# Теория множеств
# Введение

Математическая логика и теория алгоритмов

Алексей Романов

18 ноября 2023 г.

МИЭТ

## Понятие множества

- Множество — это набор (или совокупность) элементов, который рассматривается как единый объект.
- «$a$ — элемент $A$» записывается как $a \in A$.
- $A$ — подмножество $B$ ($A \subseteq B$), если

# Понятие множества

- Множество — это набор (или совокупность) элементов, который рассматривается как единый объект.
- «$a$ — элемент $A$» записывается как $a \in A$.
- $A$ — подмножество $B$ ($A \subseteq B$), если $\forall x\ (x \in A \to x \in B)$.
- $A = B$, если

# Понятие множества

- Множество — это набор (или совокупность) элементов, который рассматривается как единый объект.
- «$a$ — элемент $A$» записывается как $a \in A$.
- $A$ — подмножество $B$ ($A \subseteq B$), если $\forall x\ (x \in A \to x \in B)$.
- $A = B$, если $\forall x\ (x \in A \leftrightarrow x \in B)$ (или $A \subseteq B \land B \subseteq A$).
- Элементом множества может быть другое множество.
- Не обязательно все элементы множества имеют один «тип», т.е. все они числа, или множества, или отрезки…
- Очень часто говорят о множествах с какой-то дополнительной структурой.

# Задание множеств

- Стандартный способ задать множество это указать какое-то условие, которое выполняется для всех его элементов и не выполняется для не-элементов. Обозначается $\{x \mid A(x)\}$. Тогда $\forall x\ (x \in \{x \mid A(x)\} \leftrightarrow$

# Задание множеств

- Стандартный способ задать множество это указать какое-то условие, которое выполняется для всех его элементов и не выполняется для не-элементов. Обозначается $\{x \mid A(x)\}$. Тогда $\forall x\ (x \in \{x \mid A(x)\} \leftrightarrow A(x))$.
- $x$ в $\{x \mid \ldots\}$ — связанная переменная.
- Задание перечислением:
  $\{a_1, \ldots, a_n\} = \{x \mid$

# Задание множеств

- Стандартный способ задать множество это указать какое-то условие, которое выполняется для всех его элементов и не выполняется для не-элементов. Обозначается $\{x \mid A(x)\}$. Тогда $\forall x\ (x \in \{x \mid A(x)\} \leftrightarrow A(x))$.
- $x$ в $\{x \mid \ldots\}$ — связанная переменная.
- Задание перечислением: $\{a_1, \ldots, a_n\} = \{x \mid x = a_1 \vee \ldots \vee x = a_n\}$.
- Пустое множество: $\varnothing = \{x \mid$

# Задание множеств

- Стандартный способ задать множество это указать какое-то условие, которое выполняется для всех его элементов и не выполняется для не-элементов. Обозначается $\{x \mid A(x)\}$. Тогда $\forall x\ (x \in \{x \mid A(x)\} \leftrightarrow A(x))$.
- $x$ в $\{x \mid \ldots\}$ — связанная переменная.
- Задание перечислением: $\{a_1, \ldots, a_n\} = \{x \mid x = a_1 \vee \ldots \vee x = a_n\}$.
- Пустое множество: $\varnothing = \{x \mid x \neq x\}$.
- Часто значения $x$ берутся из какого-то множества $X$: $\{x : X \mid A(x)\} = \{x \mid x \in X \wedge A(x)\}$ (или $\{x \in X \mid A(x)\}$).
- Слева может быть не переменная, а выражение: $\{f(x) \mid x : X\}$.
- $:$ вместо $\in$ позволяет отличить $\{x : \mathbb{N} \mid x \in \mathbb{R}\}$ от $\{x \in \mathbb{N} \mid x : \mathbb{R}\}$.
- Одно множество может быть задано несколькими разными свойствами

# Задание множеств

- Стандартный способ задать множество это указать какое-то условие, которое выполняется для всех его элементов и не выполняется для не-элементов. Обозначается $\{x \mid A(x)\}$. Тогда $\forall x\, (x \in \{x \mid A(x)\} \leftrightarrow A(x))$.
- $x$ в $\{x \mid \ldots\}$ — связанная переменная.
- Задание перечислением: $\{a_1, \ldots, a_n\} = \{x \mid x = a_1 \vee \ldots \vee x = a_n\}$.
- Пустое множество: $\varnothing = \{x \mid x \neq x\}$.
- Часто значения $x$ берутся из какого-то множества $X$: $\{x : X \mid A(x)\} = \{x \mid x \in X \wedge A(x)\}$ (или $\{x \in X \mid A(x)\}$).
- Слева может быть не переменная, а выражение: $\{f(x) \mid x : X\}$.
- $:$ вместо $\in$ позволяет отличить $\{x : \mathbb{N} \mid x \in \mathbb{R}\}$ от $\{x \in \mathbb{N} \mid x : \mathbb{R}\}$.
- Одно множество может быть задано несколькими разными свойствами, если они эквивалентны.

# Операции над множествами

- Объединение: $A \cup B = \{x \mid$

# Операции над множествами

- Объединение: $A \cup B = \{x \mid x \in A \vee x \in B\}$
- Пересечение: $A \cap B = \{x \mid$

# Операции над множествами

- Объединение: $A \cup B = \{x \mid x \in A \vee x \in B\}$
- Пересечение: $A \cap B = \{x \mid x \in A \wedge x \in B\} = \{x : A \mid x \in B\}$
- Множество всех подмножеств: $\mathcal{P}(A) = \{B \mid B \subseteq A\}$ (также обозначается $2^A$).

## Наивная теория множеств и парадокс Рассела

- Для любого ли свойства есть множество всех объектов, обладающих этим свойством?
- *Наивная теория множеств* считала, что да.
- Тогда рассмотрим множество всех множеств, не являющихся элементами самих себя: $R = \{X \mid X \notin X\}$.
- Вопрос: является ли $R$ элементом самого себя?

# Наивная теория множеств и парадокс Рассела

- Для любого ли свойства есть множество всех объектов, обладающих этим свойством?
- *Наивная теория множеств* считала, что да.
- Тогда рассмотрим множество всех множеств, не являющихся элементами самих себя: $R = \{X \mid X \notin X\}$.
- Вопрос: является ли $R$ элементом самого себя?
- $R \in R \leftrightarrow R \in \{X \mid X \notin X\} \leftrightarrow$

# Наивная теория множеств и парадокс Рассела

- Для любого ли свойства есть множество всех объектов, обладающих этим свойством?
- *Наивная теория множеств* считала, что да.
- Тогда рассмотрим множество всех множеств, не являющихся элементами самих себя: $R = \{X \mid X \notin X\}$.
- Вопрос: является ли $R$ элементом самого себя?
- $R \in R \leftrightarrow R \in \{X \mid X \notin X\} \leftrightarrow R \notin R$.
- Пришли к противоречию!

# Наивная теория множеств и парадокс Рассела

- Для любого ли свойства есть множество всех объектов, обладающих этим свойством?
- *Наивная теория множеств* считала, что да.
- Тогда рассмотрим множество всех множеств, не являющихся элементами самих себя: $R = \{X \mid X \notin X\}$.
- Вопрос: является ли $R$ элементом самого себя?
- $R \in R \leftrightarrow R \in \{X \mid X \notin X\} \leftrightarrow R \notin R$.
- Пришли к противоречию!
- Надо как-то ограничить то, какие свойства задают множества.
- Это делается заданием некоторого набора аксиом, позволяющих строить множества постепенно, исходя из уже построенных.
- Конкретных *аксиоматических теорий множеств* довольно много, самая стандартная *теория Цермело-Френкеля* (*ZFC* или *ZF*).

## Упорядоченные пары и кортежи

- *Упорядоченная пара* это способ по любым двум объектам $a$ и $b$ построить такой $(a, b)$, что

# Упорядоченные пары и кортежи

- *Упорядоченная пара* это способ по любым двум объектам $a$ и $b$ построить такой $(a, b)$, что

$$(a, b) = (c, d) \leftrightarrow a = c \land b = d$$

- Это понятие обобщается на упорядоченные тройки, четвёрки и т.д. Общее название — *кортеж*.
- Если есть пары, то можно задать и тройки: $(a_1, a_2, a_3) =$

## Упорядоченные пары и кортежи

- *Упорядоченная пара* это способ по любым двум объектам $a$ и $b$ построить такой $(a, b)$, что

$$(a, b) = (c, d) \leftrightarrow a = c \wedge b = d$$

- Это понятие обобщается на упорядоченные тройки, четвёрки и т.д. Общее название — *кортеж*.
- Если есть пары, то можно задать и тройки: $(a_1, a_2, a_3) = (a_1, (a_2, a_3))$ и так далее.
- Можно определить пары как множества. Например, определение Куратовского:

$$(a, b) = \{\{a\}, \{a, b\}\}$$

- Упражнение: доказать основное свойство пар для этого определения.
- Декартово произведение:

$$A_1 \times \ldots \times A_n =$$

# Упорядоченные пары и кортежи

- *Упорядоченная пара* это способ по любым двум объектам $a$ и $b$ построить такой $(a, b)$, что

$$(a, b) = (c, d) \leftrightarrow a = c \land b = d$$

- Это понятие обобщается на упорядоченные тройки, четвёрки и т.д. Общее название — *кортеж*.
- Если есть пары, то можно задать и тройки: $(a_1, a_2, a_3) = (a_1, (a_2, a_3))$ и так далее.
- Можно определить пары как множества. Например, определение Куратовского:

$$(a, b) = \{\{a\}, \{a, b\}\}$$

- Упражнение: доказать основное свойство пар для этого определения.
- Декартово произведение:

$$A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid a_1 : A_1, \ldots, a_n : A_n\}$$

# Функции

- *Функция* (или *отображение*) из множества $A$ в множество $B$ сопоставляет каждому элементу $A$ ровно один элемент из $B$:

$$\forall x : A \; \exists! y : B \; y = f(x)$$

# Функции

- *Функция* (или *отображение*) из множества $A$ в множество $B$ сопоставляет каждому элементу $A$ ровно один элемент из $B$:

$$\forall x : A\ \exists! y : B\ y = f(x)$$

- Если значение функции $f$ на аргументе $x$ задаётся выражением $expr$, пишем $f(x) = expr$ или $f = x \mapsto expr$.
- *Лямбда-выражение* $x \mapsto expr$ удобно использовать как часть более сложных выражений.

# Функции

- *Функция* (или *отображение*) из множества $A$ в множество $B$ сопоставляет каждому элементу $A$ ровно один элемент из $B$:

$$\forall x : A\ \exists! y : B\ y = f(x)$$

- Если значение функции $f$ на аргументе $x$ задаётся выражением $expr$, пишем $f(x) = expr$ или $f = x \mapsto expr$.
- *Лямбда-выражение* $x \mapsto expr$ удобно использовать как часть более сложных выражений.
- *График функции* это множество пар $\{(x, f(x)) \mid x : A\}$. В теории множеств функцию отождествляют с её графиком (или с тройкой $(A, B, \text{график})$).
- Можно ли определить $A$ и $B$ по графику?

# Функции

- *Функция* (или *отображение*) из множества $A$ в множество $B$ сопоставляет каждому элементу $A$ ровно один элемент из $B$:

$$\forall x : A\ \exists! y : B\ y = f(x)$$

- Если значение функции $f$ на аргументе $x$ задаётся выражением *expr*, пишем $f(x) = expr$ или $f = x \mapsto expr$.
- *Лямбда-выражение* $x \mapsto expr$ удобно использовать как часть более сложных выражений.
- *График функции* это множество пар $\{(x, f(x)) \mid x : A\}$. В теории множеств функцию отождествляют с её графиком (или с тройкой $(A, B, \text{график})$).
- Можно ли определить $A$ и $B$ по графику? $A$ да, $B$ нет.

# Функции

- *Функция* (или *отображение*) из множества $A$ в множество $B$ сопоставляет каждому элементу $A$ ровно один элемент из $B$:

$$\forall x : A\ \exists! y : B\ y = f(x)$$

- Если значение функции $f$ на аргументе $x$ задаётся выражением $expr$, пишем $f(x) = expr$ или $f = x \mapsto expr$.
- *Лямбда-выражение* $x \mapsto expr$ удобно использовать как часть более сложных выражений.
- *График функции* это множество пар $\{(x, f(x)) \mid x : A\}$. В теории множеств функцию отождествляют с её графиком (или с тройкой $(A, B, \text{график})$).
- Можно ли определить $A$ и $B$ по графику? $A$ да, $B$ нет. Множество всех функций из $A$ в $B$ обозначается $A \to B$ или $B^A$. Формально:

$$A \to B = \{F \mid F \subseteq A \times B,\ \forall x : A\ \exists! y : B\ (x, y) \in F\}$$

# Образы, прообразы

- Если $f(x) = y$, также говорят, что $y$ — *образ* $x$, а $x$ — *прообраз* $y$ (возможно, один из прообразов). Это продолжается на подмножества областей определения и значений:
- Если $C \subseteq A$, то *образ* $C$ это $f[C] =$

# Образы, прообразы

- Если $f(x) = y$, также говорят, что $y$ — *образ* $x$, а $x$ — *прообраз* $y$ (возможно, один из прообразов). Это продолжается на подмножества областей определения и значений:
- Если $C \subseteq A$, то *образ* $C$ это $f[C] = \{f(x) \mid x : C\}$.

# Образы, прообразы

- Если $f(x) = y$, также говорят, что $y$ — *образ* $x$, а $x$ — *прообраз* $y$ (возможно, один из прообразов). Это продолжается на подмножества областей определения и значений:
- Если $C \subseteq A$, то *образ* $C$ это $f[C] = \{f(x) \mid x : C\}$.
- Если $C \subseteq B$, то *прообраз* $C$ это $f^{-1}[C] =$

# Образы, прообразы

- Если $f(x) = y$, также говорят, что $y$ — *образ* $x$, а $x$ — *прообраз* $y$ (возможно, один из прообразов). Это продолжается на подмножества областей определения и значений:
- Если $C \subseteq A$, то *образ* $C$ это $f[C] = \{f(x) \mid x : C\}$.
- Если $C \subseteq B$, то *прообраз* $C$ это $f^{-1}[C] = \{x : A \mid f(x) \in C\}$.
- Часто пишут круглые скобки вместо квадратных, но как раз в теории множеств вполне бывает, что $C \subseteq A$ и $C \in A$ одновременно.

# Вложения, наложения и биекции

- Функция $f : A \to B$ называется *вложением* или *инъекцией*, если $\forall x, y : A\ x \neq y \to f(x) \neq f(y)$. То есть каждое значение в $B$ имеет не более одного прообраза. Заметьте, что это не зависит от $B$.
- $f : A \to B$ называется *наложением* или *сюръекцией*, если $\forall y : B\ \exists x : A\ y = f(x)$. То есть каждое значение в $B$ имеет хотя бы один прообраз. Эквивалентно, $f[A] = B$.
- $f : A \to B$ называется *взаимно однозначной* или *биекцией*, если она одновременно вложение $A$ в $B$ и наложение $A$ на $B$: $\forall y : B\ \exists! x : A\ y = f(x)$. Соответственно, каждое значение в $B$ имеет ровно один прообраз.

# Мощность множеств

- Вы уже знакомы с понятием мощности конечных множеств: $|A|$ — количество элементов в $A$.
- Пусть $A$ и $B$ конечны. В каком случае существует вложение $A$ в $B$ (обозначаем $A \lesssim B$ и говорим *$A$ вкладывается в $B$*)?

# Мощность множеств

- Вы уже знакомы с понятием мощности конечных множеств: $|A|$ — количество элементов в $A$.
- Пусть $A$ и $B$ конечны. В каком случае существует вложение $A$ в $B$ (обозначаем $A \lesssim B$ и говорим $A$ *вкладывается в* $B$)? Когда $|A| \leq |B|$.

# Мощность множеств

- Вы уже знакомы с понятием мощности конечных множеств: $|A|$ — количество элементов в $A$.
- Пусть $A$ и $B$ конечны. В каком случае существует вложение $A$ в $B$ (обозначаем $A \lesssim B$ и говорим $A$ *вкладывается в* $B$)? Когда $|A| \leq |B|$.
- А наложение (обозначим $A \gtrsim B$)? Биекция ($A \sim B$)?

# Мощность множеств

- Вы уже знакомы с понятием мощности конечных множеств: $|A|$ — количество элементов в $A$.
- Пусть $A$ и $B$ конечны. В каком случае существует вложение $A$ в $B$ (обозначаем $A \lesssim B$ и говорим *$A$ вкладывается в $B$*)? Когда $|A| \leq |B|$.
- А наложение (обозначим $A \gtrsim B$)? Биекция ($A \sim B$)? Когда $|A| \geq |B|$ и

# Мощность множеств

- Вы уже знакомы с понятием мощности конечных множеств: $|A|$ — количество элементов в $A$.
- Пусть $A$ и $B$ конечны. В каком случае существует вложение $A$ в $B$ (обозначаем $A \lesssim B$ и говорим $A$ *вкладывается в $B$*)? Когда $|A| \le |B|$.
- А наложение (обозначим $A \gtrsim B$)? Биекция ($A \sim B$)? Когда $|A| \ge |B|$ и когда $|A| = |B|$ соответственно.

# Мощность множеств

- Вы уже знакомы с понятием мощности конечных множеств: $|A|$ — количество элементов в $A$.
- Пусть $A$ и $B$ конечны. В каком случае существует вложение $A$ в $B$ (обозначаем $A \lesssim B$ и говорим $A$ *вкладывается в* $B$)? Когда $|A| \leq |B|$.
- А наложение (обозначим $A \gtrsim B$)? Биекция ($A \sim B$)? Когда $|A| \geq |B|$ и когда $|A| = |B|$ соответственно.
- В логике это берётся как определение мощности.
- То есть пока что мощности (кроме натуральных чисел) это какие-то абстрактные объекты, которые можно только сравнивать.
- Позже мы увидим, как мощности представить как множества.

# Свойства отношений мощности

- Верно ли, что $\lesssim$ рефлексивно, то есть

## Свойства отношений мощности

- Верно ли, что $\lesssim$ рефлексивно, то есть $\forall A \; A \lesssim A$?

## Свойства отношений мощности

- Верно ли, что $\lesssim$ рефлексивно, то есть $\forall A\ A \lesssim A$? Да. $id_A = x \mapsto x$ будет вложением $A$ в $A$.
- Транзитивно ли? Пусть $f : A \to B$ и $g : B \to C$ вложения. Можно ли найти вложение $A \to C$?

## Свойства отношений мощности

- Верно ли, что $\lesssim$ рефлексивно, то есть $\forall A\ A \lesssim A$? Да. $id_A = x \mapsto x$ будет вложением $A$ в $A$.
- Транзитивно ли? Пусть $f : A \to B$ и $g : B \to C$ вложения. Можно ли найти вложение $A \to C$? Да, это композиция $g \circ f = x \mapsto$

## Свойства отношений мощности

- Верно ли, что $\lesssim$ рефлексивно, то есть $\forall A\ A \lesssim A$? Да. $id_A = x \mapsto x$ будет вложением $A$ в $A$.
- Транзитивно ли? Пусть $f : A \to B$ и $g : B \to C$ вложения. Можно ли найти вложение $A \to C$? Да, это композиция $g \circ f = x \mapsto g(f(x))$. Конечно, нужно ещё доказать, что это вложение.
- Симметрично ли?

# Свойства отношений мощности

- Верно ли, что $\lesssim$ рефлексивно, то есть $\forall A\ A \lesssim A$? Да. $id_A = x \mapsto x$ будет вложением $A$ в $A$.
- Транзитивно ли? Пусть $f : A \to B$ и $g : B \to C$ вложения. Можно ли найти вложение $A \to C$? Да, это композиция $g \circ f = x \mapsto g(f(x))$. Конечно, нужно ещё доказать, что это вложение.
- Симметрично ли? Нет!
- Антисимметрично ли?

# Свойства отношений мощности

- Верно ли, что $\lesssim$ рефлексивно, то есть $\forall A\ A \lesssim A$? Да. $id_A = x \mapsto x$ будет вложением $A$ в $A$.
- Транзитивно ли? Пусть $f : A \to B$ и $g : B \to C$ вложения. Можно ли найти вложение $A \to C$? Да, это композиция $g \circ f = x \mapsto g(f(x))$. Конечно, нужно ещё доказать, что это вложение.
- Симметрично ли? Нет!
- Антисимметрично ли? Тоже нет! Может быть $A \lesssim B \wedge B \lesssim A \wedge A \neq B$. Когда (хотя бы для конечных множеств)?

# Свойства отношений мощности

- Верно ли, что $\lesssim$ рефлексивно, то есть $\forall A\ A \lesssim A$? Да. $id_A = x \mapsto x$ будет вложением $A$ в $A$.
- Транзитивно ли? Пусть $f : A \to B$ и $g : B \to C$ вложения. Можно ли найти вложение $A \to C$? Да, это композиция $g \circ f = x \mapsto g(f(x))$. Конечно, нужно ещё доказать, что это вложение.
- Симметрично ли? Нет!
- Антисимметрично ли? Тоже нет! Может быть $A \lesssim B \wedge B \lesssim A \wedge A \neq B$. Когда (хотя бы для конечных множеств)? Если $|A| = |B|$.
- Окажется, что не только для конечных: $A \lesssim B \wedge B \lesssim A \Rightarrow A \sim B$. Это нетривиальная теорема Кантора-Бернштейна, сейчас без доказательства.
- Тоже нетривиально, но можно доказать: $A \lesssim B \Leftrightarrow B \gtrsim A$ и $A \lesssim B \vee B \lesssim A$.

## Свойства отношений мощности

- А как насчёт $\sim$? Оно тоже рефлексивно: $id_A$ не только вложение, но и

# Свойства отношений мощности

- А как насчёт $\sim$? Оно тоже рефлексивно: $id_A$ не только вложение, но и биекция.

# Свойства отношений мощности

- А как насчёт $\sim$? Оно тоже рефлексивно: $id_A$ не только вложение, но и биекция.
- Транзитивно, потому что

## Свойства отношений мощности

- А как насчёт $\sim$? Оно тоже рефлексивно: $id_A$ не только вложение, но и биекция.
- Транзитивно, потому что композиция биекций окажется биекцией.

## Свойства отношений мощности

- А как насчёт $\sim$? Оно тоже рефлексивно: $id_A$ не только вложение, но и биекция.
- Транзитивно, потому что композиция биекций окажется биекцией.
- И симметрично: у любой биекции есть

# Свойства отношений мощности

- А как насчёт $\sim$? Оно тоже рефлексивно: $id_A$ не только вложение, но и биекция.
- Транзитивно, потому что композиция биекций окажется биекцией.
- И симметрично: у любой биекции есть обратная функция, которая тоже окажется биекцией.

## Свойства отношений мощности

- А как насчёт $\sim$? Оно тоже рефлексивно: $id_A$ не только вложение, но и биекция.
- Транзитивно, потому что композиция биекций окажется биекцией.
- И симметрично: у любой биекции есть обратная функция, которая тоже окажется биекцией.
- То есть это отношение

# Свойства отношений мощности

- А как насчёт $\sim$? Оно тоже рефлексивно: $id_A$ не только вложение, но и биекция.
- Транзитивно, потому что композиция биекций окажется биекцией.
- И симметрично: у любой биекции есть обратная функция, которая тоже окажется биекцией.
- То есть это отношение эквивалентности.
- А $\lesssim$ — отношение порядка «с точностью до $\sim$».

# Свойства отношений мощности

- А как насчёт $\sim$? Оно тоже рефлексивно: $id_A$ не только вложение, но и биекция.
- Транзитивно, потому что композиция биекций окажется биекцией.
- И симметрично: у любой биекции есть обратная функция, которая тоже окажется биекцией.
- То есть это отношение эквивалентности.
- А $\lesssim$ — отношение порядка «с точностью до $\sim$».
- Мы можем сказать, что $|A|$ это класс эквивалентности $A$ по отношению $\sim$.
- В силу этих свойств $=$ и $\leq$ на мощностях ведут себя как обычно.

# Конечные множества

- Множество $A$ называется *конечным*, если $\exists n \in \mathbb{N}\ A \sim \{0, \ldots, n-1\}$.
- Соответственно, любое другое множество *бесконечно*.
- Это не единственный способ определить конечные и бесконечные подмножества.

# Счётные множества

- Множество $A$ называется *счётным*, если $A \sim \mathbb{N}$.
- Другими словами, все элементы счётного множества можно перенумеровать.
- $|\mathbb{N}|$ имеет своё обозначение: $\aleph_0$ (читается *алеф-ноль* или *нуль*).
- Другие счётные множества (докажем на доске): множество чётных чисел, $\mathbb{Z}, \mathbb{N} \times \mathbb{N}$.

# Счётные множества

- Множество $A$ называется *счётным*, если $A \sim \mathbb{N}$.
- Другими словами, все элементы счётного множества можно перенумеровать.
- $|\mathbb{N}|$ имеет своё обозначение: $\aleph_0$ (читается *алеф-ноль* или *нуль*).
- Другие счётные множества (докажем на доске): множество чётных чисел, $\mathbb{Z}, \mathbb{N} \times \mathbb{N}$.
- То есть хотя интуитивно множество целых чисел должно быть больше, чем натуральных, в этом смысле их «одинаковое количество».

# Счётные множества

- Множество $A$ называется *счётным*, если $A \sim \mathbb{N}$.
- Другими словами, все элементы счётного множества можно перенумеровать.
- $|\mathbb{N}|$ имеет своё обозначение: $\aleph_0$ (читается *алеф-ноль* или *нуль*).
- Другие счётные множества (докажем на доске): множество чётных чисел, $\mathbb{Z}, \mathbb{N} \times \mathbb{N}$.
- То есть хотя интуитивно множество целых чисел должно быть больше, чем натуральных, в этом смысле их «одинаковое количество».
- $\aleph_0$ это минимальная бесконечная мощность, то есть любое бесконечное подмножество счётного множества счётно (или вложимое в счётное множество).

# Счётные множества

- Множество $A$ называется *счётным*, если $A \sim \mathbb{N}$.
- Другими словами, все элементы счётного множества можно перенумеровать.
- $|\mathbb{N}|$ имеет своё обозначение: $\aleph_0$ (читается *алеф-ноль* или *нуль*).
- Другие счётные множества (докажем на доске): множество чётных чисел, $\mathbb{Z}, \mathbb{N} \times \mathbb{N}$.
- То есть хотя интуитивно множество целых чисел должно быть больше, чем натуральных, в этом смысле их «одинаковое количество».
- $\aleph_0$ это минимальная бесконечная мощность, то есть любое бесконечное подмножество счётного множества счётно (или вложимое в счётное множество).
- Всякое бесконечное множество содержит счётное подмножество.

## Теорема Кантора

- А есть ли какие-то бесконечные мощности, кроме $\aleph_0$?

## Теорема Кантора

- А есть ли какие-то бесконечные мощности, кроме $\aleph_0$?
- Окажется, что для любого $A$ $|A \to \{0,1\}| > |A|$, т.е. $(A \lesssim A \to \{0,1\}) \land (A \nsim A \to \{0,1\})$.
- Это называется теоремой Кантора.

# Теорема Кантора

- А есть ли какие-то бесконечные мощности, кроме $\aleph_0$?
- Окажется, что для любого $A$ $|A \to \{0,1\}| > |A|$, т.е. $(A \lesssim A \to \{0,1\}) \wedge (A \nsim A \to \{0,1\})$.
- Это называется теоремой Кантора.
- В том числе $|\mathbb{N} \to \{0,1\}| > |\mathbb{N}|$. То есть множество всех функций из натуральных чисел в $\{0,1\}$ несчётно.
- Удобнее сначала увидеть доказательство этого частного случая, а потом общего.

# Теорема Кантора

- А есть ли какие-то бесконечные мощности, кроме $\aleph_0$?
- Окажется, что для любого $A$ $|A \to \{0,1\}| > |A|$, т.е. $(A \lesssim A \to \{0,1\}) \land (A \nsim A \to \{0,1\})$.
- Это называется теоремой Кантора.
- В том числе $|\mathbb{N} \to \{0,1\}| > |\mathbb{N}|$. То есть множество всех функций из натуральных чисел в $\{0,1\}$ несчётно.
- Удобнее сначала увидеть доказательство этого частного случая, а потом общего.
- 1. $A \lesssim A \to \{0,1\}$. Как построить такое вложение?
- 2. Предположим, что $f : A \to (A \to \{0,1\})$ наложение. Тогда определим $g : A \to \{0,1\}$ так: $g(x) = 1 - f(x)(x)$.
- Поскольку дано, что $f$ наложение, то $\exists y \in A\ g = f(y)$. Но тогда

# Теорема Кантора

- А есть ли какие-то бесконечные мощности, кроме $\aleph_0$?
- Окажется, что для любого $A$ $|A \to \{0,1\}| > |A|$, т.е. $(A \lesssim A \to \{0,1\}) \wedge (A \nsim A \to \{0,1\})$.
- Это называется теоремой Кантора.
- В том числе $|\mathbb{N} \to \{0,1\}| > |\mathbb{N}|$. То есть множество всех функций из натуральных чисел в $\{0,1\}$ несчётно.
- Удобнее сначала увидеть доказательство этого частного случая, а потом общего.
- 1. $A \lesssim A \to \{0,1\}$. Как построить такое вложение?
- 2. Предположим, что $f : A \to (A \to \{0,1\})$ наложение. Тогда определим $g : A \to \{0,1\}$ так: $g(x) = 1 - f(x)(x)$.
- Поскольку дано, что $f$ наложение, то $\exists y \in A\ g = f(y)$. Но тогда $g(y) = 1 - f(y)(y) \neq f(y)(y) = g(y)$. Противоречие!

# Парадокс Кантора

- Из теоремы Кантора можно заключить, что не существует множества всех множеств. Почему?

## Парадокс Кантора

- Из теоремы Кантора можно заключить, что не существует множества всех множеств. Почему?
- Допустим, что оно существует, и обозначим его $U$.
- Можно показать, что $\mathcal{P}(A) \sim A \to \{0, 1\}$, поэтому $|\mathcal{P}(A)| > |A|$ для любого множества.
- В том числе $|\mathcal{P}(U)| > |U|$. Но элементы $|\mathcal{P}(U)|$ — множества, поэтому

# Парадокс Кантора

- Из теоремы Кантора можно заключить, что не существует множества всех множеств. Почему?
- Допустим, что оно существует, и обозначим его $U$.
- Можно показать, что $\mathcal{P}(A) \sim A \to \{0, 1\}$, поэтому $|\mathcal{P}(A)| > |A|$ для любого множества.
- В том числе $|\mathcal{P}(U)| > |U|$. Но элементы $|\mathcal{P}(U)|$ — множества, поэтому $\mathcal{P}(U) \subseteq U$ и

## Парадокс Кантора

- Из теоремы Кантора можно заключить, что не существует множества всех множеств. Почему?
- Допустим, что оно существует, и обозначим его $U$.
- Можно показать, что $\mathcal{P}(A) \sim A \to \{0, 1\}$, поэтому $|\mathcal{P}(A)| > |A|$ для любого множества.
- В том числе $|\mathcal{P}(U)| > |U|$. Но элементы $|\mathcal{P}(U)|$ — множества, поэтому $\mathcal{P}(U) \subseteq U$ и $|\mathcal{P}(U)| \leq |U|$.
- Пришли к противоречию!

# Парадокс Кантора

- Из теоремы Кантора можно заключить, что не существует множества всех множеств. Почему?
- Допустим, что оно существует, и обозначим его $U$.
- Можно показать, что $\mathcal{P}(A) \sim A \to \{0, 1\}$, поэтому $|\mathcal{P}(A)| > |A|$ для любого множества.
- В том числе $|\mathcal{P}(U)| > |U|$. Но элементы $|\mathcal{P}(U)|$ — множества, поэтому $\mathcal{P}(U) \subseteq U$ и $|\mathcal{P}(U)| \leq |U|$.
- Пришли к противоречию!
- Заметьте, что функции у нас тоже множества, так что переходить к $\mathcal{P}$ было не обязательно.

## Понятие класса

- Чтобы всё-таки иметь возможность говорить о всех множествах вместе, вводится понятие *класса*.
- Это любая совокупность множеств, которые имеют какое-то свойство.
- Некоторые классы являются множествами, некоторые нет.
- Вторые называются *собственными классами* и не могут быть элементами классов или множеств.
- Ещё один пример собственного класса — все одноэлементные множества. Почему?

# Понятие класса

- Чтобы всё-таки иметь возможность говорить о всех множествах вместе, вводится понятие *класса*.
- Это любая совокупность множеств, которые имеют какое-то свойство.
- Некоторые классы являются множествами, некоторые нет.
- Вторые называются *собственными классами* и не могут быть элементами классов или множеств.
- Ещё один пример собственного класса — все одноэлементные множества. Почему?
- Нетрудно построить биекцию между ними и классом всех множеств.

## Понятие класса

- Чтобы всё-таки иметь возможность говорить о всех множествах вместе, вводится понятие *класса*.
- Это любая совокупность множеств, которые имеют какое-то свойство.
- Некоторые классы являются множествами, некоторые нет.
- Вторые называются *собственными классами* и не могут быть элементами классов или множеств.
- Ещё один пример собственного класса — все одноэлементные множества. Почему?
- Нетрудно построить биекцию между ними и классом всех множеств.
- Окажется, что любой несобственный класс «того же размера».

# Операции над мощностью

- Как можно определить операции над мощностями множеств по аналогии с конечными множествами?
- $|A| + |B| =$

## Операции над мощностью

- Как можно определить операции над мощностями множеств по аналогии с конечными множествами?
- $|A| + |B| = |A \cup B|$, где $A \cap B = \varnothing$.

## Операции над мощностью

- Как можно определить операции над мощностями множеств по аналогии с конечными множествами?
- $|A| + |B| = |A \cup B|$, где $A \cap B = \varnothing$.
- $|A| \cdot |B| =$

# Операции над мощностью

- Как можно определить операции над мощностями множеств по аналогии с конечными множествами?
- $|A| + |B| = |A \cup B|$, где $A \cap B = \varnothing$.
- $|A| \cdot |B| = |A \times B|$.

# Операции над мощностью

- Как можно определить операции над мощностями множеств по аналогии с конечными множествами?
- $|A| + |B| = |A \cup B|$, где $A \cap B = \varnothing$.
- $|A| \cdot |B| = |A \times B|$.
- $|A|^{|B|} =$

# Операции над мощностью

- Как можно определить операции над мощностями множеств по аналогии с конечными множествами?
- $|A| + |B| = |A \cup B|$, где $A \cap B = \varnothing$.
- $|A| \cdot |B| = |A \times B|$.
- $|A|^{|B|} = |B \to A|$.
- В частности, $2^{|A|} =$

# Операции над мощностью

- Как можно определить операции над мощностями множеств по аналогии с конечными множествами?
- $|A| + |B| = |A \cup B|$, где $A \cap B = \varnothing$.
- $|A| \cdot |B| = |A \times B|$.
- $|A|^{|B|} = |B \to A|$.
- В частности, $2^{|A|} = |A \to \{0, 1\}| = |\mathcal{P}(A)|$.

# Операции над мощностью

- Как можно определить операции над мощностями множеств по аналогии с конечными множествами?
- $|A| + |B| = |A \cup B|$, где $A \cap B = \varnothing$.
- $|A| \cdot |B| = |A \times B|$.
- $|A|^{|B|} = |B \to A|$.
- В частности, $2^{|A|} = |A \to \{0, 1\}| = |\mathcal{P}(A)|$.

# Операции над мощностью

- Как можно определить операции над мощностями множеств по аналогии с конечными множествами?
- $|A| + |B| = |A \cup B|$, где $A \cap B = \varnothing$.
- $|A| \cdot |B| = |A \times B|$.
- $|A|^{|B|} = |B \to A|$.
- В частности, $2^{|A|} = |A \to \{0, 1\}| = |\mathcal{P}(A)|$.
- Важно, что при замене $A$ или $B$ на равномощное результат не меняется. Это нужно доказать (для каждого из определений).
- Контрпример: рассмотрим определение $|A| \oplus |B| = |A \cup B|$ (без условий). В чём проблема с ним?
- Имеем $\aleph_0 + \aleph_0 = \aleph_0$ и $\aleph_0 \cdot \aleph_0 = \aleph_0$.

# Мощность континуума

- $2^{\aleph_0}$ (то есть мощность $\mathbb{N} \to \{0, 1\}$ или $\mathcal{P}(\mathbb{N})$) имеет своё название *мощность континуума* и обозначение $\mathfrak{c}$.
- Ту же мощность имеют множества $\mathbb{R}$, $(0, 1)$, $\mathbb{R}^n$ и т.д.
- То есть $\mathfrak{c} + \mathfrak{c} = \mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$.

# Аксиоматические теории множеств

- Как упоминалось ближе к началу лекции, современная теория множеств задаётся аксиомами в логике предикатов.
- Самый распространённый набор аксиом это ZFC. Его аксиомы можно найти в Википедии: Система Цермело — Френкеля.
- Также можно посмотреть NBG (теорию фон Неймана — Бернайса — Гёделя).