

Теория множеств

Теория множеств

1. Георг Кантор: 1877 год, «наивная теория множеств». Множество — это «объединение в одно целое объектов, хорошо различаемых нашей интуицией или нашей мыслью».
2. Неограниченный принцип абстракции $\{x \mid P(x)\}$
3. Парадокс Бурали-Фортэ (1895, Кантор). Парадокс Рассела: $X := \{x \mid x \notin x\}$; $X \in X$?
4. Вариант решения парадокса: а, может, запретить все «опасные» ситуации?
5. Аксиоматика Цермело — 1908 год, оставим только то, что используют математики.
6. Что такое множество? Неформально мы понимаем, формально:

Определение

Теория множеств — теория первого порядка, с дополнительным нелогическим двухместным функциональным символом \in , и следующими дополнительными нелогическими аксиомами и схемами аксиом

Аксиоматика ZF, равенство

Определение

Равенство «по Лейбницу»: объекты равны, если неразличимы.

Если нечто ходит как утка, выглядит как утка и крякает как утка, то это утка.

Определение

Принцип объёмности: объекты равны, если состоят из одинаковых частей

Определение

$$A \subseteq B \equiv \forall x. x \in A \rightarrow x \in B$$

$$A = B \equiv A \subseteq B \ \& \ B \subseteq A$$

Определение

Аксиома равенства: равные множества содержатся в одних и тех же множествах. $\forall x. \forall y. \forall z. x = y \ \& \ x \in z \rightarrow y \in z$.

Аксиоматика ZF, конструктивные аксиомы

Определение

Аксиома пустого. Существует пустое множество \emptyset .

$$\exists s. \forall t. \neg t \in s$$

Определение

Аксиома пары. Существует $\{a, b\}$. Каковы бы ни были два множества a и b , существует множество, состоящее в точности из них.

$$\forall a. \forall b. \exists s. a \in s \ \& \ b \in s \ \& \ \forall c. c \in s \rightarrow c = a \vee c = b$$

Аксиоматика ZF, конструктивные аксиомы 2

Определение

Аксиома объединения: существует $\cup x$. Для любого непустого множества x найдется такое множество, состоящее в точности из тех элементов, из которых состоят элементы x .

$$\forall x. (\exists y. y \in x) \rightarrow \exists p. \forall y. y \in p \leftrightarrow \exists s. y \in s \ \& \ s \in x$$

Определение

Аксиома степени: существует $\mathcal{P}(x)$. Каково бы ни было множество x , существует множество, содержащее в точности все возможные подмножества множества x .

$$\forall x. \exists p. \forall y. y \in p \leftrightarrow y \subseteq x$$

Аксиоматика ZF. Схема аксиом выделения

Определение

Схема аксиом выделения: существует $\{t \in x \mid \varphi(t)\}$. Для любого множества x и любой формулы от одного аргумента $\varphi(y)$ (b не входит свободно в φ), найдется b , в которое входят те и только те элементы из множества x , что $\varphi(y)$ истинно.

$$\forall x. \exists b. \forall y. y \in b \leftrightarrow (y \in x \ \& \ \varphi(y))$$

Немного теорем

Теорема

Для любого множества X существует множество $\{X\}$, содержащее в точности X .

Доказательство.

Воспользуемся аксиомой пары: $\{X, X\}$



Теорема

Пустое множество единственно.

Доказательство.

Пусть $\forall p. \neg p \in s$ и $\forall p. \neg p \in t$. Тогда $s \subseteq t$ и $t \subseteq s$.



Теорема

Для двух множеств s и t существует множество, являющееся их пересечением.

Доказательство.

$$s \cap t = \{x \in s \mid x \in t\}$$



Упорядоченная пара

Определение

Упорядоченная пара. Упорядоченной парой двух множеств a и b назовём $\{\{a\}, \{a, b\}\}$, или $\langle a, b \rangle$

Теорема

Упорядоченную пару можно построить для любых множеств.

Доказательство.

Применить аксиому пары, теорему о существовании $\{X\}$, аксиому пары. □

Теорема

$\langle a, b \rangle = \langle c, d \rangle$ тогда и только тогда, когда $a = c$ и $b = d$.

Аксиома бесконечности

Определение

Инкремент: $x' \equiv x \cup \{x\}$

Определение

Аксиома бесконечности. Существует

$$N : \emptyset \in N \ \& \ \forall x. x \in N \rightarrow x' \in N$$

В N есть всевозможные множества вида $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots$

(неформально) $\omega = \{\emptyset, \emptyset', \emptyset'', \dots\}$. Тогда

$N_1 = \omega \cup \{\omega, \omega', \omega'', \dots\}$ подходит.

Полный порядок (вполне упорядоченные множества)

1. Частичный: рефлексивность ($a \preceq a$), антисимметричность ($a \preceq b \rightarrow b \preceq a \rightarrow a = b$), транзитивность ($a \preceq b \rightarrow b \preceq c \rightarrow a \preceq c$).
2. Линейный: частичный + $\forall a. \forall b. a \preceq b \vee b \preceq a$.
3. Полный: линейный + в любом непустом подмножестве есть наименьший элемент.

Пример

\mathbb{Z} не вполне упорядочено: в \mathbb{Z} нет наименьшего.

Пример

Отрезок $[0, 1]$ не вполне упорядочен: $(0, 1)$ не имеет наименьшего.

Пример

\mathbb{N} вполне упорядочено.

Ординалы (порядковые числа)

Определение

Транзитивное множество X : $\forall x. \forall y. x \in y \ \& \ y \in X \rightarrow x \in X$.

Определение

Ординал (порядковое число) — вполне упорядоченное отношением (\in) транзитивное множество.

Пример

Ординалы: $\emptyset, \emptyset', \emptyset'', \dots$

Определение

Предельный ординал: такой x , что $x \neq \emptyset$ и нет $y : y' = x$

Определение

Ординал x конечный, если он меньше любого предельного.

Теорема

Если x, y — ординалы, то $x = y$, или $x \in y$, или $y \in x$.

Предельные ординалы, ω

Определение

ω — наименьший предельный ординал.

Теорема

ω существует.

Доказательство.

Пусть $\omega = \{x \in N \mid x \text{ конечен}\}$. Пусть θ таков, что $\theta \in \omega$. Тогда θ конечен. Пусть θ таков, что $\theta' = \omega$. Тогда $\theta \in \omega$. \square

Пример

ω' — тоже ординал.

Операции над ординалами

Определение

$\sup x$ — наименьший ординал, содержащий x : $x \subseteq \sup x$.

Пример

$$\sup\{\emptyset', \emptyset'', \emptyset'''\} = \{\emptyset, \emptyset', \emptyset'', \emptyset''', \emptyset''''\} = \emptyset''''$$

$$a + b \equiv \begin{cases} a, & b \equiv \emptyset \\ (a + c)', & b \equiv c' \\ \sup\{a + c \mid c \prec b\}, & b \text{ — предельный ординал} \end{cases}$$

Пример

$$\omega + 1 = \omega \cup \{\omega\}; \quad 1 + \omega = \sup\{1 + \emptyset, 1 + 1, 1 + 2, \dots\} = \omega$$

Ещё операции над ординалами

$$a \cdot b \equiv \begin{cases} 0, & b \equiv \emptyset \\ (a \cdot c) + a, & b \equiv c' \\ \sup\{a \cdot c \mid c \prec b\}, & b \text{ — предельный ординал} \end{cases}$$

$$a^b \equiv \begin{cases} 1, & b \equiv \emptyset \\ (a^c) \cdot a, & b \equiv c' \\ \sup\{a^c \mid c \prec b\}, & b \text{ — предельный ординал} \end{cases}$$

Пример

$$\omega \cdot \omega = \sup\{\omega \cdot 0, \omega \cdot 1, \omega \cdot 2, \omega \cdot 3, \dots\} = \sup\{0, \omega, \omega \cdot 2, \omega \cdot 3, \dots\}$$

Ординалы (порядковые числа) и порядок

Определение

Будем говорить, что $\langle S, (\prec) \rangle$ имеет порядковое число (тип) X , если существует биекция $f : S \rightarrow X$, причём $a \prec b$ тогда и только тогда, когда $f(a) \in f(b)$.

Пример

- ▶ Добавить элемент перед бесконечностью: \mathbb{N} и \mathbb{N}_0 .
 $1 + \omega = \omega$.
- ▶ Добавить элемент после бесконечности $(+\infty)$. $\omega + 1 \neq \omega$

Пары и списки

Пример

Упорядоченные пары натуральных чисел имеют порядковый тип ω^2 .

$$\langle 3, 5 \rangle < \langle 4, 3 \rangle \quad \omega \cdot 3 + 5 < \omega \cdot 4 + 3.$$

Пример

Списки натуральных чисел — порядковый тип ω^ω .

$$\langle 3, 1, 4, 1, 5, 9 \rangle \quad \omega^5 \cdot 3 + \omega^4 \cdot 1 + \omega^3 \cdot 4 + \omega^2 \cdot 1 + \omega^1 \cdot 5 + 9$$

Дизъюнктные множества

Определение

Дизъюнктное (разделённое) множество — множество, элементы которого не пересекаются.

$$Dj(x) \equiv \forall y. \forall z. (y \in x \ \& \ z \in x \ \& \ \neg y = z) \rightarrow \neg \exists t. t \in y \ \& \ t \in z$$

Пример

Дизъюнктное: $\{\{1, 2\}, \{\rightarrow\}, \{\alpha, \beta, \gamma\}\}$

Не дизъюнктное: $\{\{1, 2\}, \{\rightarrow\}, \{\alpha, \beta, \gamma, 1\}\}$

Прямое произведение множеств

Определение

Прямое произведение дизъюнктного множества a — множество $\times a$ всех таких множеств b , что:

- ▶ b пересекается с каждым из элементов множества a в точности в одном элементе
- ▶ b содержит элементы только из $\cup a$.

$$\forall b. b \in \times a \leftrightarrow (b \subseteq \cup a \ \& \ \forall y. y \in a \rightarrow \exists! x. x \in y \ \& \ x \in b)$$

Пример

$$\times \{ \{ \triangle, \square \}, \{ 1, 2, 3 \} \} = \\ \{ \{ \triangle, 1 \}, \{ \triangle, 2 \}, \{ \triangle, 3 \}, \{ \square, 1 \}, \{ \square, 2 \}, \{ \square, 3 \} \}$$

Аксиома выбора

Определение

Прямое произведение непустого дизъюнктного множества, не содержащего пустых элементов, не пусто.

$$\forall t. Dj(t) \rightarrow (\forall x. x \in t \rightarrow \exists p. p \in x) \rightarrow (\exists p. p \in \times t)$$

Альтернативные варианты: любое множество можно вполне упорядочить, любая сюръективная функция имеет частичную обратную, и т.п.

Определение

Аксиоматика ZF + аксиома выбора = ZFC

Дискуссия вокруг аксиомы выбора

Пример

Парадокс Банаха-Тарского: трёхмерный шар равносоставлен двум своим копиям.

Теорема

Теорема (Гёдель, 1938): аксиома выбора не добавляет противоречий в ZF .

Теорема

Теорема (Коэн, 1963): аксиома выбора не следует из других аксиом ZF .

Пример

Односторонние функции: $Sha256$ и т.п. У $Sha256$ есть обратная.

Теорема

Теорема Диаконеску: ZFC поверх интуиционистского исчисления предикатов содержит правило исключённого третьего.

Аксиома фундирования

Определение

Аксиома фундирования. В каждом непустом множестве найдется элемент, не пересекающийся с исходным множеством.

$$\forall x. x \neq \emptyset \vee \exists y. y \in x \ \& \ \forall z. z \in x \rightarrow z \not\subseteq y$$

Иными словами, в каждом множестве есть элемент, минимальный по отношению (\in).

Идея Рассела: каждому множеству припишем *тип* (тип пустого 0, тип множеств 1, тип множеств множеств 2 и т.п.). Тогда конструкция невозможна: $\{x \mid x \in x\}$. Аксиома фундирования позволяет определить функцию ранга:

$$rk(x) = \sup\{rk(y) \mid y \in x\}$$

Схема аксиом подстановки

Определение

Схема аксиом подстановки. Пусть задана некоторая функция f , представляемая в исчислении предикатов: то есть задана некоторая формула ϕ , такая, что $f(x) = y$ тогда и только тогда, когда $\phi(x, y) \ \& \ \exists! z. \phi(x, z)$. Тогда для любого множества S существует множество $f(S)$ — образ множества S при отображении f .

$$\forall s. (\forall x. \forall y_1. \forall y_2. x \in s \& \phi(x, y_1) \& \phi(x, y_2) \rightarrow y_1 = y_2) \rightarrow (\exists t. \forall y. y \in t \leftrightarrow \exists x. x \in s \& \phi(x, y))$$