Введение в математическую логику и теорию алгоритмов

Лекция 12

Алексей Львович Семенов

- Терминология
  - Содержательная теория множеств
  - Формальная теория множеств
- План
  - Полные порядки (ординал)
  - Аксиома выбора, связь с полными порядками
  - Формулировки некоторых следствий из Аксиомы выбора

Полные порядки
(содержательная теория множеств)

- Линейный порядок на классе A называется *полным*, если в любом непустом подклассе класса A имеется наименьший элемент, то есть $B \subset A$, B непусто $\Rightarrow \exists u\ (u \in B \wedge \forall v(v < u \to v \notin B))$.

  Класс A называется *вполне упорядоченным* (*ординалом*).
- Эквивалентное определение – в A нет бесконечной убывающей цепочки $a_0 > a_1 > a_2 >\ldots$.
- Примеры вполне упорядоченных классов:
  – конечный класс с любым линейным порядком,
  – класс натуральных чисел N.

Свойства полного порядка:

Полный порядок *A*

1. В A существует наименьший элемент – 0.
2. Всякий непустой подкласс A вполне упорядочен.
3. Для каждого не наибольшего x существует единственный непосредственно следующий за ним, то есть такой y, что $x < y$, но не существует такого z, что $x < z < y$.

Этот элемент y мы будем обозначать $x + 1$, и т. д.

Бывает и $x - 1$ … .

Элемент x, не являющийся наименьшим и не имеющий непосредственно предшествующего – *предельный*.

4. Всякий элемент вполне упорядоченного класса имеет вид n или $a + n$ для некоторого натурального n и предельного a.

   Доказательство. Цепочка $x > x - 1 > x - 2 > . . .$ не может быть бесконечной, она заканчивается предельным элементом или элементом 0.

Операции над упорядоченными классами
(арифметика ординалов)

Определение (повторно). Пусть A и B — два упорядоченных класса. Тогда $A \times B$ – это класс пар (a, b), где $a \in A, b \in B$, упорядоченный так:

$(a_0, b_0) < (a_1, b_1)$ если $b_0 < b_1$ или $b_0 = b_1$ и $a_0 < a_1$.

Если A и B — два непересекающихся упорядоченных класса, то $A + B$ – это объединение $A \cup B$, порядок на котором задан так:

если $a \in A$, $b \in B$, то $a < b$,

если a, $b \in A$ (a, $b \in B$) то порядок определяется порядком на A (соответственно, на B).

Свойства полного порядка (продолжение):

5. Если A и B — вполне упорядоченные классы, то классы $A + B$ и $A \times B$ вполне упорядочены.
6. Классы $N + k$, $N + N = N \times 2$, $k \times N$, $N \times k$ вполне упорядочены, здесь k — конечный порядок.

Обозначения

Порядок на натуральных числах

- 0, 1, 2,…
- Можно считать, что

  $0 = \varnothing$, $1 = \{\varnothing\}$, $2 = \{0,1\}$, $3 = \{0, 1, 2\}$,… .
- $\omega = \{0, 1, 2, 3,\ldots\}$,
- $\omega+1$, $\omega+2$, $\omega+3$, …, $\omega+\omega=\omega\times 2$, …, $\omega\times\omega=\omega^2$,
- ω^2+1, …, $\omega^2+\omega$, …, ω^3, …,
- ω^ω , …,
- ω^{ω^ω}, …
- Несчетные классы. Трансфинитные числа.

Начальные отрезки

Определение. Подкласс B вполне упорядоченного класса A называется *начальным отрезком* A, если вместе с каждым элементом он содержит и все меньшие, то есть $a \in B$, $b < a \Rightarrow b \in B$.

Свойства полного порядка (продолжение)

7. $[0, a)$ и $[0, a]$ являются начальными отрезками.
8. Любой начальный отрезок класса A, отличный от A, имеет вид $[0, a)$.
9. Объединение любого семейства начальных отрезков является начальным отрезком.

Определение. Подкласс B упорядоченного класса A *кофинален* классу A, если для любого $a \in A$ найдется такой $b \in B$, что $b \geq a$.

Трансфинитная индукция

- Индуктивные определения (при всех меньших…)
- Индуктивные доказательства (при всех меньших…)
- Возможны варианты шага в зависимости от того, предельный или непредельный элемент.

Теорема о возрастающем отображении

Пусть A *— вполне упорядоченный класс,*

$f : A \to A$ *— возрастающее отображение,*

то есть $a < b \;\Rightarrow\; f(a) < f(b)$.

Тогда $f(a) \geq a$ *для всех* $a \in A$,

образ $f(A)$ *кофинален* A.

Доказательство. Пусть a – наименьший элемент для которого $a > f(a)$. Тогда $f(a) > f(f(a))$ (возрастание f), т.е. $f(a)$ обладает тем же свойством и меньше a, противоречие.

Теорема о вложении полных порядков

- *Пусть A и B — два вполне упорядоченных класса. Тогда или A изоморфно некоторому начальному отрезку B, или B изоморфно некоторому начальному отрезку A, причем этот изоморфизм единствен.*

Теорема о вложении полных порядков

Доказательство. Назовем начальный отрезок I класса A *корректным*, если он изоморфен некоторому начальному отрезку класса B. Пусть I — корректный отрезок, а f_I — соответствующий изоморфизм, определенный на I.

• Тогда $f_I(0) = 0$ и для любого $a \in I$ $f_I([0, a))$ — начальный отрезок класса B. Значит: $f_I(a)$ = *наименьший элемент в* $\{b \mid b \in B, b \neq f_I(a')$ *для всех* $a' < a\}$. Поэтому $f_I(a)$ полностью определяется значениями f_I на меньших элементах. Отсюда по трансфинитной индукции следует, что для данного I такой изоморфизм единствен.

• Если J – начальный отрезок класса A, $J \subset I$, то J тоже корректный и (из единственности) $f_J = f_I$ на J.

• Пусть отрезок I_0 — объединение всех корректных начальных отрезков. Он корректен, поскольку отображение f — объединение всех f_I — будет требуемым изоморфизмом.

• Если $A = I_0$ или $B = f(I_0)$, то все доказано.

• Если $I_0 = [0, a)$ для некоторого $a \in A$ и $f(I_0) \neq B$, то доопределим отображение f на a, как *наименьший элемент класса* $B \setminus f(I_0)$, получим противоречие с тем, что отрезок $[0, a]$ уже не корректный.

Порядок на упорядоченных классах

Следствие. Любой подкласс B вполне упорядоченного класса A изоморфен начальному отрезку класса A.

Доказательство. Класс *A* не изоморфен собственному начальному отрезку класса *B*, поскольку такой отрезок не кофинален *A* (противоречие с теоремой о возрастающем отображении).

Определение. Класс *A* меньше класса *B* ($A < B$), если *A* изоморфно собственному начальному отрезку *B*.

Для любого *A* неверно $A < A$, поскольку требуемый изоморфизм единствен.

Любые два класса *A*, *B* или изоморфны, или $A < B$, или $B < A$.

Лемма. В любом непустом семействе вполне упорядоченных классов есть ”наименьший элемент”, изоморфный начальному отрезку любого другого элемента семейства.

Доказательство. Пусть *A* – элемент семейства и он не ”наименьший”, то есть найдутся элементы семейства, изоморфные $[0, a)$ при каких-то $a \in A$. Найдем наименьший среди таких элементов – a_0. Элемент, изоморфный $[0, a_0)$, будет наименьшим в семействе.

В теории ZF

Множество $R \subset a \times a$ – *порядок* на множестве a,

если задаваемое им отношение R:

(1) антисимметрично: $\forall u (u \in a \to \neg R(u, u))$,

(2) транзитивно: $\forall u,v,w\, (R(u, v) \wedge R(v,w) \to R(u,w))$

(вместо $R(u, v)$ будем писать $u < v$).

Порядок *линеен*, если

(3) $\forall u,v\, (u \in a \wedge v \in a \to ((u = v) \vee (u < v) \vee (v < u)))$.

Порядок *фундирован*, если

(4) $\forall u\, (u \subset a \wedge u \neq \varnothing \to$

$\to \exists v (v \in u \wedge \forall w (w < v \to w \notin u)))$.

Порядок *полон*, если выполнены и (3), и (4).

Функция выбора

Определение. Пусть a – множество, а f – функция, причем $Dom(f) = P(a)\setminus\{\varnothing\}$, $Ra(f) \subset a$. Пусть $f(x) \in x$ для любого $x \subset a$, $x \neq \varnothing$. Тогда f называется *функцией выбора.*

Если множество может быть вполне упорядочено, то для него есть функция выбора: в множестве x выбираем наименьший элемент.

Эрнст Цермело

27 07 1871 — 21 05 1953

Теорема Цермело. Если для множества существует функция выбора, то оно может быть вполне упорядоченно.

Доказательство. Пусть a – некоторое множество, f – функция выбора для a. Определим функцию (выбора в дополнении) g: $P(a) \setminus \{a\} \rightarrow a$

так, что $g(x) = f(a \setminus x)$.

Тогда $\forall u\, (u \subset a \wedge u \neq a \rightarrow g(u) \in a \setminus u)$.

Пусть $b \subset a$, $<_b$ — порядок на b. Пару $< b <_b >$ будем называть корректной, если

(1) порядок $<_b$ полный и

(2) $\forall u\, (u \in b \rightarrow u = g(\{v \mid v \in b,\, v <_b u\}))$ (то есть функция g получает u из всех его $<_b$ -меньших).

Лемма. Корректные пары согласованы, то есть, если $< b <_b >$ и $< c <_c >$ – корректные пары, то одна из них является начальным отрезком другой. *(g – фиксирована, получает элемент из всех меньших.)*

Д. По теореме о вложении полных порядков существует изоморфизм h, отображающий (например) множество b на начальный отрезок c. Докажем, что тогда $h(x) = x$ трансфинитной индукцией по элементам b.

Ясно, что h переводит наименьший элемент b в наименьший элемент c. Но оба этих элемента – это $g(\varnothing)$.

Пусть d – произвольный элемент множества b, и отрезки $[0, d)$ и $[0, h(d))$, как и отношения $<_b$ и $<_c$ на них совпадают по индуктивному предположению.

Но $d = g(\{x \mid x <_b d\})$ и $h(d) = g(\{x \mid x <_c h(d)\})$, значит $d = h(d)$. *Лемма доказана.*

Теорема Цермело. Если для множества существует функция выбора, то оно может быть вполне упорядоченно.

Продолжение доказательства.

- Пусть $S = \{< b, r > \mid < b, r > - \textit{корректная пара}\}$.
- $U = Un\{b \mid \exists u(< b, u > \in S)\}$ порядок на U –

$x < y \Leftrightarrow x <_b y$ для некоторого порядка $< b <_b > \in S$.

- Это полный порядок, поскольку если $x \subset U$, $x \neq \varnothing$,

то $x \cap b \neq \varnothing$ для некоторого b, и наименьший (в смысле порядка $<_b$) элемент в этом пересечении будет наименьшим элементом x.

- Если $U \neq a$, то доопределим порядок на $U \cup \{g(U)\}$, положив $x < g(U)$ для любого $x \in U$.
- Получим корректную пару, что противоречит определению U, т. к. $g(U)$ *не входит в* U.

Аксиома выбора

Для любого множества существует функция выбора, формально:

$$\forall \boldsymbol{u}\, \exists \boldsymbol{f}\, (\boldsymbol{Func}(\boldsymbol{f}) \wedge \boldsymbol{Dom}(\boldsymbol{f}) = \boldsymbol{P}(\boldsymbol{u}) \setminus \{\varnothing\} \wedge \forall \boldsymbol{v}\, (\boldsymbol{v} \in \boldsymbol{Dom}(\boldsymbol{f}) \rightarrow \boldsymbol{f}\,(\boldsymbol{v}) \in \boldsymbol{v})).$$

- Теория, полученная добавлением к **ZF** аксиомы выбора, обозначается **ZFC**.
- С этого момента мы рассматриваем модели этой теории.

Парадокс Банаха – Тарского

Т. Шар можно разбить на пять частей, передвинув которые можно сложить (без пустот и пересечений) два шара такого же радиуса.

Сте́фан Ба́нах
30.03.1892 —
31.08.1945

Детерминированность игр

Игра Банаха – Мазура

- Отрезок [0;1]. Два игрока: I и II.
- *A* – множество выигрыша для I.
- Поочередно в [0;1] выбирают отрезки $S_{n+1} \subseteq S_n$.
- Первый выигрывает, если в пересечении всех отрезков найдется точка из *A.*
- В противном случае выигрывает второй.
- О. Стратегия. Выигрышная стратегия.
- **Аксиома детерминированности игр**. Во всякой игре Банаха – Мазура один из игроков имеет выигрышную стратегию.
- Из **АС** вытекает <u>отрицание</u> аксиомы детерминированности игр.

- Лекция 12
  – Полные порядки
  – Аксиома выбора, связь с полными порядками
  – Формулировки некоторых следствий из Аксиомы выбора