Введение в математическую логику и теорию алгоритмов

Лекция 11. Теория множеств Цермело – Френкеля.

Мы приступаем к знакомству с системой аксиом (теорией) **ZF**. Эта теория претендует на то, что любое математическое утверждение естественно записывается в виде замкнутой формулы в сигнатуре **ZF**, а доказательство утверждения может быть записано как (синтаксический) вывод в данной теории. Теория **ZF** называется *теорией множеств Цермело — Френкеля*. 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 течение данной лекции) *множество* – это класс элементов структуры M, имеющий вид $\{b$ из $M|$ для некоторого a из $M, M \vDash b \in a\}$.

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.

Аксиома объемности

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

Таким образом, каждому элементу $a \in M$ однозначно соответствует класс $\{b \in M | b \in a\}$, но, повторимся – вовсе не любому набору элементов структуры M должен соответствовать элемент $a \in M$ (должно соответствовать множество).

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 набор 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

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

для всех формул $\Phi(\overline{x}, y)$. Здесь и далее $\overline{x}$ обозначает список элементов.

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

Аксиомы замены

Список аксиом

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

для всех формул $\Phi(\overline{x}, y)$.

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

Аксиома замены гарантирует, что если для каждого a набор $\{z|\Phi(\overline{b}, a, z)\}$ является множеством и мы выбираем a из некоторого множества c (то есть рассматриваем ограничение этого отображения на множестве c), то объединение таких наборов, то есть набор $\{z|\exists u(u \in c \wedge \Phi(\overline{b}, u, z))\}$, 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 записать аксиому степени в виде

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

То есть аксиома степени гарантирует, что для любого элемента a набор $\{x|x \subset a\}$ является множеством.

Аксиома бесконечности

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

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)

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

Эта аксиома утверждает, что в любом множестве a есть такой элемент b, что пересечение наборов $\{x|x \in a\}$ 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.

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** – совместность, полнота, исследование всевозможных моделей и пр. 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.

Задача. *Совместна ли теория* **ZF** *без аксиомы бесконечности?*

Да, в качестве модели можно взять конечные множества конечных множеств. Более формально: в качестве модели можно взять структуру $< \mathbb{N}, \{\in\} >$, где $\in$ определено так, что $i \in j \Leftrightarrow i$-тый знак в двоичной записи числа j равен 1 (то есть $[j/2^i]$ нечетно). Нетрудно проверить, что в данной структуре выполнены все нужные аксиомы.

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

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

— эти формулы равносильны, поскольку $\exists! u \forall v (v \notin u)$. Аналогично для выражений $\varnothing = x, x \in \varnothing$.

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

Из аксиом степени и объемности следует, что $\mathbf{ZF} \vDash \forall u \exists! s \forall v (v \subset u \equiv v \in s)$. 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 $\mathbf{ZF} \vDash \forall u, v \exists! s \forall w (w \in s \equiv (w = u \vee w = v))$. 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 $< x, y >$. Нетрудно доказать основное свойство упорядоченных пар:

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

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 $< x, y, z >$ определяется как $< x, < y, z >>$, аналогично определяется упорядоченная n-ка.

Декартово произведение $x \times y$ определяется как класс $\{z | \exists u, v (u \in x \wedge v \in y \wedge z =< x, y >\}$. 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 $< a, b >$ мы будем называть *функцией* и обозначать это как $Func(f)$, если $\forall u, v, w (< u, v >\in f \wedge < u, w >\in f \to v = w)$. Если f — функция, то множество $\{z | \exists u (< z, u >\in f)\}$ называется *областью определения* $(Dom(f))$, а множество $\{z | \exists u (< u, z >\in f)\}$ — *областью значения* $(Im(f))$ 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 $< x, y >\in f$.

Натуральные числа (ω)

Теперь мы готовы к тому, чтобы определить, что соответствует в нашей модели классу натуральных чисел. Натуральным числам $0; 1; 2; \ldots$ будут соответствовать классы $\varnothing; \{\varnothing\}; \{\varnothing, \{\varnothing\}\}; \ldots$. 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 $0 = \varnothing, 1 = S(0), 2 = S(1), \ldots$, а аксиому бесконечности

$\exists s(\exists u(u \in s \wedge \forall v(v \notin u)) \wedge$

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

можно записать в виде

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

то есть в нашей структуре существует элемент s, удовлетворяющий формуле

$\varnothing \in s \wedge \forall u(u \in s \to S(u) \in s)$

Такие множества мы будем называть *индуктивными*. Легко видеть, что пересечение индуктивных множеств является индуктивным. Обозначим через ω пересечение всех индуктивных множеств

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

Из аксиомы бесконечности и аксиомы подмножеств следует, что ω является множеством, по аксиоме объемности это множество определено однозначно. Очевидно, что ω является наименьшим индуктивным множеством, то есть $\omega \subset a$ для любого индуктивного 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
ZF $\vDash \forall u(u \subset \omega \wedge u \neq \varnothing \to (0 \in u \vee \exists v(v \in \omega \wedge v \notin u \wedge S(v) \in u)))$

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

Символами $n, m, k, \ldots$ 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 свойств мы будем достаточно кратко, опуская выражение **ZF** $\vDash$ и пр. Так, свойство (0) полностью должно быть записано так:

ZF $\vDash \forall n(n \in \omega \to (0 = n \vee \exists m(m \in \omega \wedge n = S(m))))$

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

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

(1) $n < S(n)$ (определение)

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

Доказательство. Возможно, что доказательство написанно 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 $a \neq \varnothing$, 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) 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, 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 *и* w *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

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

Доказательство. Рассмотрим множество $b = \{n | n \in \omega, \exists m(m \in a \wedge m \leqslant n)\}$. 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 $[n, m]$ — $\{k | k \in \omega, k \leqslant m, n \leqslant k\}$.

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

(0) $\Sigma(< n, 0 >) = n$
(1) $\Sigma(< n, m + 1 >) = \Sigma(< n, m >) + 1$

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 $\Sigma_k \colon \omega \times [0, k] \to \omega$, удовлетворяющее указанным рекурсивным соотношениям при $m \leqslant k$. 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

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

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 $\Sigma \colon \omega \times [0, k] \to \omega$ 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. □

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

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

(0) $\Pi(< n, 0 >) = 0$
(1) $\Pi(< n, m + 1 >) = \Pi(< n, m >) + n$

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 $< 0, n >$ и $< 1, n >, (n \in \omega)$, имея в виду, что $< 0, n >$ соответствует положительному числу, а $< 1, n >$ – отрицательному. Множество $\mathbb{Q}_M$ нетрудно определить как множество классов эквивалентности (подмножеств) множества $\mathbb{Z}_M \times \omega \setminus \{0\}$, с обычной эквивалентностью $< x_1, x_2 > \sim < y_1, y_2 > \Leftrightarrow x_1 y_2 = x_2 y_1$. 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**.