Глава 1

Теория множеств Цермело–Френкеля

1.1 Теоремы Геделя о неполноте

1.1.1 Представление натуральных чисел, конечных последовательностей натуральных чисел и их функций в теории множеств

Для каждого натурального n можно написать естественным образом формулу $\mathrm{Name}_n(x)$ с одной свободной переменной x, которая выражает свойство $x = n$. Например, для $n = 0$ формула имеет вид $\forall y\, y \notin x$, для $n = 1$ она имеет вид $\forall y(y \in x \leftrightarrow \mathrm{Name}_0(y))$. И вообще, для любого n формула $\mathrm{Name}_{n+1}(x)$ утверждает, что элементами x являются то y, для которого выполнено $\mathrm{Name}_n(y)$, а также все его элементы.

Построенные формулы обладают следующим свойством: для любого n в ZF можно доказать существование и единственность x, для которого выполнено $\mathrm{Name}_n(x)$. Поэтому для каждого n мы можем использовать в формулах новую константу, обозначаемую $\boldsymbol{n}$. При этом любая формула $B(\boldsymbol{n})$, содержащая константу $\boldsymbol{n}$, будет пониматься, как формула

$$\exists x(\mathrm{Name}_n(x) \wedge B(x))$$

или как формула

$$\forall x(\mathrm{Name}_n(x) \to B(x)).$$

Какое из двух пониманий выбрать, неважно, поскольку в теории множеств выводимо утверждение о существовании единственного такого x, что $\mathrm{Name}_n(x)$.

Есть и следующий альтернативный способ представления натуральных чисел в теории множеств. Для каждого натурального n можно было бы добавить в сигнатуру теории множеств новую константу $\boldsymbol{n}$, а к аксиомам ZF добавить формулу $\mathrm{Name}_n(\boldsymbol{n})$. Это удобнее, но при таком подходе придется доказывать, что получится теория, эквивалентная исходной теории для формул исходной сигнатуры. Поэтому мы не будем так делать.

Любые простые факты о натуральных числах доказуемы в ZF. Например, если $n = m+k$ или $n = mk$ или $n = m^k$ или $n < m$, то доказуемы, соответственно, формулы $\forall z(A_+(\boldsymbol{m}, \boldsymbol{k}, z) \leftrightarrow \mathrm{Name}_n(z))$, $\forall z(A_*(\boldsymbol{m}, \boldsymbol{k}, z) \leftrightarrow \mathrm{Name}_n(z))$ $\forall z(A_{\exp}(\boldsymbol{m}, \boldsymbol{k}, z) \leftrightarrow \mathrm{Name}_n(z))$, $A_<(\boldsymbol{n}, \boldsymbol{m})$. Здесь $A_+, A_*, A_{\exp}, A_<$ обозначают формулы, определяющие сложение, умножение, возведение в степень и порядок на натуральных числах. Кроме того, если утверждение $n < m$ неверно, то доказуемо $\neg A_<(\boldsymbol{n}, \boldsymbol{m})$.

Это свойство предиката порядка и операций сложения, умножения и возведения в степень можно обобщить следующим образом. Говорят, что функция $f(x_1, \dots, x_n)$, аргументы и значения которой — натуральные числа, *представима в ZF формулой* $A(x_1, \dots, x_n, y)$, если для любых натуральных чисел $a_1, \dots, a_n, b$ таких, что $b = f(a_1, \dots, a_n)$ в теории множеств выводится формула

$$\forall y(A(\boldsymbol{a}_1, \dots, \boldsymbol{a}_n, y) \leftrightarrow \mathrm{Name}_b(y)).$$

Говорят, что предикат $P(x_1, \dots, x_n)$, аргументы которого являются натуральными числами, *представим в ZF формулой* $B(x_1, \dots, x_n)$ если для любых натуральных чисел $a_1, \dots, a_n$ таких, что $P(a_1, \dots, a_n) = 1$ в теории множеств выводится формула $B(\boldsymbol{a}_1, \dots, \boldsymbol{a}_n)$, а для любых натуральных $a_1, \dots, a_n$ таких, что $P(a_1, \dots, a_n) = 0$ в теории множеств выводится формула $\neg B(\boldsymbol{a}_1, \dots, \boldsymbol{a}_n)$.

Таким образом, функции сложения, умножения и возведения в степень и предикат порядка представимы в ZF некоторыми формулами. Нетрудно также доказать, что предикат равенства представим (формулой $x = y$).

Точно так же в теории множеств можно представлять конечные последовательности натуральных чисел и функции, аргументами и значениями которых являются конечные последовательности натуральных чисел. Для этого для каждой конечной последовательности α натуральных чисел естественным образом напишем формулу $\mathrm{Name}_\alpha(x)$ с одной свободной переменной x, для которой в теории множеств доказуемо существование и единственность такого x, что $\mathrm{Name}_\alpha(x)$. Через $B(\boldsymbol{\alpha})$, мы будем обозначать формулу $\exists x(\mathrm{Name}_\alpha(x) \wedge B(x))$. Представимость функций и предикатов на последовательностях натуральных чисел определяется точно так же, как и раньше. Например представимой является функция, которая сопоставляет конечным последовательностям α и β в их конкатенацию.

Можно доказать: что все вычислимые функции и разрешимые предикаты представимы в теории множеств. Обратное тоже верно в предположении непротиворечивости теории множеств. (Если же теория множеств противоречива, то представимы все функции и предикаты.)

1.1.2 Представление формул теории множеств в теории множеств

Формулы теории множеств являются конечными последовательностями символов $=, \in, (,), \wedge, \vee, \neg, \to, \exists, \forall$ и предметных переменных $x_1, x_2, \dots$. Мы отождествим эти символы с натуральными числами (например, отождествив каждый символ с его номером в том порядке, в котором мы их выписали). Тогда каждая формула A языка теории множеств будет отождествлена с соответствующей конечная последовательностью натуральных чисел (но не каждая последовательность натуральных чисел будет формулой, а только те, которые построены по некоторым правилам). В дальнейшем мы будем конечные последовательности натуральных чисел называть кратко *строками.*

Можно естественным образом написать формулы с одной свободной переменной x, которая представляет в теории множеств предикаты “быть переменной”, “быть формулой”, “быть формулой с одной свободной переменной” и тому подобные. Более того, можно написать формулы с двумя свободными переменными, которая представляет в теории множеств предикат “последовательность натуральных чисел x является выводом в теории множеств формулы y”. Эту формулу мы будем обозначать через $\mathrm{Proof}(x, y)$. С помощью этой формулы можно выразить выводимость: формула $\exists x\, \mathrm{Proof}(x, y)$ выражает то, что y является выводимой в теории множеств формулой. Эту формулу мы будем обозначать через $\mathrm{Pr}(y)$. Заметим, что формула $\mathrm{Pr}(y)$ не представляет предикат выводимости. А именно, не выполнено второе требование: существует невыводимая формула A, для которой формула $\neg\mathrm{Pr}(\boldsymbol{A})$ не выводима (если теория множеств непротиворечива). Такой пример мы рассмотрим в следующем параграфе.

Однако, первое требование требование в определении представимости предиката выводимости формулой $\mathrm{Pr}(y)$ выполнено:

Лемма 1. *Если формула A выводима в теории множеств, то и формула $Pr(\boldsymbol{A})$ также выводима.*

Доказательство. Действительно, в этом случае рассмотрим последовательность формул α, являющуюся выводом формулы A. Тогда можно вывести $\exists y \exists x(\mathrm{Name}_A(y) \wedge \mathrm{Name}_\alpha(x) \wedge \mathrm{Proof}(x, y))$, из которой очевидно выводится формула $\exists y(\mathrm{Name}_A(y) \wedge \exists x\, \mathrm{Proof}(x, y))$, то есть $\mathrm{Pr}(\boldsymbol{A})$. $\square$

1.1.3 Первая теорема Геделя о неполноте

Будем формулу $\mathrm{Pr}(\boldsymbol{A})$ сокращать через $\Box A$.

Теорема 2. *Если теория множеств непротиворечива, то существует замкнутая невыводимая в теории множеств формула A, для которой формула $\neg\Box A$ (выражающая невыводимость формулы A) невыводима.*

Доказательство. Доказательство основано на конструкции, придуманной Геделем, которую сейчас принято называть “принципом отражения”.

Лемма 3. *Пусть дана произвольная формула $B(z)$ сигнатуры теории множеств с одной свободной переменной z. Тогда существует замкнутая формула A сигнатуры теории множеств, для которой в теории множеств выводится формула*

$$A \leftrightarrow B(\boldsymbol{A}).$$

Доказательство. Рассмотрим функцию, которая сопоставляет паре конечных последовательностей натуральных чисел новую последовательность натуральных чисел по правилу

$$C(x), \alpha \mapsto C(\boldsymbol{\alpha}),$$

или более подробно

$$C(x), \alpha \mapsto \exists x(\mathrm{Name}_\alpha(x) \wedge C(x)).$$

Здесь $C(x)$ — произвольная формула с одной свободной переменной, которая обозначена через x. Если первый аргумент функции не является формулой с одной свободной переменной, то функция определена какимнибудь тривиальным образом. Эту функцию будем называть *функцией подстановки.*

В представимость функции подстановки нетрудно поверить и мы будем обозначать через $\mathrm{Subst}(x, y, z)$ формулу, представляющую. Таким образом, если формула D имеет вид $C(\boldsymbol{\alpha})$, где $C(x)$ — произвольная формула с одной свободной переменной x, то в теории множеств доказуема формула

$$\forall z(\mathrm{Subst}(\boldsymbol{C}, \boldsymbol{\alpha}, z) \leftrightarrow \mathrm{Name}_D(z)).$$

Теперь рассмотрим формулу

$$\exists z(\mathrm{Subst}(x, x, z) \wedge B(z)),$$

которая выражает следующее утверждение: результат замены в формуле x с одной свободной переменной x этой переменной на саму эту формулу удовлетворяет свойству $B(z)$. Эта формула содержит одну свободную переменную x. Обозначим эту формулу через $C(x)$ и положим

$$\begin{aligned} A = C(\boldsymbol{C}) &= \exists x(\mathrm{Name}_C(x) \wedge C(x)) \\ &= \exists x(\mathrm{Name}_C(x) \wedge \exists z(\mathrm{Subst}(x, x, z) \wedge B(z))). \end{aligned}$$

Говоря неформально, эта формула A утверждает, что формула, полученная из формулы $C(x)$ подстановкой $\boldsymbol{C}$ вместо x, удовлетворяет свойству $B(z)$. Но поскольку при указанной подстановке получится как раз формула A, получается, что A утверждает, что она сама удовлетворяет свойству $B(z)$. Поэтому не удивительно, что формула A удовлетворяет утверждению леммы. Докажем это.

Формула A утверждает существование x, z, для которых

$$\mathrm{Name}_C(x) \wedge \mathrm{Subst}(x, x, z) \wedge B(z), \tag{1.1}$$

Поскольку формула Subst представляет в ZF функцию подстановки, выводима формула

$$\forall x(\mathrm{Name}_C(x) \to \forall z(\mathrm{Subst}(x, x, z) \leftrightarrow \mathrm{Name}_A(z))).$$

Поэтому формула (1.1) доказуемо равносильна формуле

$$\mathrm{Name}_C(x) \wedge \mathrm{Name}_A(z) \wedge B(z),$$

Поскольку первая часть последней формулы ($\mathrm{Name}_C(x)$) никак не связана со второй, формула A доказуемо равносильна конъюнкции формул $\exists x\, \mathrm{Name}_C(x)$ и $\exists z(\mathrm{Name}_A(z) \wedge B(z))$. Первая из этих формул доказуема, а вторая и есть $B(\boldsymbol{A})$, поэтому в ZF доказуема равносильность A и $B(\boldsymbol{A})$. $\square$

Продолжим доказательство теоремы. Применим лемму к формуле $B(x)$, равной $\neg\mathrm{Pr}(x)$. Тогда для формулы A, существующей по лемме, в теории множеств выводима формула

$$A \leftrightarrow \neg\Box A.$$

Отсюда сразу следует, что либо обе формулы $A, \neg\Box A$ доказуемы, либо обе доказуемы. Ясно что первое невозможно, поскольку по лемме 1 из доказуемости формул A следует доказуемость формулы $\Box A$, что противоречит предположению о непротиворечивости теории множеств. Поэтому имеет место вторая альтернатива, что и утверждает теорема. $\square$

1.1.4 Вторая теорема Геделя о неполноте

Будем обозначать через $\perp$ какую-нибудь фиксированную формулу вида $B \wedge \neg B$. Доказуемость формулы $\perp$ в теории множеств означает противоречивость последней.

Теорема 4. *Если теория множеств непротиворечива, то формула $\neg\Box\perp$ (выражающая непротиворечивость теории множеств) невыводима.*

Доказательство. Рассмотрим формулу A из доказательства предыдущей теоремы, для н выводима формула

$$A \leftrightarrow \neg\Box A.$$

Доказательство противоречивости ZF в предположении о выводимости формулы A было проведено в рамках самой теории множеств, поэтому в теории множеств выводима формула

$$\Box A \to \Box\perp.$$

Рассуждая от противного, допустим, что формула $\neg\Box\bot$ выводима в ZF. Тогда выводима и формула $\neg\Box A$, а значит и формула A (поскольку доказуема формула $A \leftrightarrow \neg\Box A$). Но тогда по лемме 1 доказуема и формула $\Box A$, и теория множеств оказывается противоречивой вопреки предположению. $\Box$

Вторая теорема о неполноте справедлива не только для теории ZF, но и для теории ZFC. Для того, чтобы сформулировать и доказать теорему для ZFC, надо изменить формулы $\mathrm{Proof}(x, y)$, $\mathrm{Pr}(y)$ $\Box A$, учтя добавленную аксиому выбора, а затем повторить все рассуждения из доказательства. Можно добавить и какие-нибудь другие аксиомы и даже любое разрешимое множество новых аксиом: если полученная теория непротиворечива, то утверждение о ее непротиворечивости в ней не доказуемо. Предположение о разрешимости множества новых аксиом нужно для того, чтобы вообще было возможным представить предикат выводимости некоторой формулой.

В следующем разделе мы обсудим вопрос, при каких условиях на теорию первого порядка и формулу, выражающую доказуемость, справедлива теорема Геделя о неполноте. Ответ такой: если в теории первого порядка вообще можно естественным способом определить формулу доказуемости, то для н справедлива вторая теорема о неполноте.

1.1.5 Вторая теорема для других теорий первого порядка

Пусть дана теория первого порядка T некоторой сигнатуры для которой выполнены следующие условия.

1 Для каждой строки α зафиксирована формула Name_α с одной свободной переменной, такая, что в теории T выводимо $\exists! x\, \mathrm{Name}_\alpha(x)$.

2 Существует алгоритм, который по α находит формулу $\mathrm{Name}_\alpha(x)$,

3 Каждая вычислимая функция, аргументами и значениями которой являются строки, представима в T (в смысле определения из первого раздела).

4 Зафиксирована формула $\mathrm{Proof}(x, y)$, представляющая в T предикат “x есть доказательство формулы y”; с его помощью мы определяем формулу $\mathrm{Pr}(y)$, как $\exists x\, \mathrm{Proof}(x, y)$ и оператор $\Box A$, как $\mathrm{Pr}(\boldsymbol{A})$.

Из этих требований так же как и в случае ZF следуют утверждения лемм 1 и 3 (в формулировке которых теорию множеств надо заменить на теорию T). Но, к сожалению, этих требований недостаточно. Убедиться в этом можно на следующем примере. Для T равной ZF рассмотрим формулу $\mathrm{Proof}'(x,y)$, определенную как $\mathrm{Proof}(x,y) \wedge \neg\, \mathrm{Name}_{\perp}(y)$. Эта формула дополнительно к тому, что x является доказательством y утверждает, что y отлична от $\perp$. Если теория ZF непротиворечива, то формула $\perp$ не имеет вывода, поэтому формула $\mathrm{Proof}'(x,y)$ также представляет предикат доказуемости. Если на основе этого предиката определить оператор $\Box'$, то формула $\neg\Box'\perp$ будет тривиально выводимой — у формулы $\perp$ не может быть доказательства, поскольку это “запрещено специальным указом”. Более подробно, формула $\neg\Box'\perp$ равна

$$\neg\exists x(\mathrm{Proof}(x,\perp) \wedge \neg\, \mathrm{Name}_{\perp}(\perp)),$$

то есть,

$$\exists y(\mathrm{Name}_{\perp}(y) \wedge \neg\exists x(\mathrm{Proof}(x,y) \wedge \neg\, \mathrm{Name}_{\perp}(y)),$$

и равносильна выводимой формуле $\exists y\ \mathrm{Name}_{\perp}(y)$.

Поэтому потребуем дополнительно чтобы формула, представляющая предикат доказуемости имела следующие два свойства.

5 Утверждение Леммы 1 доказуемо в T для любой конкретной формулы A. А именно, для любой замкнутой формулы A в T выводима формула $\Box A \to \Box\Box A$.

6 В T выводимо утверждение о том, что множество выводимых формул замкнуто относительно применения правила Modus Ponens. А именно, для любых замкнутых формул A, B в T выводима формула $\Box(A \to B) \wedge \Box A \to \Box B$, или в эквивалентной форме, $\Box(A \to B) \to (\Box A \to \Box B)$.

Свойства 5 и 6 называют *второй и третьей аксиомами Бернайса*, а *первой аксиомой Бернайса* называют утверждение Леммы 1. Нетрудно проверить, что формула доказуемости $\Box'$ не удовлетворяет третьей аксиоме Бернайса (в предположении непротиворечивости ZF): контрпримером являются формулы $A = \perp'$ и $B = \perp$, где $\perp'$ обозначает какое-нибудь противоречие, отличное от $\perp$. Тогда формулы $\Box' A$ и $\Box'(A \to B)$ равносильны обычным формулам $\Box A$ и $\Box(A \to B)$. Поэтому формула

$\Box'(A \to B)$ выводима в ZF, а формула $\neg\Box' A$ не выводима (в предположении непротиворечивости ZF). С другой стороны, формула $\neg\Box' B$ выводима. Поэтому, если бы третья аксиома была выполнена для $\Box'$, то мы смогли бы вывести $\neg\Box' A$.

Теорема 5. *Если для теории непротиворечивой теории T оператор $\Box$ удовлетворяет всем трем аксиомам Бернайса и Принципу отражения (лемма 3), то в T не выводится формула $\neg\Box\bot$.*

Доказательство. По принципу отражения существует формула A, для которой в ZF, а значит и в T, выводимы формулы

$$\Box A \to \neg A, \qquad \neg\Box A \to A.$$

С помощью первой и третьей аксиом Бернайса из первой из этих формул выводима формула $\Box\Box A \to \Box\neg A$. С другой стороны, по второй аксиоме Бернайса выводится формула $\Box A \to \Box\Box A$. Поэтому выводима формула $\Box A \to \Box\neg A$.

Значит из утверждения о выводимости A следует утверждение о выводимости ее отрицания, то есть противоречивость теории T. Докажем это аккуратно. В исчислении высказываний, а значит и в T, выводима формула $A \to (\neg A \to \bot)$. С помощью первой и третьей аксиом Бернайса из этой формулы выводится формула $\Box A \to (\Box\neg A \to \Box\bot)$. Поэтому из уже выведенной формулы $\Box A \to \Box\neg A$ выводима формула $\Box A \to \Box\bot$.

Полезно сравнить вышеприведенное доказательство выводимости в T формулы $\Box A \to \Box\bot$ с с доказательством выводимости в ZF формулы $\Box A \to \Box\bot$, использованным в доказательстве теоремы 4 для ZF. Там мы сначала доказали, что из выводимости A в ZF следует противоречивость ZF, а потом просто сказали, что это доказательство было проведено в рамках самой теории множеств, поэтому в теории множеств выводима формула $\Box A \to \Box\bot$.

Дальше рассуждение в точности повторяет доказательство второй теоремы для ZF. Рассуждая от противного, допустим, что в T выводима формула $\neg\Box\bot$. Тогда из этой формулы и уже выведенной формулы $\Box A \to \Box\bot$ мы сможем вывести формулу $\neg\Box A$. С помощью формулы $\neg\Box A \to A$ мы тогда сможем вывести и формулу A, а затем с помощью первой аксиомы Бернайса и формулу $\Box A$. Таким образом, теория T противоречива вопреки предположению. $\Box$

Можно ли для данной непротиворечивой теории T как-нибудь выразить формулой $\mathrm{Pr}'(x)$ предикат доказуемости в T так, чтобы в теории T (а лучше в более слабой теории, чем T) можно было доказать непротиворечивость T? Для теории множеств кажется очевидным следующее. Пока не будет установлено, что эта формула $\mathrm{Pr}'(x)$ доказуемости равносильна "канонической" формуле $\mathrm{Pr}(x)$, новая формула доказуемости не будет признана адекватным способом выражения доказуемости. И иначе (если будет доказано, что новая формула доказуемости равносильна канонической), то для нее, очевидно, будет выполнена вторая теорема о неполноте.

Для произвольных же теорий T ситуация осложняется тем, что может не быть "канонического" способа записи доказуемости. Но даже и в этом случае, естественно потребовать, чтобы в теории T были выразимы синтаксические понятия и доказуемы их простые свойства. Разумеется, при этом необязательно представлять строки одной переменной, а можно, скажем двумя или тремя (или любым фиксированным числом). Также не обязательно требовать, чтобы у каждой строки было ровно одно имя — если это не так, то можно разрешить представлять предикат равенства строк более сложной формулой, чем формула $x = y$. Но в любом случае от любого "адекватного" способа представления строк естественно требовать выполнения свойств 1–5 или их аналогов. Что касается требований 6 и 7, то и они кажутся довольно законными. В самом деле, если субъект, рассуждающий о выводимости, не в состоянии доказать замкнутость множества выводимых формул относительно применения правила Modus Ponens или не в состоянии доказать утверждения о выводимости некоторой выводимой формулы, то вряд ли он вообще понимает, о м говорит! При всех этих предположениях в любой непротиворечивой теории T, в которой вообще возможно адекватным образом записать утверждение о ее непротиворечивости, это утверждение не доказуемо.