Теория множеств
Вполне упорядоченные множества и аксиома выбора

Математическая логика и теория алгоритмов

Алексей Романов

11 декабря 2024 г.

МИЭТ

Отношения порядка

- Напомню: бинарное отношение $\preccurlyeq$ на множестве A называется *отношением (частичного, нестрогого) порядка*, если оно:
  - Рефлексивно: $\forall x : A\ x \preccurlyeq x$
  - Антисимметрично: $\forall x, y : A\ x \preccurlyeq y \land y \preccurlyeq x \to x = y$
  - Транзитивно: $\forall x, y, z : A\ x \preccurlyeq y \land y \preccurlyeq z \to x \preccurlyeq z$
- Если ещё $\forall x, y : A\ x \preccurlyeq y \lor y \preccurlyeq x$, то это *отношение линейного порядка*.
- Пара $(A, \preccurlyeq)$ называется *частично (соотв. линейно) упорядоченным множеством*, сокращённо ЧУМ (ЛУМ).
- $x \prec y$, если $x \preccurlyeq y \land x \neq y$.

Отношения порядка

- Напомню: бинарное отношение $\preccurlyeq$ на множестве A называется *отношением (частичного, нестрогого) порядка*, если оно:
  - Рефлексивно: $\forall x : A\ x \preccurlyeq x$
  - Антисимметрично: $\forall x, y : A\ x \preccurlyeq y \wedge y \preccurlyeq x \to x = y$
  - Транзитивно: $\forall x, y, z : A\ x \preccurlyeq y \wedge y \preccurlyeq z \to x \preccurlyeq z$
- Если ещё $\forall x, y : A\ x \preccurlyeq y \vee y \preccurlyeq x$, то это *отношение линейного порядка*.
- Пара $(A, \preccurlyeq)$ называется *частично (соотв. линейно) упорядоченным множеством*, сокращённо ЧУМ (ЛУМ).
- $x \prec y$, если $x \preccurlyeq y \wedge x \neq y$.
- x — *наименьший элемент* A, если $\forall y : A\ x \preccurlyeq y$, и *минимальный*, если $\neg\exists y : A\ y \prec x$.
- Для ЛУМ минимальный и наименьший одно и то же, а для ЧУМ нет.

Порядковые изоморфизмы

- Биекция $f : A \to B$ между двумя ЧУМ называется *порядковым изоморфизмом*, если $\forall x, y : A\ x \preccurlyeq_A y \leftrightarrow f(x) \preccurlyeq_B f(y)$.
- В этой лекции все изоморфизмы порядковые, дальше это слово опускаем.

Порядковые изоморфизмы

- Биекция $f : A \to B$ между двумя ЧУМ называется *порядковым изоморфизмом*, если $\forall x, y : A\ x \preccurlyeq_A y \leftrightarrow f(x) \preccurlyeq_B f(y)$.
- В этой лекции все изоморфизмы порядковые, дальше это слово опускаем.
- Если A — ЛУМ из n элементов, то оно изоморфно $\{1, \ldots, n\}$.

Порядковые изоморфизмы

- Биекция $f : A \to B$ между двумя ЧУМ называется *порядковым изоморфизмом*, если $\forall x, y : A\ x \preccurlyeq_A y \leftrightarrow f(x) \preccurlyeq_B f(y)$.
- В этой лекции все изоморфизмы порядковые, дальше это слово опускаем.
- Если A — ЛУМ из n элементов, то оно изоморфно $\{1, \ldots, n\}$.
- Доказательство: в A есть наименьший элемент. Обозначим его a_1 и сопоставим с 1. $A \setminus \{a_1\}$ снова конечно и линейно упорядочено.

Порядковые изоморфизмы

- Биекция $f : A \to B$ между двумя ЧУМ называется *порядковым изоморфизмом*, если $\forall x, y : A\ x \preccurlyeq_A y \leftrightarrow f(x) \preccurlyeq_B f(y)$.
- В этой лекции все изоморфизмы порядковые, дальше это слово опускаем.
- Если A — ЛУМ из n элементов, то оно изоморфно $\{1, \ldots, n\}$.
- Доказательство: в A есть наименьший элемент. Обозначим его a_1 и сопоставим с 1. $A \setminus \{a_1\}$ снова конечно и линейно упорядочено. Выберем из него наименьший a_2 и сопоставим с 2. И т.д.

Порядковые изоморфизмы

- Биекция $f : A \to B$ между двумя ЧУМ называется *порядковым изоморфизмом*, если $\forall x, y : A\ x \preccurlyeq_A y \leftrightarrow f(x) \preccurlyeq_B f(y)$.
- В этой лекции все изоморфизмы порядковые, дальше это слово опускаем.
- Если A — ЛУМ из n элементов, то оно изоморфно $\{1, \ldots, n\}$.
- Доказательство: в A есть наименьший элемент. Обозначим его a_1 и сопоставим с 1. $A \setminus \{a_1\}$ снова конечно и линейно упорядочено. Выберем из него наименьший a_2 и сопоставим с 2. И т.д.
- Следствие: два равномощных конечных ЛУМ изоморфны.
- Для бесконечных это не так! Например,

Порядковые изоморфизмы

- Биекция $f : A \to B$ между двумя ЧУМ называется *порядковым изоморфизмом*, если $\forall x, y : A\ x \preccurlyeq_A y \leftrightarrow f(x) \preccurlyeq_B f(y)$.
- В этой лекции все изоморфизмы порядковые, дальше это слово опускаем.
- Если A — ЛУМ из n элементов, то оно изоморфно $\{1, \ldots, n\}$.
- Доказательство: в A есть наименьший элемент. Обозначим его a_1 и сопоставим с 1. $A \setminus \{a_1\}$ снова конечно и линейно упорядочено. Выберем из него наименьший a_2 и сопоставим с 2. И т.д.
- Следствие: два равномощных конечных ЛУМ изоморфны.
- Для бесконечных это не так! Например, $\mathbb{N}$, $\mathbb{Z}$ и $\mathbb{Q}$ не изоморфны (почему?).

Фундированные и вполне упорядоченные множества

- Вспомните *принцип полной индукции* на $\mathbb{N}$:

Фундированные и вполне упорядоченные множества

- Вспомните *принцип полной индукции* на $\mathbb{N}$: Пусть $P(x)$ свойство натуральных чисел, и можно доказать, что если оно верно для всех $y \prec x$, то оно верно для x. Тогда оно верно для всех натуральных чисел. Формально: $\forall x\ (\forall y < x\ P(y)) \to P(x)) \to \forall x\ P(x)$

Фундированные и вполне упорядоченные множества

- Вспомните *принцип полной индукции* на $\mathbb{N}$: Пусть $P(x)$ свойство натуральных чисел, и можно доказать, что если оно верно для всех $y \prec x$, то оно верно для x. Тогда оно верно для всех натуральных чисел. Формально: $\forall x\ (\forall y < x\ P(y)) \to P(x)) \to \forall x\ P(x)$
- Для каких ещё ЧУМ он выполняется?
- Теорема: следующие 3 утверждения равносильны для любого ЧУМ A:
    1. В любом непустом подмножестве A есть минимальный элемент.
    2. В A нет бесконечных убывающих последовательностей $a_1 \succ a_2 \succ \ldots$.
    3. Принцип полной индукции для A.
- Такое ЧУМ называется *фундированным*.

Множество фундировано $\Leftrightarrow$ нет бесконечных убывающих последовательностей

- $1 \Rightarrow 2$: Если $a_1 \succ a_2 \succ \ldots$ — бесконечная убывающая последовательность, то

Множество фундировано $\Leftrightarrow$ нет бесконечных убывающих последовательностей

- $1 \Rightarrow 2$: Если $a_1 \succ a_2 \succ \ldots$ — бесконечная убывающая последовательность, то $\{a_1, a_2, \ldots\}$ — непустое множество без минимального элемента.

Множество фундировано $\Leftrightarrow$ нет бесконечных убывающих последовательностей

- $1 \Rightarrow 2$: Если $a_1 \succ a_2 \succ \ldots$ — бесконечная убывающая последовательность, то $\{a_1, a_2, \ldots\}$ — непустое множество без минимального элемента.
- $2 \Rightarrow 1$: Если B — непустое подмножество A без минимального элемента, то

Множество фундировано $\Leftrightarrow$ нет бесконечных убывающих последовательностей

- $1 \Rightarrow 2$: Если $a_1 \succ a_2 \succ \ldots$ — бесконечная убывающая последовательность, то $\{a_1, a_2, \ldots\}$ — непустое множество без минимального элемента.
- $2 \Rightarrow 1$: Если B — непустое подмножество A без минимального элемента, то возьмём его произвольный элемент и обозначим a_1.

Множество фундировано $\Leftrightarrow$ нет бесконечных убывающих последовательностей

- $1 \Rightarrow 2$: Если $a_1 \succ a_2 \succ \ldots$ — бесконечная убывающая последовательность, то $\{a_1, a_2, \ldots\}$ — непустое множество без минимального элемента.
- $2 \Rightarrow 1$: Если B — непустое подмножество A без минимального элемента, то возьмём его произвольный элемент и обозначим a_1. Так как он не минимальный, то есть $a_2 \prec a_1$.

Множество фундировано $\Leftrightarrow$ нет бесконечных убывающих последовательностей

- $1 \Rightarrow 2$: Если $a_1 \succ a_2 \succ \dots$ — бесконечная убывающая последовательность, то $\{a_1, a_2, \dots\}$ — непустое множество без минимального элемента.
- $2 \Rightarrow 1$: Если B — непустое подмножество A без минимального элемента, то возьмём его произвольный элемент и обозначим a_1. Так как он не минимальный, то есть $a_2 \prec a_1$. Аналогично есть $a_3 \prec a_2 \dots$

Множество фундировано $\Leftrightarrow$ принцип полной индукции

- $1 \Rightarrow 3$: Пусть $P(x)$ — свойство на A, для которого верно $\forall x\ (\forall y \prec x\ P(y)) \to P(x)$, но не $\forall x\ P(x)$. Рассмотрим $B = \{x : A \mid \neg P(x)\}$. Оно непусто. Так как A фундировано, в B есть минимальный элемент b. Но тогда

Множество фундировано $\Leftrightarrow$ принцип полной индукции

- $1 \Rightarrow 3$: Пусть $P(x)$ — свойство на A, для которого верно $\forall x\ (\forall y \prec x\ P(y)) \to P(x)$, но не $\forall x\ P(x)$. Рассмотрим $B = \{x : A \mid \neg P(x)\}$. Оно непусто. Так как A фундировано, в B есть минимальный элемент b. Но тогда $\forall x : A\ x \prec b \Rightarrow x \notin B \Rightarrow P(x)$ и по предположению ППИ $P(b)$, то есть $b \notin B$. Противоречие!

Множество фундировано $\Leftrightarrow$ принцип полной индукции

- $1 \Rightarrow 3$: Пусть $P(x)$ — свойство на A, для которого верно $\forall x\ (\forall y \prec x\ P(y)) \to P(x)$, но не $\forall x\ P(x)$. Рассмотрим $B = \{x : A \mid \neg P(x)\}$. Оно непусто. Так как A фундировано, в B есть минимальный элемент b. Но тогда $\forall x : A\ x \prec b \Rightarrow x \notin B \Rightarrow P(x)$ и по предположению ППИ $P(b)$, то есть $b \notin B$. Противоречие!
- $3 \Rightarrow 1$: Если B — подмножество A без минимального элемента, то рассмотрим $P(x) \Leftrightarrow x \notin B$. Имеем $(\forall y \prec x\ P(y)) \Rightarrow (\forall y \prec x\ y \notin B) \Rightarrow x \notin B$ (иначе x минимальный в B) $\Rightarrow P(x)$

Множество фундировано $\Leftrightarrow$ принцип полной индукции

- $1 \Rightarrow 3$: Пусть $P(x)$ — свойство на A, для которого верно $\forall x\ (\forall y \prec x\ P(y)) \to P(x)$, но не $\forall x\ P(x)$. Рассмотрим $B = \{x : A \mid \neg P(x)\}$. Оно непусто. Так как A фундировано, в B есть минимальный элемент b. Но тогда $\forall x : A\ x \prec b \Rightarrow x \notin B \Rightarrow P(x)$ и по предположению ППИ $P(b)$, то есть $b \notin B$. Противоречие!
- $3 \Rightarrow 1$: Если B — подмножество A без минимального элемента, то рассмотрим $P(x) \Leftrightarrow x \notin B$. Имеем $(\forall y \prec x\ P(y)) \Rightarrow (\forall y \prec x\ y \notin B) \Rightarrow x \notin B$ (иначе x минимальный в B) $\Rightarrow P(x)$. По ППИ $\forall x\ P(x) \Rightarrow \forall x\ x \notin B \Rightarrow B$ пусто.

Операции над ЧУМ

- Любое подмножество B ЧУМ A имеет *индуцированный порядок*.
- Если A и B непересекающиеся ЧУМ, то $A+B$ это $A \cup B$ с порядком

$$x \prec_{A+B} y \Leftrightarrow (x, y \in A \wedge x \prec_A y) \vee (x, y \in B \wedge x \prec_B y) \vee (x \in A \wedge y \in B)$$

- Порядок на $A \times B$ лексикографический, то есть

$$(a_1, b_1) \prec_{A \times B} (a_2, b_2) \Leftrightarrow a_1 \prec_A a_2 \vee (a_1 = a_2 \wedge b_1 \prec_B b_2)$$

- Если A и B фундированы и/или линейны, то $A+B$ и $A \times B$ тоже. Доказательство как упражнение.

Вполне упорядоченные множества

- Фундированное ЛУМ называется *вполне упорядоченным*.
- Некоторые простые свойства:
- Любое непустое ВУМ имеет наименьший элемент.
- Если элемент x ВУМ не наибольший, то есть непосредственно следующий за ним $S(x)$ (или $x + 1$).
- У не-наименьшего элемента ВУМ может не быть непосредственно предыдущего. Такой элемент называется *предельным*.
- Любое ограниченное сверху подмножество ВУМ имеет супремум (точную верхнюю грань).
- Любое подмножество ВУМ само вполне упорядочено.

Начальные отрезки

- $B \subseteq A$ — *начальный отрезок* A, если любой элемент B меньше любого элемента $A \setminus B$. Равносильно: все элементы, меньшие какого-то элемента B, лежат в B.
- Это определение имеет смысл для любого ЛУМ, но нам интересно только для ВУМ.
- В том числе $\varnothing$ и A — начальные отрезки A.
- Если все элементы множества D — начальные отрезки ВУМ A, то $\bigcup D$ тоже начальный отрезок A.
- B — собственный начальный отрезок ВУМ A (т.е. $B \neq A$) $\Leftrightarrow \exists x : A\ B = \{y : A \mid y \prec x\}$. Обозначим $\{y : A \mid y \prec x\}$ как $A_{\prec x}$.
- Если B и C начальные отрезки ВУМ A, то $B \subseteq C \vee C \subseteq B$.

Теоремы о сравнении ВУМ

- Теорема: пусть A и B ВУМ. Тогда либо A изоморфно какому-то начальному отрезку B (возможно, самому B), либо наоборот.
- Теорема: ВУМ A никогда не изоморфно своему собственному начальному отрезку B.
- Доказательства: сейчас давать не буду, можно найти в книге Шеня-Верещагина.
- Следствие: любые ВУМ A и B либо изоморфны, либо ровно одно из них изоморфно собственному начальному отрезку другого.

Аксиома выбора

- Пусть A произвольное множество непустых множеств. Тогда существует такая *функция выбора* $ch_A : A \to \bigcup A$, что $\forall B : A\ ch_A(B) \in B$.
- Можно сформулировать то же для индексированных семейств непустых множеств: если $A = \langle A_i \rangle_{i:I}$, то $ch_A : I \to \bigcup_{i:I} A_i,\ \forall i : I\ ch_A(i) \in A_i$.
- Эта аксиома не входит в исходную теорию Цермело–Френкеля *ZF*, её добавление даёт *ZFC*, стандартное основание математики.
- Заметьте, что «дано непустое множество, выберем в нём элемент» не требует аксиомы выбора.
- То же и для конечных A (и I) в определении выше.
- Аксиома выбора нужна, чтобы сделать одновременно бесконечно много таких выборов и зафиксировать их.

Лемма Цорна

- *Цепь* в ЧУМ — такое подмножество, любые два элемента которого сравнимы.
- Если в ЧУМ A любая цепь B имеет верхнюю грань ($\exists x : A\ \forall y : B\ y \preccurlyeq x$), то в A есть максимальный элемент.
- (Вспомните разницу между максимальным и наибольшим!)
- Доказательство тоже в учебнике.

Лемма Цорна

- *Цепь* в ЧУМ — такое подмножество, любые два элемента которого сравнимы.
- Если в ЧУМ A любая цепь B имеет верхнюю грань ($\exists x : A \; \forall y : B \; y \preccurlyeq x$), то в A есть максимальный элемент.
- (Вспомните разницу между максимальным и наибольшим!)
- Доказательство тоже в учебнике.
- Можно немного усилить и показать, что для любого x в таком A есть максимальный y такой, что $y \succcurlyeq x$.

Лемма Цорна

- *Цепь* в ЧУМ — такое подмножество, любые два элемента которого сравнимы.
- Если в ЧУМ A любая цепь B имеет верхнюю грань $(\exists x : A\ \forall y : B\ y \preccurlyeq x)$, то в A есть максимальный элемент.
- (Вспомните разницу между максимальным и наибольшим!)
- Доказательство тоже в учебнике.
- Можно немного усилить и показать, что для любого x в таком A есть максимальный y такой, что $y \succcurlyeq x$.

- Типичное применение леммы Цорна: в любом линейном пространстве L есть базис.

Лемма Цорна

- *Цепь* в ЧУМ — такое подмножество, любые два элемента которого сравнимы.
- Если в ЧУМ A любая цепь B имеет верхнюю грань ($\exists x : A\ \forall y : B\ y \preccurlyeq x$), то в A есть максимальный элемент.
- (Вспомните разницу между максимальным и наибольшим!)
- Доказательство тоже в учебнике.
- Можно немного усилить и показать, что для любого x в таком A есть максимальный y такой, что $y \succcurlyeq x$.

- Типичное применение леммы Цорна: в любом линейном пространстве L есть базис.
- Для доказательства возьмём $A = \{S \subset L \mid S$ линейно независимо$\}$ с порядком по включению.
- Верхняя грань любой цепи в нём — объединение.
- Максимальный элемент и будет базисом.

Теорема Цермело

- На любом множестве A можно задать отношение вполне порядка $\preccurlyeq$.
- Идея доказательства (остаётся доказать 2 и 4):
  1. Возьмём множество WO_A пар $(B, \preccurlyeq_B)$, где $B \subseteq A, \preccurlyeq_B$ — вполне порядок на B. Отношение «быть начальным отрезком» — частичный порядок на нём.
  2. Для любой цепи в этом порядке объединение множеств будет верхней гранью.
  3. По лемме Цорна есть максимальное $(B^*, \preccurlyeq_{B^*}) \in WO_A$.
  4. Если $B^* \neq A$, то оно не будет максимальным.
  5. Значит, $B^* = A$, и $\preccurlyeq_{B^*}$ — искомый вполне порядок на A.
- При этом ни на каком несчётном множестве задать такое отношение порядка явно формулой ZFC невозможно.

Эквивалентные формы аксиомы выбора

- Аксиома выбора, теорема Цермело и лемма Цорна эквивалентны.
- Доказательство аксиомы выбора из теоремы Цермело просто: введём вполне порядок $\prec$ на $\bigcup A$ и для любого $B \in A$ выберем из B

Эквивалентные формы аксиомы выбора

- Аксиома выбора, теорема Цермело и лемма Цорна эквивалентны.
- Доказательство аксиомы выбора из теоремы Цермело просто: введём вполне порядок $\prec$ на $\bigcup A$ и для любого $B \in A$ выберем из B $\min B$ по $\prec$.
- Шутка Джерри Бона: «АВ очевидно истинна, ТЦ очевидно ложна, а кто может сказать про ЛЦ?».

Эквивалентные формы аксиомы выбора

- Аксиома выбора, теорема Цермело и лемма Цорна эквивалентны.
- Доказательство аксиомы выбора из теоремы Цермело просто: введём вполне порядок $\prec$ на $\bigcup A$ и для любого $B \in A$ выберем из B $\min B$ по $\prec$.
- Шутка Джерри Бона: «АВ очевидно истинна, ТЦ очевидно ложна, а кто может сказать про ЛЦ?».
- Другие эквивалентные им утверждения:
  1. Декартово произведение непустого множества непустых множеств непусто (его элементы и есть функции выбора на этом множестве).
  2. У каждого наложения есть правая обратная функция.
  3. В любом ЧУМ существует максимальная цепь (принцип максимума Хаусдорфа).
  4. Любое бесконечное A равномощно $A \times A$.
  5. Любые два множества сравнимы по мощности.
  6. В любом линейном пространстве есть базис.

Следствия аксиомы выбора

- Парадокс Банаха–Тарского (также известный как парадокс удвоения шара) следует из аксиомы выбора.
- Как и вообще существование неизмеримых множеств.
- Если множество A бесконечно, то существует вложение $\mathbb{N} \to A$.
- Если бесконечные A и B равномощны и не пересекаются, то $A \cup B \sim A$.
- Если в векторном пространстве нет конечного базиса, то в нём есть бесконечное линейно независимое множество векторов.

Слабые формы аксиомы выбора

- Аксиома счётного выбора AC_ω это аксиома выбора для счётных множеств A. С индексами: если дана последовательность непустых множеств $\langle A_n \rangle_{n:\mathbb{N}}$, то можно выбрать по элементу из каждого: существует f :

Слабые формы аксиомы выбора

- Аксиома счётного выбора AC_ω это аксиома выбора для счётных множеств A. С индексами: если дана последовательность непустых множеств $\langle A_n \rangle_{n:\mathbb{N}}$, то можно выбрать по элементу из каждого: существует $f : \mathbb{N} \to \bigcup_{n \in \mathbb{N}} A_n$,

Слабые формы аксиомы выбора

- Аксиома счётного выбора AC_ω это аксиома выбора для счётных множеств A. С индексами: если дана последовательность непустых множеств $\langle A_n \rangle_{n:\mathbb{N}}$, то можно выбрать по элементу из каждого: существует $f : \mathbb{N} \to \bigcup_{n \in \mathbb{N}} A_n, \forall n \; f(n) \in A_n$.
  - Пример следствия (но не эквивалентно!): объединение счётного множества счётных множеств счётно.

Слабые формы аксиомы выбора

- Аксиома счётного выбора AC_ω это аксиома выбора для счётных множеств A. С индексами: если дана последовательность непустых множеств $\langle A_n \rangle_{n:\mathbb{N}}$, то можно выбрать по элементу из каждого: существует $f : \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n, \forall n\, f(n) \in A_n$.
  - Пример следствия (но не эквивалентно!): объединение счётного множества счётных множеств счётно.
- Аксиома зависимого выбора DC: если A непустое множество, R бинарное отношение на нём и $\forall x : A\ \exists y : A\ xRy$, то существует бесконечная последовательность $x_n : A$ такая, что $\forall n : \mathbb{N}\ x_n R x_{n+1}$.
  - Это эквивалентно лемме Цорна для конечных цепей: если в ЧУМ все цепи конечны, то там есть максимальный элемент.

Слабые формы аксиомы выбора

- Аксиома счётного выбора AC_ω это аксиома выбора для счётных множеств A. С индексами: если дана последовательность непустых множеств $\langle A_n \rangle_{n:\mathbb{N}}$, то можно выбрать по элементу из каждого: существует $f : \mathbb{N} \to \bigcup_{n \in \mathbb{N}} A_n, \forall n\ f(n) \in A_n$.
  - Пример следствия (но не эквивалентно!): объединение счётного множества счётных множеств счётно.
- Аксиома зависимого выбора DC: если A непустое множество, R бинарное отношение на нём и $\forall x : A\ \exists y : A\ xRy$, то существует бесконечная последовательность $x_n : A$ такая, что $\forall n : \mathbb{N}\ x_n R x_{n+1}$.
  - Это эквивалентно лемме Цорна для конечных цепей: если в ЧУМ все цепи конечны, то там есть максимальный элемент.
- $AC \Rightarrow DC \Rightarrow AC_\omega$.

Ординалы

- *Ординалы* можно определить по аналогии с мощностями: это классы эквивалентности ВУМ по отношению изоморфности (*порядковые типы*).
- То есть у любого ВУМ есть ординал, и ординалы изоморфных ВУМ равны.
- Но есть более удобное индуктивное определение:
  - $0 = \varnothing$ это ординал.
  - Если α ординал, то $\alpha + 1 = S(\alpha) = \alpha \cup \{\alpha\}$ тоже ординал.
  - Если A множество, все элементы которого ординалы, то $\sup A = \bigcup A$ тоже ординал.
- *Предельный ординал* — такой, который не 0 и не следует ни за каким ординалом.
- То есть его можно получить только как супремум.
- С помощью аксиомы выбора, можно доказать, что любое ВУМ изоморфно одному из таких ординалов.
- Класс всех ординалов обозначается *Ord*.

Структура счётных ординалов (до ω^ω)

- $0 = \varnothing$.
- $1 = S(0) = 0 \cup \{0\} = \{0\}$.

Структура счётных ординалов (до ω^ω)

- $0 = \varnothing$.
- $1 = S(0) = 0 \cup \{0\} = \{0\}$.
- $2 = S(1) = \{0, 1\}$.
- $\ldots$

Структура счётных ординалов (до ω^ω)

- $0 = \varnothing$.
- $1 = S(0) = 0 \cup \{0\} = \{0\}$.
- $2 = S(1) = \{0, 1\}$.
- $\ldots$
- $\omega = \sup\{0, 1, 2, \ldots\} = 0 \cup 1 \cup 2 \cup \ldots =$

Структура счётных ординалов (до ω^ω)

- $0 = \varnothing$.
- $1 = S(0) = 0 \cup \{0\} = \{0\}$.
- $2 = S(1) = \{0, 1\}$.
- $\dots$
- $\omega = \sup\{0, 1, 2, \dots\} = 0 \cup 1 \cup 2 \cup \dots = \{0, 1, 2, \dots\}$.

Структура счётных ординалов (до ω^ω)

- $0 = \varnothing$.
- $1 = S(0) = 0 \cup \{0\} = \{0\}$.
- $2 = S(1) = \{0, 1\}$.
- $\ldots$
- $\omega = \sup\{0, 1, 2, \ldots\} = 0 \cup 1 \cup 2 \cup \ldots = \{0, 1, 2, \ldots\}$.
- $\omega + 1 = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}$.
- $\omega + 2 = \{0, 1, 2, \ldots, \omega, \omega + 1\}$.
- $\ldots$

Структура счётных ординалов (до ω^ω)

- $0 = \varnothing$.
- $1 = S(0) = 0 \cup \{0\} = \{0\}$.
- $2 = S(1) = \{0, 1\}$.
- $\ldots$
- $\omega = \sup\{0, 1, 2, \ldots\} = 0 \cup 1 \cup 2 \cup \ldots = \{0, 1, 2, \ldots\}$.
- $\omega + 1 = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}$.
- $\omega + 2 = \{0, 1, 2, \ldots, \omega, \omega + 1\}$.
- $\ldots$
- $\omega \cdot 2 = \sup\{\omega, \omega + 1, \omega + 2, \ldots\} =$

Структура счётных ординалов (до ω^ω)

- $0 = \varnothing$.
- $1 = S(0) = 0 \cup \{0\} = \{0\}$.
- $2 = S(1) = \{0, 1\}$.
- $\ldots$
- $\omega = \sup\{0, 1, 2, \ldots\} = 0 \cup 1 \cup 2 \cup \ldots = \{0, 1, 2, \ldots\}$.
- $\omega + 1 = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}$.
- $\omega + 2 = \{0, 1, 2, \ldots, \omega, \omega + 1\}$.
- $\ldots$
- $\omega \cdot 2 = \sup\{\omega, \omega + 1, \omega + 2, \ldots\} = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\}$.
- $\omega \cdot 2 + 1 = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega \cdot 2\}$.
- $\ldots$

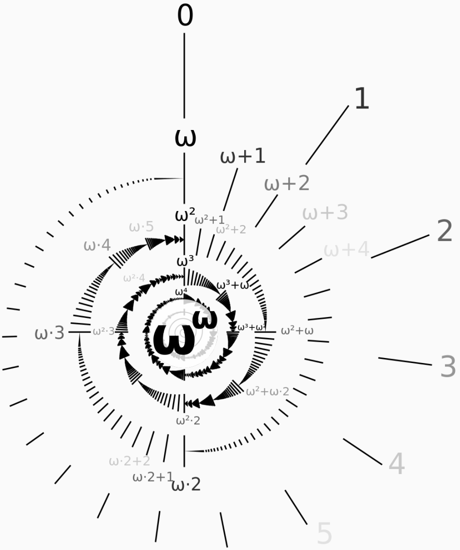
Структура счётных ординалов (до ω^ω)

- $0 = \varnothing$.
- $1 = S(0) = 0 \cup \{0\} = \{0\}$.
- $2 = S(1) = \{0, 1\}$.
- $\ldots$
- $\omega = \sup\{0, 1, 2, \ldots\} = 0 \cup 1 \cup 2 \cup \ldots = \{0, 1, 2, \ldots\}$.
- $\omega + 1 = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}$.
- $\omega + 2 = \{0, 1, 2, \ldots, \omega, \omega + 1\}$.
- $\ldots$
- $\omega \cdot 2 = \sup\{\omega, \omega + 1, \omega + 2, \ldots\} = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\}$.
- $\omega \cdot 2 + 1 = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega \cdot 2\}$.
- $\ldots$
- $\omega^2 = \omega \cdot \omega = \sup\{\omega, \omega \cdot 2, \omega \cdot 3, \ldots\} =$

Структура счётных ординалов (до ω^ω)

- $0 = \varnothing$.
- $1 = S(0) = 0 \cup \{0\} = \{0\}$.
- $2 = S(1) = \{0, 1\}$.
- $\ldots$
- $\omega = \sup\{0, 1, 2, \ldots\} = 0 \cup 1 \cup 2 \cup \ldots = \{0, 1, 2, \ldots\}$.
- $\omega + 1 = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}$.
- $\omega + 2 = \{0, 1, 2, \ldots, \omega, \omega + 1\}$.
- $\ldots$
- $\omega \cdot 2 = \sup\{\omega, \omega + 1, \omega + 2, \ldots\} = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\}$.
- $\omega \cdot 2 + 1 = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega \cdot 2\}$.
- $\ldots$
- $\omega^2 = \omega \cdot \omega = \sup\{\omega, \omega \cdot 2, \omega \cdot 3, \ldots\} =$
  $\{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega \cdot 2, \omega \cdot 2 + 1, \ldots\}$.
- $\ldots$

Структура счётных ординалов (до ω^ω)



Порядок на ординалах

- $\alpha < \beta \Leftrightarrow \alpha \in \beta \Leftrightarrow \alpha \subsetneq \beta$.
- Каждый ординал равен множеству всех ординалов, меньших него: $\alpha = \{\beta | \beta < \alpha\}$.
- Легко доказать, что $\leq$ действительно отношение порядка: рефлексивно, транзитивно и антисимметрично. И линейно.
- Более того, ординалы вполне упорядочены: в любом классе (не только множестве) ординалов есть наименьший.
- Теперь можно проверить, что если A множество ординалов, то $\bigcup A$ это действительно $\sup A$, то есть наименьшая верхняя грань.

Парадокс Бурали-Форти

- Ограничение «если A множество» в определении ординала-супремума существенное: множества всех ординалов не существует.
- Допустим, что Ord множество. Тогда $O = \sup Ord + 1$ ординал, но это не элемент Ord. Почему?

Парадокс Бурали-Форти

- Ограничение «если A множество» в определении ординала-супремума существенное: множества всех ординалов не существует.
- Допустим, что Ord множество. Тогда $O = \sup Ord + 1$ ординал, но это не элемент Ord. Почему?
- Например, потому что он больше всех элементов Ord.

Парадокс Бурали-Форти

- Ограничение «если A множество» в определении ординала-супремума существенное: множества всех ординалов не существует.
- Допустим, что Ord множество. Тогда $O = \sup Ord + 1$ ординал, но это не элемент Ord. Почему?
- Например, потому что он больше всех элементов Ord.
- Но тогда получится, что Ord содержит не все ординалы. Пришли к противоречию!

Арифметика над ординалами

- Операции над ординалами определяются по рекурсии:
  - $\alpha + 0 = \alpha$.
  - $\alpha + S(\beta) = S(\alpha + \beta)$.
  - $\alpha + \sup A = \sup\{\alpha + \beta | \beta \in A\}$.
-
  - $\alpha \cdot 0 = 0$.
  - $\alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha$.
  - $\alpha \cdot \sup A = \sup\{\alpha \cdot \beta | \beta \in A\}$.
-
  - $\alpha^0 = 1$.
  - $\alpha^{S(\beta)} = \alpha^\beta \cdot \alpha$.
  - $\alpha^{\sup A} = \sup\{\alpha^\beta | \beta \in A\}$.

Арифметика над ординалами

- Например, $1 + \omega = 1 + \sup\{0, 1, 2, \ldots\}$

Арифметика над ординалами

- Например, $1 + \omega = 1 + \sup\{0, 1, 2, \ldots\} = \sup\{1, 2, 3, \ldots\} = \bigcup\{1, 2, 3, \ldots\} = \{0, 1, \ldots\} = \omega$.
- Многие привычные свойства арифметики для ординалов сохраняются, но как видим, не все.

Кардиналы

- С помощью ординалов мы можем дать окончательное определение $|A|$ так, чтобы она была множеством.

Кардиналы

- С помощью ординалов мы можем дать окончательное определение $|A|$ так, чтобы она была множеством.
- По теореме Цермело A можно вполне упорядочить. То есть A биективно какому-то ординалу.
- Тогда класс $\{\alpha | \alpha : Ord, A \sim \alpha\}$ непуст и имеет

Кардиналы

- С помощью ординалов мы можем дать окончательное определение $|A|$ так, чтобы она была множеством.
- По теореме Цермело A можно вполне упорядочить. То есть A биективно какому-то ординалу.
- Тогда класс $\{\alpha|\alpha : Ord, A \sim \alpha\}$ непуст и имеет минимум. Этот минимум и есть $|A|$.
- Видно ли, что если $A \sim B$, то $|A| = |B|$, как и требуется?
- Все значения $|A|$ (то есть минимальные ординалы какой-то мощности) называются кардиналами.

Кардиналы

- С помощью ординалов мы можем дать окончательное определение $|A|$ так, чтобы она была множеством.
- По теореме Цермело A можно вполне упорядочить. То есть A биективно какому-то ординалу.
- Тогда класс $\{\alpha | \alpha : Ord, A \sim \alpha\}$ непуст и имеет минимум. Этот минимум и есть $|A|$.
- Видно ли, что если $A \sim B$, то $|A| = |B|$, как и требуется?
- Все значения $|A|$ (то есть минимальные ординалы какой-то мощности) называются кардиналами.
- Они сами тоже вполне упорядочены.
- $\aleph_0$ это наименьший бесконечный кардинал, $\aleph_1$ это наименьший кардинал $> \aleph_0$, и так далее.
- Индексы алефов — ординалы, то есть для любого ординала α определено $\aleph_\alpha$.

Континуум-гипотеза

- Мы знаем, что $\mathfrak{c} > \aleph_0$, то есть $\mathfrak{c} \mathbin{?} \aleph_1$.

Континуум-гипотеза

- Мы знаем, что $\mathfrak{c} > \aleph_0$, то есть $\mathfrak{c} \geq \aleph_1$.

Континуум-гипотеза

- Мы знаем, что $\mathfrak{c} > \aleph_0$, то есть $\mathfrak{c} \geq \aleph_1$.
- Естественно предположить, что $\mathfrak{c} = \aleph_1$, то есть нет промежуточных мощностей между $\aleph_0$ и $\mathfrak{c}$.
- Это называется *континуум-гипотезой CH*.

Континуум-гипотеза

- Мы знаем, что $\mathfrak{c} > \aleph_0$, то есть $\mathfrak{c} \geq \aleph_1$.
- Естественно предположить, что $\mathfrak{c} = \aleph_1$, то есть нет промежуточных мощностей между $\aleph_0$ и $\mathfrak{c}$.
- Это называется *континуум-гипотезой CH*.
- Оказывается, что в *ZFC* это нельзя ни доказать, ни опровергнуть: есть модели *ZFC*, в которых $\mathfrak{c} = \aleph_1$, а есть такие, в которых $\mathfrak{c} = \aleph_2$, $\aleph_\omega$ и т.д.
- То же самое верно для *обобщённой континуум-гипотезы GCH*: $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ для всех α.

Континуум-гипотеза

- Мы знаем, что $\mathfrak{c} > \aleph_0$, то есть $\mathfrak{c} \geq \aleph_1$.
- Естественно предположить, что $\mathfrak{c} = \aleph_1$, то есть нет промежуточных мощностей между $\aleph_0$ и $\mathfrak{c}$.
- Это называется *континуум-гипотезой CH*.
- Оказывается, что в *ZFC* это нельзя ни доказать, ни опровергнуть: есть модели *ZFC*, в которых $\mathfrak{c} = \aleph_1$, а есть такие, в которых $\mathfrak{c} = \aleph_2$, $\aleph_\omega$ и т.д.
- То же самое верно для *обобщённой континуум-гипотезы GCH*: $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ для всех α.
- Проще найти модель, в которой *GCH* верна: это *конструктивный универсум L*, состоящий из таких множеств, которые можно определить с помощью формул *ZFC*, в которых используются только ранее сконструированные множества.

Трансфинитная иерархия всех множеств и конструктивная иерархия

- Универсум всех множеств V можно разбить на ранги:
  - $V_0 = \varnothing$.
  - $V_{\alpha+1} = \mathcal{P}(V_\alpha)$ — множество всех подмножеств V_α. Оно будет включать V_α.
  - Если λ предельный ординал, то $V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha$.
  - $V = \bigcup_{\alpha:Ord} V_\alpha$.
- При этом можно записать формулу *ZFC* $rk(X, \alpha)$, которая означает $X \in V_\alpha$.
- И можно доказать $\forall X \exists \alpha\ ord(\alpha) \wedge rk(X, \alpha)$ (то есть любое X имеет какой-то ранг α и является элементом V).

Трансфинитная иерархия всех множеств и конструктивная иерархия

- Универсум всех множеств V можно разбить на ранги:
  - $V_0 = \varnothing$.
  - $V_{\alpha+1} = \mathcal{P}(V_\alpha)$ — множество всех подмножеств V_α. Оно будет включать V_α.
  - Если λ предельный ординал, то $V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha$.
  - $V = \bigcup_{\alpha:Ord} V_\alpha$.
- При этом можно записать формулу ZFC $rk(X, \alpha)$, которая означает $X \in V_\alpha$.
- И можно доказать $\forall X \exists \alpha \; ord(\alpha) \wedge rk(X, \alpha)$ (то есть любое X имеет какой-то ранг α и является элементом V).
- Теперь определение L отличается только в одном:
  - $L_{\alpha+1}$ это множество не всех подмножеств L_α, а тех, которые можно определить формулой сигнатуры ZFC с параметрами из L_α и только с кванторами по L_α.
  - Вместо понятия определимости можно использовать фиксированный набор операций над элементами L_α.