Введение в математическую логику и теорию алгоритмов

Лекция 14

Алексей Львович Семенов

План

- Система аксиом Теории множеств ZF
- Сокращения
- Натуральные числа

Построение математики

- Язык для записи математических утверждений
  - Логика отношений.
- Исчисление.
  - Правильная система математических аксиом.
  - Правила вывода – исчисление логики отношений
- Обоснование полноты системы аксиом?
  - Теорема Гёделя о неполноте.
- Обоснование непротиворечивости системы аксиом?
  - Вторая теорема Гёделя: невозможность доказать непротиворечивость даже в самом исчислении

Теория множеств Цермело – Френкеля ZF

- Сигнатура **ZF** = {=, ∈}, $a \in b$
- *Множество* – {b из $M \mid M \models b \in a$ для некоторого a из M }
- **Задача.** Может ли сама структура M быть множеством?

Эрнст Цермело

27 07 1871 — 21 05 1953

Абрахам Фре́нкель

(17.02.1891 – 15.10.1965)

Аксиомы ZF

- $\exists s \forall v (v \in s \equiv \Phi(v))$
  Можно ли для каждой формулы $\Phi(x)$ добавить такую аксиому?
- $\Phi(x) = x \notin x$
  $\exists s \forall v (v \in s \equiv v \notin v)$
  $s = \{ v \mid v \notin v \}$
- $s \in s \Leftrightarrow s \notin s$
- парадокс Рассела
  $\{x \mid x \notin x\}$ – не (образуют) множество

Аксиомы ZF

- Четыре типа (схемы) аксиом существования множеств
- *Аксиомы подмножеств*
  $\forall t \forall u \exists s \forall v (v \in s \equiv (v \in u \wedge \Phi(t,v)))$,

t – цепочка $t_1,\ldots, t_n$

- для любой формулы $\Phi(y, x)$
  $\{x | x \in a, \Phi(b, x)\}$ – множество

Аксиомы ZF

- *Аксиомы замены*
- $\forall t(\forall u \exists v \forall w(w \in v \equiv \Phi(t, u, w)) \rightarrow$
  $\rightarrow \forall v \exists s \forall w(\exists u(u \in v \wedge \Phi(t,u,w)) \equiv w \in s)$)

Чтобы понять, что это значит, рассмотрим случай без t:

- $\forall u \exists v \forall w(w \in v \equiv \Phi(u, w)) \rightarrow$
  $\rightarrow \forall z \exists s \forall w(\exists u(u \in z \wedge \Phi(u,w)) \equiv w \in s)$
- Если для всякого u формула $\Phi(u,w)$ задает множество v элементов w, то из всякого множества z выберем элементы w, находящиеся в отношении $\Phi(u,w)$ с каким-то u из z . Все эти элементы образуют множество s.
- $\Phi(t, x, y) \Leftrightarrow F_t(x) = \{y \mid \Phi(t, x, y)\}$
  для любого x, $F_t(x)$ – множество $\Rightarrow$
  $\Rightarrow$ для любого a, $\{y \mid x \in a, y \in F_t(x)\}$ – множество

Аксиомы ZF

- *Акисома степени*
  $\forall u \exists s \forall v (\forall w (w \in v \rightarrow w \in u) \equiv v \in s)$

Обозначение $x \subset y \Leftrightarrow \forall u (u \in x \rightarrow u \in y)$

- Аксиома означает, что $\{x | x \subset a\}$ – множество

Аксиомы ZF

- *Аксиома бесконечности*
  $\exists s(\exists u(u \in s \wedge \forall v(v \notin u)) \wedge$

$\wedge \forall u(u \in s \rightarrow \exists v(v \in s \wedge \forall w(w \in v \equiv (w \in u \vee w = u)))))$

- **3**. Что это значит содержательно?
- Аксиомы существования закончились

Аксиомы ZF

- *Аксиома объемности*
  $\forall u, v\ (\forall w(w \in u \equiv w \in v) \rightarrow u = v)$
- Описываемая структура – класс всех ”чистых” множеств. Множество полностью определяется своими элементами (тоже множествами).

Аксиомы ZF

- *Аксиома регулярности (фундирования)*
  $\forall u(\exists v(v \in u) \rightarrow \exists v(v \in u \wedge \neg\exists w(w \in v \wedge w \in u)))$
- Не бывает бесконечных цепочек
  $\cdots \in a_n \in a_{n-1} \in \cdots \in a_2 \in a_1$
- Мы не будем использовать эту аксиому

Аксиомы ZF

- *У нас были аксиомы:*
- *Аксиома пустого множества*
  $\exists s \forall u (u \notin s)$
- *Аксиома пары*

$\forall u, v\ \exists s \forall w (w \in s \equiv (w = u \vee w = v))$ $\{x | x = a \vee x = b\}$

- Без них можно обойтись (вывести их из других)

- Мы считаем, что у теории **ZF** есть модель.
- выражение **ZF** $\models \Phi$ обозначает, что утверждение Φ следует из теории **ZF**, то есть утверждение Φ истинно во всех моделях теории **ZF**.

Обозначения и сокращения

- $\exists!u\,\Phi(u)$ сокращение для
  $\exists u(\Phi(u) \wedge \forall v(\Phi(v) \rightarrow u = v))$ **ZF** $\models \exists!s\forall u(u \notin s)$
- Пустое множество $\emptyset$
- $\emptyset \in x$ сокращение для
  $\exists u(\forall v(v \notin u) \wedge u \in x)$ или
  $\forall u\,(\forall v\,(v \notin u\,) \rightarrow u \in x\,)$

Обозначения и сокращения

- Если **ZF** $\models \forall u \exists! v \Phi(u, v)$, то можно ввести операцию $\phi(x)$: $y \in \phi(x)$ сокращение для $\exists u(\Phi(x, u) \wedge y \in u)$ или $\forall u(\Phi(x, u) \rightarrow y \in u)$
  $y = \phi(x) \Leftrightarrow \Phi(x,y)$
- **ZF** $\models \forall u \exists! s \forall v(v \subset u \equiv v \in s)$
  $P(x) = y \Leftrightarrow \forall v(v \subset x \equiv v \in y)$
  $P(x)$ – множество подмножеств x
- **ZF** $\models \forall u, v \exists! s \forall w(w \in s \equiv (w = u \vee w = v))$
- $\{x, y\}$ – (неупорядоченная) пара множеств x и y
  $\{x\}$ – обозначение для $\{x, x\}$

Обозначения и сокращения

- $Un(x) = \{y \mid \exists u(y \in u \wedge u \in x)\}$ – *объединение* множества x
  3. Существование и единственность:
  Аксиома замены при $\Phi(t, x, y) = y \in x$
  ZF $\vDash \forall x \exists s \forall y(\exists u(u \in x \wedge y \in u) \equiv y \in s)$
- $x \cup y$ – сокращение для $Un(\{x, y\})$
  $x \cap y$ – *пересечение*: $\{z \mid z \in x \wedge z \in y\}$
- $x \setminus y$ – *разность*: $\{z \mid z \in x \wedge z \notin y\}$
- $< x, y >$ – *упорядоченная пара*: $\{\{x\}, \{x, y\}\}$

$<x,y>=<x',y'> \Leftrightarrow x=x' \wedge y=y'$

- Упорядоченная тройка $< x, y, z >=< x, < y, z >>$

Обозначения и сокращения

- *(Декартово) произведение*
  $x \times y = \{z \mid \exists u,v(u \in x \wedge v \in y \wedge z =< u,v >)\}$
- **Задача.** $a \in x \times y \Rightarrow a \in P(P(x \cup y))$, произведение - множество
- *Функция f* (*Func*(*f*)): множество пар $< a, b >$
  $\forall u, v, w\ (< u, v > \in f \wedge < u, w > \in f \rightarrow v = w)$
- *Область определения* (*Dom*(*f*)) $= \{z \mid \exists u(< z, u > \in f)\}$
  Мнаожество значений (*Ra*(*f*)) $= \{z \mid \exists u(< u, z > \in f)\}$
- **Задача.** Почему область определения и множество значений функции – множества?
- $f(x) = y \Leftrightarrow < x, y > \in f$

Множество ω

- 0;1;2;... = ∅;{∅};{∅,{∅}};...
- Следующий элемент: $S(x) = x \cup \{x\}$
  Аксиома бесконечности: $\exists s(\exists u(u \in s \wedge \forall v(v \notin u)) \wedge$
  $\wedge \forall u(u \in s \rightarrow \exists v(v \in s \wedge \forall w(w \in v \equiv (w \in u \vee w = u)))))$
- Иначе: $\exists s(\emptyset \in s \wedge \forall u(u \in s \rightarrow S(u) \in s))$
- *О. s – ”бес-конечное”* множество $\Leftrightarrow \emptyset \in s \wedge \forall u(u \in s \rightarrow S(u) \in s)$
  Задача. Пересечение ”бес-конечных” множеств ”бес-конечно”
- $\omega = \{x | \forall s((\emptyset \in s \wedge \forall u(u \in s \rightarrow S(u) \in s)) \rightarrow x \in s)\}$
  ω – множество , единственно и ”бес-конечно”.
- *b* – ”бес-конечно” $\Rightarrow \omega \subset b$

Множество ω

- *Правило индукции:* **ZF** $\vDash \forall u(u \subset \omega \wedge u \neq \emptyset \rightarrow$
  $\rightarrow (0 \in u \vee \exists v(v \in \omega \wedge v \notin u \wedge S(v) \in u)))$
  Д-во. Пусть для какого-то $a \subset \omega$ это не так;
  возьмем $b = \omega \setminus a$; b – множество.
  $0 \in b \wedge \forall u(u \in b \rightarrow S(u) \in b) \Rightarrow$
  b – ”бес-конечно” $\Rightarrow \omega \subset b \Rightarrow a = \emptyset$
- $k,l,m,n\cdots$обозначают элементы ω
  $n < m \Leftrightarrow n \in m$; $S(m) = m \cup \{m\}$
- **Задачи.**
- (0) $n = 0 \vee n = S(m)$
  Решение. От противного.
- $\{n \in \omega \mid n \neq 0 \wedge \forall v(v \in \omega \rightarrow n \neq S(v))\} = a$ – множество, $a \subset \omega$.
  Правило индукции:
  $0 \in a \vee \exists v(v \in \omega \wedge v \notin a \wedge S(v) \in a)$. Противоречие

Множество ω

Обозначение: $n < m \Leftrightarrow n \in m$;

Обозначение: $x \not\subset y$ надо понимать как $\neg(x \subset v)$

Задачи.

(1) $n < S(n)$ (определение)
(2) $b \in n \rightarrow b \subset n$
Решение. $\{n \in \omega \mid \exists x(x \in n \wedge x \not\subset n)\} = a$;
$0 \notin a$, $m \notin a$, $S(m) \in a$, $b \in S(m)$, $b \not\subset S(m)$
(i) $b = m$. Противоречие.
(ii) $b \in m \Rightarrow b \subset m \subset S(m)$. Противоречие.

(3)порядок транзитивен: $n<m \wedge m<k \rightarrow n<k$ из (2)

(4) $\neg(n < n)$ (индукция)
(5) $0 < S(n)$ (индукция)
(6) $n < m \rightarrow m = S(n) \vee S(n) < m$ (индукция по m)

(7)порядок линеен: $n<m \vee n=m \vee m<n$(индукция по ...)

Рекурсия

- (8) $a \subset \omega, a \neq \emptyset \Rightarrow \exists b(b \in a \wedge \forall c(c < b \rightarrow c \notin a))$
  Указание. $a' = \{u \in \omega | \exists x(x \in a \wedge x \ ? \ u)\}$
- **Обозначения**. $x + 1 \Leftrightarrow S(x)$; x-1... $[n, m] \Leftrightarrow \{k | k \in \omega, n \ ? \ k \ ? \ m\}$
- Сложение – функция $\Sigma: \omega \times \omega \rightarrow \omega$
  (0) $\Sigma(< n, 0 >) = n$
  (1) $\Sigma(< n, m + 1 >) = \Sigma(< n, m >) + 1$
  Докажем, что существует и единственна функция, удовлетворяющая (0) и (1)
- $k \in \omega$ *корректен* $\Leftrightarrow \exists \Sigma k(\Sigma k : \omega \times [0, k] \rightarrow \omega)$. Пусть m — наименьший некорректный элемент.
- $\Sigma m = \Sigma m-1 \cup \{<n,m,\Sigma m-1(n,m-1)+1> | n \in \omega\}$. Противоречие. Единственность Σk.
  $k<k' \Rightarrow \Sigma k \subset \Sigma k'$.
- $\Sigma = Un\{\Sigma k | k \in \omega\}$ – функция (аксиома замены).
  $n + m = \Sigma(< n, m >)$

Числа

- Умножение П: $\omega \times \omega \to \omega$
  (0) $П(< n, 0 >) = 0$
  (1) $П(< n, m + 1 >) = П(< n, m >) + n$
- Целые числа $Z_M = \{<0,n> | n \in \omega\} \cup \{<1,n> | n \in \omega \setminus \{0\}\}$
- Рациональные числа
  $Q_M = \{a \subset Z_M \times \omega \setminus \{0\} | a$ – класс эквивалентности$\}$
  – $<x_1,x_2> \sim <y_1,y_2> \Leftrightarrow x_1y_2 = x_2y_1$
- Действительные числа
  $R_M = \{<a,b> | a \subset Q_M, b \subset Q_M, <a,b>$ – дедекиндово сечение$\}$