Введение в математическую логику и теорию алгоритмов

Лекция 14
Теория множеств

Алексей Львович Семенов

Язык для записи математических утверждений
Логика отношений.

Истинность теории, следование
Структуры, модели. Перечислимость следования.
Теорема о полноте.

Правильная система математических аксиом.
?

Обоснование непротиворечивости системы аксиом.
Вторая теорема Гёделя.

Обоснование полноты системы аксиом.
Теорема Гёделя о неполноте.

Теория множеств Цермело – Френкеля ZF

Сигнатура **ZF** $= \{=, \in\}$

Мы будем использовать запись $a \in b$

Множество, подмножество, функция **vs.** класс, набор, совокупность, подкласс, отображение

Множество – $\{b \in M |$ для некоторого $a \in M, M \models b \in a\}$

Задача. Может ли сама структура M быть множеством?

Аксиомы ZF

$\exists s \forall v (v \in s \equiv \Phi(v))$
Можно ли для каждой формулы $\Phi(x)$ добавить такую аксиому?

$\Phi(x) = x \notin x$
$\exists s \forall v (v \in s \equiv v \notin v)$
$s = \{v | v \notin v\}$
$s \in s \Leftrightarrow s \notin s$

парадокс Рассела
$\{x | x \notin x\}$ – не множество

Аксиомы ZF

Четыре типа аксиом существования множеств
Аксиомы подмножеств

$$\forall \bar{t} \forall u \exists s \forall v (v \in s \equiv (v \in u \wedge \Phi(\bar{t}, v)))$$

$\bar{t}$ – вектор $t_1, \ldots, t_n$

для любой формулы $\Phi(\bar{y}, x)$

$\{x | x \in a, \Phi(\bar{b}, x)\}$ – множество

Аксиомы ZF

Аксиомы замены

$$\forall \bar{t}($$
$$\forall u \exists v \forall w (w \in v \equiv \Phi(\bar{t}, u, w)) \to$$
$$\to \forall v \exists s \forall w (\exists u (u \in v \wedge \Phi(\bar{t}, u, w)) \equiv w \in s)$$
$$)$$

$\Phi(\bar{t}, x, y) \Leftrightarrow F_{\bar{t}}(x) = \{y | \Phi(\bar{t}, x, y)\}$
для любого $x, F_{\bar{t}}(x)$ – множество $\Rightarrow$
$\Rightarrow$ для любого $a, \{y | x \in a, y \in F_{\bar{t}}(x)\}$ – множество

Аксиомы ZF

Аксиома степени

$$\forall u \exists s \forall v (\forall w (w \in v \to w \in u) \equiv v \in s)$$

$x \subset y \Leftrightarrow \forall u (u \in x \to u \in y)$

$\{x | x \subset a\}$ – множество

Аксиомы ZF

Аксиома бесконечности

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

Аксиомы ZF

Аксиома регулярности (фундирования)

$$\forall u(\exists v(v \in u) \to \exists v(v \in u \wedge \neg\exists w(w \in v \wedge w \in u)))$$

не бывает цепочек $\cdots \in a_n \in a_{n-1} \in \cdots \in a_2 \in a_1$

Мы не будем использовать данную аксиому

Аксиомы ZF

Аксиома объемности

$$\forall u, v(\forall w(w \in u \equiv w \in v) \to u = v)$$

Описываемая структура – класс всех ”чистых” множеств

Аксиомы ZF

Аксиома пустого множества

$$\exists s \forall u (u \notin s)$$

Аксиома пары

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

$\{x | x = a \vee x = b\}$ – множество

Предварительные замечания и соглашения

Мы считаем, что у теории **ZF** есть модель.

$\exists! u \Phi(u)$ сокращение $\exists u(\Phi(u) \wedge \forall v(\Phi(v) \to u = v))$

ZF $\models \exists! s \forall u(u \notin s)$

Пустое множество $\varnothing$

$\varnothing \in x$ сокращение для $\exists u(\forall v(v \notin u) \wedge u \in x)$ или
$\forall u(\forall v(v \notin u) \to u \in x)$

Предварительные замечания и соглашения

Если **ZF** $\vDash \forall \overline{u} \exists ! v \Phi(\overline{u}, v)$, то можно ввести $\varphi(\overline{x})$

$y \in \varphi(\overline{x})$ сокращение для $\exists u(\Phi(\overline{x}, u) \wedge y \in u)$ или

$\forall u(\Phi(\overline{x}, u) \rightarrow y \in u)$

$y = \varphi(\overline{x}) \Leftrightarrow \Phi(\overline{x}, y)$

ZF $\vDash \forall u \exists ! s \forall v(v \subset u \equiv v \in s)$

$P(x) = y \Leftrightarrow \forall v(v \subset x \equiv v \in y)$

$P(x)$ – множество подмножеств x

ZF $\vDash \forall u, v \exists ! s \forall w(w \in s \equiv (w = u \vee w = v))$

$\{x, y\}$ – (неупорядоченная) пара множеств x и y

$\{x\}$ – обозначение для $\{x, x\}$

Предварительные замечания и соглашения

$Un(x) = \{y | \exists u (y \in u \wedge u \in x)\}$ – *объединение* множества x
Аксиома замены при $\Phi(\bar{t}, x, y) = y \in x$
ZF $\models \forall v \exists s \forall w (\exists u (u \in v \wedge w \in u) \equiv w \in s)$

$x \cup y$ – сокращение для $Un(\{x, y\})$
$x \cap y$ – *пересечение*: $\{z | z \in x \wedge z \in y\}$
$x \setminus y$ – *разность*: $\{z | z \in x \wedge z \notin y\}$
$< x, y >$ – *упорядоченная пара*: $\{\{x\}, \{x, y\}\}$

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

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

Предварительные замечания и соглашения

Декартово произведение
$x \times y = \{z | \exists u, v(u \in x \wedge v \in y \wedge z =< u, v >)\}$
Задача. $a \in x \times y \Rightarrow a \in P(P(x \cup y))$

Функция f (*Func*(*f*)): множество пар $< a, b >$
$\forall u, v, w(< u, v >\in f \wedge < u, w >\in f \to v = w)$

Область определения $(Dom(f)) = \{z | \exists u(< z, u >\in f)\}$
Область значения $(Ra(f)) = \{z | \exists u(< u, z >\in f)\}$

Задача. Почему область определения и область значения функции – множества?

$f(x) = y \Leftrightarrow < x, y >\in f$

Множество ω

$0; 1; 2; \ldots$ – $\varnothing; \{\varnothing\}; \{\varnothing, \{\varnothing\}\}; \ldots$
Следующий элемент: $S(x) = x \cup \{x\}$

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

$\exists s(\varnothing \in s \wedge \forall u(u \in s \rightarrow S(u) \in s))$

s – *"бесконечное"* множество $\Leftrightarrow$
$\varnothing \in s \wedge \forall u(u \in s \rightarrow S(u) \in s)$
Задача. Пересечение "бесконечных" множеств "бесконечно"

$\omega = \{x | \forall s((\varnothing \in s \wedge \forall u(u \in s \rightarrow S(u) \in s)) \rightarrow x \in s)\}$
ω – множество , единственно и "бесконечно".
b – "бесконечно" $\Rightarrow \omega \subset b$

Множество ω

Правило индукции: **ZF** $\models \forall u(u \subset \omega \wedge u \neq \varnothing \rightarrow$
$\rightarrow (0 \in u \vee \exists v(v \in \omega \wedge v \notin u \wedge S(v) \in u)))$
Д-во. $a \subset \omega; b = \omega \setminus a; b$ – множество.
$0 \in b \wedge \forall u(u \in b \rightarrow S(u) \in b) \Rightarrow b$ – ”бесконечно”
$\Rightarrow \omega \subset b$

$k, l, m, n \dots \in \omega$
$n < m \Leftrightarrow n \in m$; $S(m) = m \cup \{m\}$

Задачи.
(0) $n = 0 \vee n = S(m)$
Решение. От противного. Правило индукции.
$\{n \in \omega | n \neq 0 \wedge \forall v(v \in \omega \rightarrow n \neq S(v))\} = a$ – 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

$n < m \Leftrightarrow n \in m$; $S(m) = m \cup \{m\}$

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

(3) порядок транзитивен: $n < m \wedge m < k \to n < k$ (2)
(4) $\neg(n < n)$ (индукция или аксиома регулярности)
(5) $0 < S(n)$ (индукция)
(6) $n < m \to m = S(n) \vee S(n) < m$ (индукция по m)
(7) порядок линеен: $n < m \vee n = m \vee m < n$ (индукция по ...)

Рекурсия

(8) $a \subset \omega, a \neq \varnothing \Rightarrow \exists b(b \in a \wedge \forall c(c < b \to c \notin a))$
Указание. $a' = \{u \in \omega | \exists x(x \in a \wedge x \leqslant u)\}$

$x + 1 \Leftrightarrow S(x)$; $[n, m] \Leftrightarrow \{k | k \in \omega, n \leqslant k \leqslant m\}$

Сложение – функция $\Sigma\colon \omega \times \omega \to \omega$
(0) $\Sigma(< n, 0 >) = n$
(1) $\Sigma(< n, m + 1 >) = \Sigma(< n, m >) + 1$
Д-во. $k \in \omega$ *корректен* $\Leftrightarrow \exists \Sigma_k(\Sigma_k\colon \omega \times [0, k] \to \omega)$.
m — наименьший некорректный элемент.
$\Sigma_m = \Sigma_{m-1} \cup \{< n, m, \Sigma_{m-1}(n, m-1) + 1 > | n \in \omega\}$.
Противоречие.
Единственность Σ_k.
$k < k' \Rightarrow \Sigma_k \subset \Sigma_{k'}$.
$\Sigma = Un\{\Sigma_k | k \in \omega\}$ – функция (аксиома замены).
$n + m \Leftrightarrow \Sigma(< n, m >)$

Рекурсия

$\Pi\colon \omega \times \omega \to \omega$
(0) $\Pi(< n, 0 >) = 0$
(1) $\Pi(< n, m+1 >) = \Pi(< n, m >) + n$

$\mathbb{Z}_M = \{< 0, n > | n \in \omega\} \cup \{< 1, n > | n \in \omega \setminus \{0\}\}$

$\mathbb{Q}_M = \{a \subset \mathbb{Z}_M \times \omega \setminus \{0\} | a$ – класс эквивалентности$\}$
$< x_1, x_2 > \sim < y_1, y_2 > \Leftrightarrow x_1 y_2 = x_2 y_1$

$\mathbb{R}_M = \{< a, b > | a \subset \mathbb{Q}_M, b \subset \mathbb{Q}_M, < a, b >$
– Дедекиндово сечение$\}$