

Введение в математическую логику и теорию алгоритмов

Лекция 14. Теория множеств Цермело – Френкеля.

Наш предварительный план состоял в том, чтобы (1) выбрать язык для записи математических утверждений (в качестве такого языка был выбран язык логики отношений) (2) определить истинность утверждений, записанных в данном языке, понятие следования утверждения из теории (мы использовали структуры и модели, доказали перечислимость следования и сформулировали теорему о полноте логики отношений). Далее следовало (3) построить теорию, пригодную для доказательства математических утверждений, (4) убедиться в непротиворечивости этой теории и (5) доказать полноту этой теории. Как показывают Вторая теорема Гёделя и теорема Гёделя о неполноте, пункты 3 и 4 не могут быть реализованы в полном объеме для достаточно содержательной теории. Несмотря на это мы сегодня рассмотрим теорию, которая претендует на реализацию пункта 3.

Мы приступаем к знакомству с *теорией множеств Цермело — Френкеля* (обозначаемой **ZF**). Эта теория разрабатывалась для того, чтобы любое математическое утверждение естественно записывалось в виде замкнутой формулы в сигнатуре **ZF**, а доказательство утверждения могло бы быть записано как (синтаксический) вывод в данной теории. Имеются разные системы аксиом теории множеств, **ZF**, по-видимому, наиболее распространенная.

Теория **ZF** является теорией с равенством, сигнатура теории (кроме, конечно =) состоит из единственного имени \in двуместного отношения, следуя традиции мы будем использовать запись $a \in b$, а не $\in (a, b)$.

Теория **ZF** предназначена для того, чтобы на формальном языке описать понятие "множества". Поэтому естественно называть элементы моделей данной теории множествами. Это приводит к некоторой двусмысленности, поскольку термин "множество" используется нами и в неформальном смысле: "множество четных чисел" и пр. Аналогичная проблема возникала, например, и в случае моделей арифметики: мы называли натуральными числами и элементы моделей и "обычные" натуральные числа. В данной лекции, чтобы избежать двусмысленности, мы используем термины множество, подмножество, функция и пр. только в формальном смысле – в смысле элементов рассматриваемой модели **ZF**. Для содержательных неформальных понятий мы будем использовать термины класс, набор, совокупность, подкласс, отображение и пр. Например обычный натуральный ряд мы будем называть "совокупностью натуральных чисел".

Таким образом (в течении данной лекции) *множество* – это класс элементов структуры M имеющий вид $\{b \text{ из } M \mid M \models b \in a\}$ для некоторого a из M .

Неформальное замечание: структура, которую мы пытаемся описать с помощью **ZF** — класс всех "чистых" множеств, то есть множеств, элементами которых являются только множества. Так у нас будет пустое множество; множество, единственным элементом которого является пустое множество; множество из двух элементов: один элемент –

пустое множество, второй – одноэлементное множество, содержащее пустое множество и т.д. Кажется, для целей математики достаточно таких множеств.

Аксиомы ZF.

Хочется для каждой формулы $\Phi(x)$ добавить аксиому $\exists u(\forall v(v \in u \equiv \Phi(v)))$ но теория станет противоречивой (рассмотрите формулу $\Phi(x) = x \notin x$) — парадокс Рассела.

Мы скажем, что класс элементов $\{x|x \notin x\}$ ”не является множеством”, имея в виду, что хотя элементы с таким свойством могут существовать в описываемой структуре, однако в ней нет такого элемента a , что $\{x|x \in a\} = \{x|x \notin x\}$.

Четыре вида аксиом существования множеств.

Аксиомы подмножеств

Список аксиом

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

для всех формул $\Phi(\bar{x}, y)$. Здесь и далее \bar{x} обозначает цепочку переменных.

Иными словами аксиомы гарантируют, что для любой формулы $\Phi(\bar{x}, y)$ и любых элементов a, b_0, \dots, b_k нашей структуры, класс $\{x|x \in a \wedge \Phi(\bar{b}, x)\}$ является множеством.

Аксиомы замены

Список аксиом

$$\begin{aligned} &\forall \bar{t} ((\forall u \exists v \forall w (w \in v \equiv \Phi(\bar{t}, u, w)) \rightarrow \\ &\rightarrow \forall v \exists s \forall w (\exists u (u \in v \wedge \Phi(\bar{t}, u, w)) \equiv w \in s))) \end{aligned}$$

для всех формул $\Phi(\bar{x}, y)$.

Пусть b_0, \dots, b_k – некоторые элементы нашей структуры, тогда формуле $\Phi(\bar{b}, y, z)$ соответствует некоторое отображение: каждому элементу a соответствует класс $\{z|\Phi(\bar{b}, a, z)\}$. Предположим, что каждый такой класс является множеством. Даже в этом случае объединение семейства таких классов может не быть множеством.

Аксиома замены гарантирует, что если для каждого a класс $\{z|\Phi(\bar{b}, a, z)\}$ является множеством и мы выбираем a из некоторого множества s (то есть рассматриваем ограничение этого отображения на множестве s), то объединение таких классов, то есть класс $\{z|\exists u (u \in s \wedge \Phi(\bar{b}, u, z))\}$, является множеством.

Аксиома степени

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

Мы будем использовать выражение $x \subset y$ как сокращение для формулы $\forall u (u \in x \rightarrow u \in y)$. Используя это сокращение можно сказать, что аксиома степени гарантирует, что для любого элемента a класс $\{x|x \subset a\}$ является множеством.

Аксиома бесконечности

$$\begin{aligned} &\exists s (\exists u (u \in s \wedge \forall v (v \notin u)) \wedge \\ &\wedge \forall u (u \in s \rightarrow \exists v (v \in s \wedge \forall w (w \in v \equiv (w \in u \vee w = u)))))) \end{aligned}$$

Это важная аксиома, однако в данной формулировке она столь сложна, что мы отложим ее обсуждение до того момента, когда мы будем исследовать множество ω . В данный момент заметим лишь, что она безусловно гарантирует существование множеств с некоторыми специальными свойствами. Это отличает ее от аксиом подмножеств, замены и степени, которые позволяли строить множества лишь исходя из существования некоторых других множеств.

Аксиома регулярности (фундирования)

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

Эта аксиома утверждает, что в любом множестве a есть такой элемент b , что пересечение множеств $\{x|x \in a\}$ и $\{x|x \in b\}$ пусто. Мы не будем обосновывать эту аксиому, заметим лишь, что она бывает полезна, хотя в наших предварительных рассмотрениях мы ее использовать не будем.

Аксиома объемности

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

Следующие два утверждения выводятся из предыдущих аксиом, но чтобы не загромождать изложение их выводом, мы включим их в теорию.

Аксиома пустого множества

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

Аксиома пары

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

то есть $\{x|x = a \vee x = b\}$ является множеством для любых элементов a и b .

Предварительные замечания и соглашения

Теория множеств понимается и как содержательная теория: утверждения о некоторой структуре "настоящих" множеств; и как анализ формальной теории **ZF** – непротиворечивость, полнота, исследование всевозможных моделей и пр. Аналогично арифметике (теории чисел) и арифметике Пеано. Мы, в основном, будем заниматься формальной теорией множеств.

Мы предположим, что у теории **ZF** есть модель и постараемся понять, как она устроена, в частности, что в такой модели соответствует натуральным числам и другим обычным математическим объектам. Это похоже на рассмотрение нестандартных арифметик, с существенным отличием: в случае арифметики мы не предполагали, а были уверены, что модели существуют.

Напомним, что выражение $\mathbf{ZF} \models \Phi$ обозначает, что утверждение Φ следует из теории **ZF**, то есть утверждение Φ истинно во всех моделях теории **ZF**. Как вы знаете (перечислимость следования, теорема о полноте логики отношений) следование из теории эквивалентно выводимости в некотором фиксированном исчислении. В данной лекции, утверждая, что $\mathbf{ZF} \models \Phi$ мы будем, в основном, пользоваться (семантическим) определением следования.

Чтобы избежать слишком длинных формул мы будем использовать сокращения. Одно из них – квантор $\exists!$ – означает ”существует единственное”. Иными словами, запись $\exists!u\Phi(u)$ является сокращением для формулы $\exists u(\Phi(u) \wedge \forall v(\Phi(v) \rightarrow u = v))$.

Из аксиомы пустого множества и аксиомы объемности следует, что $\mathbf{ZF} \models \exists!s\forall u(u \notin s)$, то есть в модели существует единственный элемент a , удовлетворяющий формуле $\forall u(u \notin a)$. Этот элемент мы будем обозначать символом \emptyset . Этот символ мы будем использовать в атомных формулах так же, как имя предмета, однако это просто сокращение: формула $\emptyset \in x$ является сокращением для $\exists u(\forall v(v \notin u) \wedge u \in x)$ или $\forall u(\forall v(v \notin u) \rightarrow u \in x)$ — эти формулы равносильны, поскольку $\exists!u\forall v(v \notin u)$. Аналогично для выражений $\emptyset = x, x \in \emptyset$.

В общем случае, пусть для некоторой формулы $\Phi(\bar{x}, y)$ выполнено $\mathbf{ZF} \models \forall \bar{u}\exists!v\Phi(\bar{u}, v)$, то есть $\Phi(\bar{x}, y)$, по существу, задаёт отображение. Тогда мы будем иногда добавлять новый функциональный символ $\varphi(\bar{x})$ и использовать его в атомных формулах, имея в виду, что, например, $y \in \varphi(\bar{x})$ является сокращением для $\exists u(\Phi(\bar{x}, u) \wedge y \in u)$ или $\forall u(\Phi(\bar{x}, u) \rightarrow y \in u)$. В частности $y = \varphi(\bar{x}) \Leftrightarrow \Phi(\bar{x}, y)$.

Из аксиом степени и объемности следует, что $\mathbf{ZF} \models \forall u\exists!s\forall v(v \subset u \equiv v \in s)$. Мы введем обозначение $P(x)$ для соответствующего отображения так, что $P(x) = y \Leftrightarrow \forall v(v \subset x \equiv v \in y)$, мы будем называть $P(x)$ множеством подмножеств x .

Из аксиомы пары и объемности следует, что $\mathbf{ZF} \models \forall u, v\exists!s\forall w(w \in s \equiv (w = u \vee w = v))$. Соответствующее отображение мы будем обозначать $\{x, y\}$ и называть (неупорядоченной) парой множеств x и y . Пару $\{x, x\}$ мы будем обозначать $\{x\}$.

Класс $Un(x) = \{y|\exists u(y \in u \wedge u \in x)\}$ называется объединением множества x . Мы хотим показать, что $Un(x)$ является множеством и это множество определено однозначно. Мы можем воспользоваться аксиомой замены для формулы $\Phi(y, z) = z \in y$, поскольку $\{x|x \in a\}$ очевидно является множеством для любого a . Множество $Un(\{x, y\})$ мы будем обозначать $x \cup y$. Через $x \cap y$ мы будем обозначать *пересечение* множеств — множество $\{z|z \in x \wedge z \in y\}$, через $x \setminus y$ — *разность*: $\{z|z \in x \wedge z \notin y\}$. Из аксиомы подмножеств непосредственно следует, что пересечение и разность являются множествами и определены однозначно.

Множество $\{\{x\}, \{x, y\}\}$ мы назовем *упорядоченной парой* множеств x, y и будем обозначать $\langle x, y \rangle$. Нетрудно доказать основное свойство упорядоченных пар:

$$\langle x, y \rangle = \langle x', y' \rangle \Leftrightarrow x = x' \wedge y = y'$$

то есть, что $\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\} \Leftrightarrow x = x' \wedge y = y'$. Постарайтесь сами провести доказательство, рассмотрев как случай $x = y$, так и $x \neq y$.

Упорядоченная тройка $\langle x, y, z \rangle$ определяется как $\langle x, \langle y, z \rangle \rangle$, аналогично определяется упорядоченная n -ка.

Декартово произведение $x \times y$ определяется как класс $\{z|\exists u, v(u \in x \wedge v \in y \wedge z = \langle u, v \rangle)\}$. Чтобы доказать, что $x \times y$ является множеством, нам достаточно показать, что все элементы класса содержатся в некотором множестве и воспользоваться аксиомой подмножеств. Это сделать нетрудно, поскольку $a \in x \times y \Rightarrow a \in P(P(x \cup y))$.

Множество f пар $\langle a, b \rangle$ мы будем называть *функцией* и обозначать это как $Func(f)$, если $\forall u, v, w (\langle u, v \rangle \in f \wedge \langle u, w \rangle \in f \rightarrow v = w)$. Если f — функция, то множество $\{z | \exists u (\langle z, u \rangle \in f)\}$ называется *областью определения* ($Dom(f)$), а множество $\{z | \exists u (\langle u, z \rangle \in f)\}$ — *областью значения* ($Ra(f)$) функции. Покажите, воспользовавшись аксиомой замены, что это действительно множества. Ясно, как определить *инъективную (взаимно однозначную) функцию*; соответствующую формулу мы обозначим $IFunc(x)$.

Если f — функция, $x \in Dom(f)$, то через $f(x)$ мы будем (не опасаясь некоторой двусмысленности) обозначать единственное множество y , такое, что $\langle x, y \rangle \in f$.

Натуральные числа (ω)

Теперь мы готовы к тому, чтобы определить, что соответствует в нашей модели классу натуральных чисел. Натуральным числам $0; 1; 2; \dots$ будут соответствовать классы $\emptyset; \{\emptyset\}; \{\emptyset, \{\emptyset\}\}; \dots$. Ясно, что каждый такой класс является множеством, однако мы хотим понять, что в нашей структуре соответствует классу всех натуральных чисел.

Обозначим через $S(x)$ множество $x \cup \{x\}$. В этих обозначениях можно сказать, что $0 = \emptyset, 1 = S(0), 2 = S(1), \dots$, а аксиому бесконечности

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

можно записать в виде

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

то есть в нашей структуре существует элемент s , удовлетворяющий формуле

$$\emptyset \in s \wedge \forall u (u \in s \rightarrow S(u) \in s)$$

Такие множества мы (временно) будем называть *”бесконечными”*. Легко видеть, что пересечение *”бесконечных”* множеств является *”бесконечным”*. Обозначим через ω пересечение всех *”бесконечных”* множеств

$$\omega = \{x | \forall s ((\emptyset \in s \wedge \forall u (u \in s \rightarrow S(u) \in s)) \rightarrow x \in s)\}$$

Из аксиомы бесконечности и аксиомы подмножеств следует, что ω является множеством, по аксиоме объемности это множество определено однозначно. Очевидно, что ω является наименьшим *”бесконечным”* множеством, то есть $\omega \subset a$ для любого *”бесконечного”* a .

Если a — непустое подмножество ω , то *граничным элементом* множества a назовем такой элемент $b \in a$, что $b = 0$ или $b = S(c)$ для некоторого $c \in \omega, c \notin a$.

Теорема индукции: в любом непустом подмножестве ω имеется граничный элемент, то есть

$$\mathbf{ZF} \models \forall u (u \subset \omega \wedge u \neq \emptyset \rightarrow (0 \in u \vee \exists v (v \in \omega \wedge v \notin u \wedge S(v) \in u)))$$

Доказательство. Пусть $a \subset \omega, b = \omega \setminus a$. Предположим, что в a нет граничного элемента, то есть $0 \in b, c \in b \rightarrow S(c) \in b$, следовательно b ”бесконечно”. Тогда, из минимальности ω , выполнено $\omega \subset b$ и a пусто. \square

Символами n, m, k, \dots мы будем в данном разделе обозначать элементы ω .

Определим порядок на ω так, что $n < m \Leftrightarrow n \in m$

Несколько простых свойств порядка на ω (некоторые из них, выбранные достаточно произвольно, мы докажем, остальные оставим в качестве упражнений). Формулировать эти свойства мы будем достаточно кратко, опуская выражение $\mathbf{ZF} \models$ и пр. Так, свойство (0) полностью должно быть записано так:

$$\mathbf{ZF} \models \forall n(n \in \omega \rightarrow (0 = n \vee \exists m(m \in \omega \wedge n = S(m))))$$

$$(0) n = 0 \vee n = S(m)$$

Доказательство. Индукция, от противного. Рассмотрим множество $\{n | n \in \omega, n \neq 0, \forall m(m \in \omega \rightarrow n \neq S(m))\}$, предположим, что оно не пусто и рассмотрим граничный элемент. \square

$$(1) n < S(n) \text{ (определение)}$$

$$(2) x \in n \rightarrow x \subset n$$

Доказательство. Возможно, что доказательство написано излишне подробно. От противного, по индукции.

Рассмотрим класс $\{y | y \in \omega \wedge \exists u(u \in y \wedge \neg(u \subset y))\}$. По аксиоме подмножеств этот класс является множеством, обозначим его a . По предположению $a \neq \emptyset$, следовательно, по теореме индукции, в нем есть граничный элемент – обозначим его n . По определению a выполнено $0 \notin a$, поэтому $n = S(m)$ для некоторого $m \in \omega \setminus a$.

Если $x \in S(m)$, то, по определению операции S , имеет место $x = m$ или $x \in m$. Если $x = m$, то $x \subset S(m)$ по определению операции S . Если $x \in m$, то $x \subset m$, поскольку $m \notin a$. Тогда $x \subset m \subset S(m)$. \square

$$(3) \text{ порядок транзитивен: } n < m \wedge m < k \rightarrow n < k \text{ (2)}$$

$$(4) \neg(n < n) \text{ (индукция или аксиома регулярности)}$$

$$(5) 0 < S(n) \text{ (индукция)}$$

$$(6) n < m \rightarrow m = S(n) \vee S(n) < m \text{ (индукция по } m)$$

$$(7) \text{ порядок линейен, то есть любые два элемента сравнимы: } n < m \vee n = m \vee m < n$$

Доказательство. По индукции. Пусть есть несравнимые элементы. Пусть $a = \{x | x \in \omega \wedge \exists w(w \in \omega \wedge x \text{ и } w \text{ не сравнимы})\}$. Пусть n — граничный элемент множества a . Из (5) следует, что $n \neq 0$, поэтому $n = S(m), m \notin a$. Пусть n не сравним с k . Однако m сравним с k . Если $k < m, k = m$, то $k < n$ из (3). Если $m < k$, то n сравнимо с k из (6). \square

(8) Стандартная индукция: в любом непустом подмножестве ω есть наименьший элемент, то есть

$$a \subset \omega, a \neq \emptyset \Rightarrow \exists k(k \in a \wedge \forall m(m < k \rightarrow m \notin a))$$

Доказательство. Рассмотрим множество $b = \{n | n \in \omega, \exists m(m \in a \wedge m \leq n)\}$. Пусть k – граничный элемент множества b . Если $k = 0$, то $0 \in a$. Если $k = S(m)$, $m \notin b$, то $k \in a$ и k – наименьший элемент. \square

Через $n+1$ мы будем обозначать $S(n)$, через $n-1$ — такое (единственное) m , что $n = S(m)$ (если такое m существует), через $[n, m]$ — $\{k | k \in \omega, k \leq m, n \leq k\}$.

Теперь нетрудно рекурсивно определить сложение на элементах ω как функцию $\Sigma: \omega \times \omega \rightarrow \omega$, удовлетворяющую следующим рекурсивным соотношениям:

$$(0) \Sigma(\langle n, 0 \rangle) = n$$

$$(1) \Sigma(\langle n, m+1 \rangle) = \Sigma(\langle n, m \rangle) + 1$$

Докажем стандартной индукцией, что такое единственное Σ существует и является всюду определенной функцией на $\omega \times \omega$.

Доказательство. Скажем, что элемент $k \in \omega$ *корректен*, если существует функция $\Sigma_k: \omega \times [0, k] \rightarrow \omega$, удовлетворяющее указанным рекурсивным соотношениям при $m \leq k$. Ясно, что класс некорректных элементов ω является множеством, предположим, что оно не пусто. Пусть k — наименьший некорректный элемент. Из (1) следует, что $k \neq 0$. Положим

$$\Sigma_k = \Sigma_{k-1} \cup \{\langle n, k, \Sigma_{k-1}(n, k-1) + 1 \rangle | n \in \omega\}$$

Ясно, что Σ_k удовлетворяет условиям (0), (1) на отрезке $[0, k]$. Это противоречит некорректности k .

Единственность Σ_k доказываем так же, рассмотрев элементы, на которых функция $\Sigma: \omega \times [0, k] \rightarrow \omega$ не единственна.

Таким образом, для любого $k \in \omega$ существует единственная функция Σ_k , удовлетворяющая рекурсивным соотношениям (0), (1) на множестве $\omega \times [0, k]$. Нетрудно заметить, что $k < k' \Rightarrow \Sigma_k \subset \Sigma_{k'}$. По аксиоме замены $Un\{\Sigma_k | k \in \omega\}$ является функцией. Эта функция и будет сложением. \square

Вместо $\Sigma(\langle n, m \rangle)$ мы будем использовать привычную запись $n + m$.

Теперь нетрудно определить умножение как функцию $\Pi: \omega \times \omega \rightarrow \omega$, удовлетворяющую рекурсивным соотношениям:

$$(0) \Pi(\langle n, 0 \rangle) = 0$$

$$(1) \Pi(\langle n, m+1 \rangle) = \Pi(\langle n, m \rangle) + n$$

Аналогично можно определить и все прочие нужные нам арифметические функции и отношения.

Далее мы можем определить множества целых (\mathbb{Z}_M), рациональных (\mathbb{Q}_M) и вещественных (\mathbb{R}_M) чисел. Индекс M указывает, что это множества в нашей структуре, а не "настоящие множества чисел".

Множество \mathbb{Z}_M можно определить как множество пар вида $\langle 0, n \rangle$ и $\langle 1, n \rangle$, ($n \in \omega$), имея в виду, что $\langle 0, n \rangle$ соответствует положительному числу, а $\langle 1, n \rangle$ – отрицательному. Множество \mathbb{Q}_M нетрудно определить как множество классов эквивалентности (подмножеств) множества $\mathbb{Z}_M \times \omega \setminus \{0\}$, с обычной эквивалентностью $\langle x_1, x_2 \rangle \sim \langle y_1, y_2 \rangle \Leftrightarrow x_1 y_2 = x_2 y_1$. Множество \mathbb{R}_M — как множество Дедекиндовых сечений (пар подмножеств множества \mathbb{Q}_M специального вида). Вы уже и сами можете понять, как обычные математические утверждения переводятся в формулы теории **ZF** и оценить, насколько сложно перформулировать обычные доказательства в следствия теории **ZF**.