки

Решётка (lattice)

- Нижняя полурешетка - посет, где для каждого подмножества есть инфимум
- Верхняя полурушетка - посет, где для каждого подмножества есть супремум
- Решетка - посет, где для каждого подмножества есть инфимум и супремум

Операции объединения (join) и пересечения (meet)

Возьмем $\{a, b\} \subseteq S$.

- Найдем такое m, что оно будет инфимумом для $\{a, b\}$. Назовем такую операцию пересечением (meet):

$$a \wedge b = m$$

- Найдем такое j, что оно будет супремумом для $\{a, b\}$. Назовем такую операцию объединением (join):

$$a \vee b = j$$

Ограниченная решётка

Решетка ограничена, если у нее есть наибольший элемент $\top$ и наименьший элемент $\bot$.

Пример для $\langle \mathbb{N}, | \rangle$*:* $\bot = 1$

Дистрибутивная и модулярная решётки

- Дистрибутивность:
  - $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
  - $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
- Модулярность:
  - $x \vee (y \wedge z) = (x \vee y) \wedge z$

Дистрибутивность $\Rightarrow$ *модулярность, но не наоборот.*

Дополненная решётка

Решетку называем дополненной, если для каждого x существует такой y, что:

$$x \vee y = \top$$
$$x \wedge y = \bot$$

Назовем операцию нахождения y для x дополнением:

$$\neg x = y$$

Булева алгебра

Дополненная дистрибутивная решетка:

$$(B, \wedge, \vee, \neg, \top, \bot)$$

- множество B
- бинарная операции $\wedge, \vee$
- унарная операция $\neg$
- два различных элемента $\top, \bot$

Примеры решёток

- Булева: $\langle \{0, 1\}, \leq \rangle$
  - $(1 \wedge 1 = 1), (\ 0 \wedge 1 = 0), (1 \vee 0 = 1)$, etc.
  - $(\neg 1 = 0), (\neg 0 = 1)$
  - Является булевой алгеброй!
- $\langle \mathbb{N}^+, | \rangle$:

- $a \wedge b = \gcd(a, b)$
- $a \vee b = \operatorname{lcm}(a, b)$
- $\langle \mathcal{P}(S), \subseteq \rangle$:
  - $a \wedge b = a \cap b$
  - $a \vee b = a \cup b$

Фундированные отношения и вполне-упорядоченные множества

Фундированное отношение (well-founded)

Отношение $R \subseteq M^2$ называется фундированным, если у каждого непустого множества есть минимальный элемент:

$$\forall S \subseteq M : (S \neq \emptyset) \to (\exists m \in S : \forall x \in S : x \not R\, m)$$

Вполне-упорядоченное множество (well-order)

Посет $\langle M, \leq \rangle$ называется вполне-упорядоченным, если у каждого непустого множества есть наименьший элемент:

$$\forall S \subseteq M : (S \neq \emptyset) \to (\exists m \in S : \forall x \in S : m \leq x)$$

То есть, well-order = well-founded + total order

Принцип вполне-упорядочения

У каждого непустого подмножества $\mathbb{N}$ есть наименьший элемент.

Индукция по фундированному отношению

Пусть есть фундированное отношение $\langle S, \prec \rangle$ и какое-то свойство $P(x)$. Чтобы доказать, что $\forall x : P(x)$, надо показать:

$$\forall x : (\forall y \prec x : P(y)) \to P(x)$$

Условия убывающих и возрастающих цепей (DCC и ACC)

Посет $\langle S, \leq \rangle$ удовлетворяет условию убывающих цепей (DCC), если не существует бесконечных строго убывающих цепей:

$$x_1 > x_2 > x_3 > \ldots$$

Well-founded удовлетворяет DCC

Пример: $\langle \mathbb{N}^+, \leq \rangle$ удовлевторяет DCC, так как любая убывающая последовательность дойдет максимум до 1.

Посет $\langle S, \leq \rangle$ удовлетворяет условию возрастающих цепей (ACC), если не существует бесконечных строго возрастающих цепей:

$$x_1 < x_2 < x_3 < \ldots$$

Нётерово отношение

Отношение называется нётеревым, если для каждого подмножества есть максимальный элемент.

Или R называется нётеревым, если R^{-1} является well-founded.

Нётерево отношение удовлетворяет ACC

Анализ завершимости (termination analysis)

Надо показать, что переходы рекурсивного алгоритма образуют well-founded отношение. Оттуда последует DCC, а значит алгоритм завершится на каком-то минимальном элементе.

Функции

Функция и частичная функция

Функция $f : A \to B$ – специальное отношение $f \subseteq A \times B$, где каждый элемент из A относится только к одному элементу B.

- Функция удовлетворяет свойству функциональности и всюду-определенности.
- Частичная функция $f : A \hookrightarrow B$ удовлетворяет только свойству функциональности.

Свойство функциональности

Каждый вход имеет не более, чем один выход:

$$\forall a \in A : \forall b_1, b_2 \in B : (f(a) = b_1 \land f(a) = b_2) \to (b_1 = b_2)$$

Свойство всюду-определённости

Каждый вход имеет не менее, чем один выход:

$$\forall a \in A : \exists b \in B : f(a) = b$$

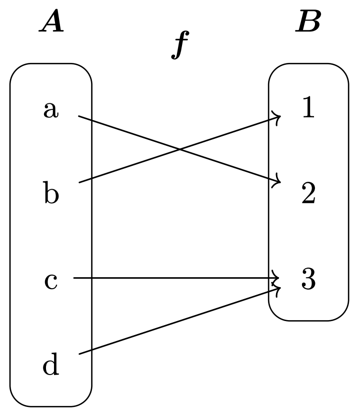
Область определения, область значений и образ функции

Граф функции

Двудольный граф $A \longrightarrow B$. Каждый $a \in A$ имеет ровно одно ребро в какое-то $b \in B$.

Пример:

$$f : \{a, b, c, d\} \longrightarrow \{1, 2, 3\}$$
$$a \mapsto 2 \quad b \mapsto 1 \quad c \mapsto 3 \quad d \mapsto 3$$



Образ и прообраз множества

Возьмем $f : A \to B$ и $S \subseteq A$. Образ S по f - множество всех элементов S, отображенных через f:

$$f(S) = \{f(s) \mid s \in S\}$$

Возьмем $f : A \to B$ и $T \subseteq B$. Прообраз $T \subseteq B$ по f - множество всех исходных элементов, которые отобразились в T:

$$f^{-1}(T) = \{a \in A \mid f(a) \in T\}$$

f^{-1} здесь не обозначает обратную функцию, а просто множество-прообраз от образа T

Пример: пусть $f(x) = x^2$. Прообраз $\{9, 16\} = \{3, 4, -3, -4\}$

Инъекция, сюръекция и биекция

- Инъекция - функция, у которой различные элементы из домена отображаются в различные элементы кодомена:

  $$\forall a_1, a_2 \in A : (f(a_1) = f(a_2)) \to (a_1 = a_2)$$

  Каждая вершина доли B имеет не более одного входящего ребра

- Сюръекция - функция, у которой каждый элемент кодомена является образом хотя бы одного элемента из домена:

  $$\forall b \in B : \exists a \in A : f(a) = b$$

  Каждая вершина доли B имеет не менее одного входящего ребра

- Биекция - сюръекция + инъекция

  Эквивалентно: биекция - функция, у которой есть обратная $f^{-1} : B \to A$

  Каждая вершина доли B имеет ровно одно ребро. Образуется однозначное соответствие между элементами A и B

Композиция функций и её степени

Пусть $f : A \to B$, $g : B \to C$. Тогда:

$$(g \circ f) : A \to C$$
$$(g \circ f)(x) = g(f(x))$$

Степень функции $f : A \to A$:

$$f^0 = \mathrm{id}_A$$
$$f^{n+1} = f^n \circ f$$

Тождественная и обратная функции

- Тождественная: $\mathrm{id}_A : A \to A \qquad f(a) = a$
- Обратная: $f^{-1} \qquad f^{-1}(b) = a \Longleftrightarrow f(a) = b$

$f \circ f^-1 = \mathrm{id}_A$

f^{-1} существует тогда и только тогда, когда f биективная.

Характеристическая (индикаторная) функция

$$\chi_S(s) = \begin{cases} 1 & s \in S \\ 0 & s \notin S \end{cases}$$

Монотонная функция

Функция называется монотонной, если оно сохраняет отношение порядка.

Пример: пусть дан посет $\langle S, \leq \rangle$ *и функция* $f : S \to S$*, тогда:*

$$x \leq y \ \to \ f(x) \leq f(y)$$

Мощность и счётность множеств

Равномощные множества

$|A| = |B|$, если существует биекция $A \to B$

Кардинальные числа

Кардинальность - мера «размера» множества. $|X|$ - кардинальное число.

- Для конечных - количество элементов в множестве: $|X| \in \mathbb{N}$
- Для счетных: $|X| = |\mathbb{N}| = \aleph_0$
- Для несчетных: $|X| = |\mathbb{R}| = 2^{|\mathbb{N}|} = \mathfrak{c}$
- Из теоремы Кантора ($|X| < |\mathcal{P}(X)|$): $\beth_0 = \aleph_0, \beth_{n+1} = 2^{\beth_n}$

Дедекиндово-бесконечные множества

Множество X является дедекиндово-бесконечным, если строгое подмножество $Y \subset X$ равномощен X, то есть существует биекция $X \longrightarrow Y$.

Эквивалентно: X дедекиндово-бесконечное, если существует инъективная, но не сюръективная функция $f : X \to X$

Парадокс отеля Гильберта

Пусть есть отель с бесконечным множеством комнат: 1, 2, 3… и все комнаты заселены.

Можно ли заселить еще одного человека? Можно. Отправим n-го гостя в (n+1)-ую комнату, а нового поместим в 1-ую. Получаем биекцию $f : n \mapsto n + 1$

Можно ли заселить еще бесконечно много человек? Можно. Отправим n-го гостя в (2n)-ую комнату, а каждого m-го новоприбывшего отправим в (2n-1)-ую комнату. Получаем биекцию $f : n \mapsto 2n$

То есть, $|\mathbb{N}| = |\mathbb{N}_{\text{четные}}| = |\mathbb{N}_{\text{нечетные}}| = \aleph_0$.

Счётно-бесконечные и несчётно-бесконечные множества

Счетно-бесконечное: если существует биекция с $\mathbb{N}$. Размер счетно-бесконечного равен $|\mathbb{N}| = \aleph_0$

Несчетно-бесконечное: если нет биекции с $\mathbb{N}$. Размер несчетно-бесконечного: $|\mathbb{R}| = \mathfrak{c}$

Диагональный аргумент Кантора

Идея в том, чтобы попытаться построить список элементов, а потом сделать такой элемент, который будет отличаться от всех, и таким образом показать несчетность.

Пример. Покажем, что множество всех бесконечных бинарных строк несчетно.

Пусть множество счетно. Тогда пронумеруем все строки:

$$\begin{bmatrix} \boldsymbol{b_{11}} & b_{12} & b_{13} & \dots \\ b_{21} & \boldsymbol{b_{22}} & b_{23} & \dots \\ b_{31} & b_{32} & \boldsymbol{b_{33}} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

Где b_{ij} - j-ый бит i-ой строки.

А теперь возьмем и сделаем такую строку:

$$\Delta = \left(\overline{b_{11}}, \overline{b_{22}}, \overline{b_{33}}, \dots\right)$$

Она отличается от i-ой строки в i-ым битом, а значит не находится в списке. Противоречие.

Континуум-гипотеза

Не существует кардинальности строго между $\aleph_0$ и $\mathfrak{c}$. Тогда $\mathfrak{c} = \aleph_1$.

1. Доказано, что гипотеза непротиворечива ZFC
2. Доказано, что обратная гипотеза тоже непротиворечива ZFC