1. Формальная арифметика

1.1. Язык формальной арифметики

Цель формальной арифметики — аксиоматизировать множество натуральных чисел. В математических курсах обычно используются два способа аксиоматизации натуральных чисел.

При *первом способе* используются аксиомы Пеано:

1) 0 — натуральное число;

2) для каждого натурального числа существует вполне определенное натуральное число $S(x)$, называемое следующим за x;

3) $S(x) \neq 0$ для любого натурального числа x;

4) из $S(x) = S(y)$ следует $x = y$;

5) (принцип индукции) каждое множество натуральных чисел, содержащее 0 и вместе с каждым числом x содержащее $S(x)$, содержит все натуральные числа.

Далее определяется по индукции сложение и умножение натуральных чисел:

$$\begin{aligned} &x + 0 = x, \\ &x + S(y) = S(x + y), \\ &x \cdot 0 = 0, \\ &x \cdot S(y) = x \cdot y + x. \end{aligned}$$

Второй способ определения натуральных чисел, используемый в математических курсах, состоит в следующем. Сначала аксиоматически определяется множество действительных чисел, как полное упорядоченное поле. Затем натуральные числа определяются как действительные числа вида $1 + 1 + \cdots + 1$.

Оба этих способа нам не подходят по следующим причинам. Способ Пеано не подходит потому, что пятая аксиома Пеано использует понятие произвольного множества натуральных чисел. А мы хотим, чтобы в аксиомах не использовалось понятие множеств. Точнее следовало бы сказать, что мы требуем, чтобы все аксиомы были *формулами языка первого порядка*. Определение формул языка первого порядка мы дадим чуть ниже. Сейчас же объясним, чем плох второй способ. При этом способе натуральные числа получаются, как часть чего-то более широкого (действительных чисел). А мы не хотим, чтобы в аксиомах упоминалось что-либо, кроме натуральных чисел. К тому же при аксиоматизации действительных чисел опять используются средства, выходящие за рамки языка первого порядка. А именно, при аксиоматизации действительных чисел используется аксиома полноты, утверждающая, что любое ограниченное *множество* имеет верхнюю грань. Можно переформулировать эту аксиому в терминах последовательностей, но это будет не лучше, поскольку будет использовано понятие последовательности действительных чисел, не выразимое средствами языка первого порядка.

Что же мы имеем в виду, требуя, чтобы все аксиомы были формулами первого порядка? Дадим определение языка первого порядка в том конкретном случае, который нас интересует. Фиксируем некоторый набор символов, называемых *индивидными переменными*. Они предназначены для обозначения натуральных чисел; обычно в таком качестве используют латинские буквы с индексами. В каждой формуле будет использоваться конечное число переменных, так что счётного набора переменных нам хватит. Определим понятие *терма*. Термом называется последовательность переменных, запятых, скобок и символов $S, +, \cdot$ (символ S обозначает операцию $x + 1$), которую можно построить по следующим правилам:

- Индивидная переменная есть терм.

- Символ 0 есть терм.
- Если t — терм, то и $S(t)$ есть терм.
- Если t_2, t_2 — термы, то $(t_1{+}t_2)$ и $(t_1{\cdot}t_2)$ суть термы.

Если t_1, t_2 — термы, то выражения $(t_1 = t_2)$, $(t_1 \leqslant t_2)$ считаются *атомарными формулами*. Формулы строятся по таким правилам:

- Атомарная формула есть формула.
- Если φ — формула, то $\neg\varphi$ — формула.
- Если φ и ψ — формулы, то выражения $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$ также являются формулами.
- Если φ есть формула, а ξ — индивидная переменная, то выражения $\forall\xi\,\varphi$ и $\exists\xi\,\varphi$ являются формулами.

Итак, понятие формулы полностью определено. Такие формулы называют *формулами первого порядка* сигнатуры $(0, S, =, \leqslant, +, \cdot)$, или формулами *языка первого порядка* этой сигнатуры. Аналогично можно определить понятие формулы языка первого порядка произвольной сигнатуры. Но нас будут интересовать только языки первого порядка подсингатур сигнатуры $\{0, S, =, \leqslant, +, \cdot\}$. Для таких сигнатур σ можно просто сказать, что формулой (термом) языка первого порядка сигнатуры σ является произвольная формула (терм) языка первого порядка сигнатуры $\{0, S, =, \leqslant, +, \cdot\}$, в которую не входит ни один из символов из $\{0, S, =, \leqslant, +, \cdot\} \setminus \sigma$.

Вот примеры формул:

$$((x{+}0) = 0),\ \forall x\,(\exists y\,(x{+}y) \leqslant 0),\ \forall x\,\exists y\,(S(x) = (y{+}(y{+}y))).$$

Определим формально понятие *параметра* формулы (переменной, от значения которой может зависеть истинность формулы). Согласно этому определению, скажем, формула $\forall x\,\exists y\,(S(x) = y)$ не имеет параметров, а формулы $\exists y\,(S(x) = y)$ и $((S(x) = 0) \wedge \forall x\,(x \leqslant x))$ имеют

единственный параметр x. Вот как выглядит это определение:

- Параметрами терма являются все входящие в него индивидные переменные.
- Параметрами атомарной формулы являются параметры всех входящих в неё термов.
- Параметры формулы $\neg\varphi$ те же, что у формулы φ.
- Параметрами формул $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ и $(\varphi \to \psi)$ являются все параметры формулы φ, а также все параметры формулы ψ.
- Параметрами формул $\forall\xi\,\varphi$ и $\exists\xi\,\varphi$ являются все параметры формулы φ, кроме переменной ξ.

Параметры иногда называют *свободными переменными* формулы. Заметим, что формула может иметь одновременно параметр x и использовать (в другом месте) квантор $\forall x$. Как говорят в этом случае, одна и та же переменная имеет *свободные* и *связанные* вхождения. Свободное вхождение переменной — это такое вхождение, которое не входит в область действия одноимённого квантора. Если аккуратно определить эту область действия, несложно проверить, что параметры формулы — это как раз переменные, имеющие свободные вхождения.

1. Приведённые выше определения применимы к любой формуле, в том числе и к странной формуле $\forall z\,(x \leqslant y)$. Какие у неё параметры? При каких значениях параметров она истинна? (Ответ: она имеет параметры x, y и эквивалентна формуле $x \leqslant y$.)

Формулы, не имеющие параметров, называются *замкнутыми формулами*, а также *предложениями* или *суждениями*. Замкнутые формулы делятся на истинные и ложные. Чтобы говорить об истинности или ложности незамкнутой формулы, надо присвоить натуральные числа значениям её параметров. Например, формула

$\forall y\,\exists x\,(x = (y + y))$ истинна, а формула $\forall x\,(S(x) = 0)$ ложна. Формула $\exists y\,(x = (y + y))$ имеет единственный параметр x. Она истинна при любом чётном значении x и ложна при любом нечётном значении x. Сейчас мы не собираемся давать формального определения истинностного значения формулы при данном значении параметров, а сделаем это несколько позже в более общем случае.

Заметим, что мы разрешаем использовать в формулах только знаки операций сложения, умножения и добавления единицы, но не разрешаем, например, возведение в степень. Причина в том, что остальные употребительные отношения и функции определяются формулами этой сигнатуры. (Заметим в скобках, что операция добавления единицы и отношение порядка тоже могли бы быть выражены формулами, не содержащими этих функций и отношений, но нам удобнее оставить их в сигнатуре.) В этом параграфе мы расскажем, как это делается. n-местным отношением на множестве натуральных чисел называется произвольное подмножество $\mathbb{N}^n$. Отношение R часто отождествляется с функцией, принимающую значение 1 (или **И**) на всех кортежах, принадлежащих R, и 0 (или **Л**) на остальных. Такие функции называются *предикатами*. Мы говорим, что n-местное отношение R *выражается* формулой $\varphi(x_1, \ldots, x_n)$, если эта формула истинна на наборе натуральных чисел $a_1, \ldots, a_n$ тогда и только тогда, когда кортеж $\langle a_1, \ldots, a_n\rangle$ принадлежит отношению R. Формула *выражает* n-местную функцию f с натуральными аргументами и значениями, если она выражает $n+1$-местное отношение, состоящее из всех кортежей $\langle x_1, \ldots, x_n, y\rangle$, для которых $f(x_1, \ldots, x_n) = y$. Выразимые с помощью формул этой сигнатуры отношения и функции называются *арифметическими*. Соответствующие множества также называются *арифметическими*. Оказывается, что почти всякое отношение, которое можно описать словами, является арифметическим.

2. Докажите, что существует множество натуральных чисел, не являющееся арифметическим. (Указание: семейство всех подмножеств множества $\mathbb{N}$ несчётно, а арифметических множеств счётное число.)

Следующие свойства арифметических отношений следую непосредственно из определения.

- Если A и B арифметические отношения одной размерности, то их пересечение и объединение арифметичны.
- Если A арифметическое отношение, то его дополнение (до $\mathbb{N}^k$, где k размерность A) арифметично.
- Проекция арифметического отношения есть арифметическое отношение (проекцией $n+1$-местного отношения A называется n-местное отношение $\{\langle k_1, \ldots, k_n\rangle \mid \exists k_{n+1}\, \langle k_1, \ldots, k_n, k_{n+1}\rangle \in A\}$).

Для начала мы установим арифметичность довольно простых отношений.

- Предикат $x \leqslant y$ является арифметическим. В самом деле, его можно записать как $\exists z\,(x + z = y)$. Аналогичным образом выражается отношение $x < y$: $\exists z\,(x + S(z) = y)$. Можно воспользоваться и тем, что $x < y$, если $x \leqslant y$ и $x \neq y$.
- Предикат $x = 1$ являются арифметическими. В самом деле, $x = 1$ тогда и только тогда, когда $x = S(0)$. (Можно также воспользоваться тем, что 1 наименьшее число, отличное от нуля, или что $y \cdot 1 = y$ при любом y.)
- Вообще для любого фиксированного числа c предикат отношение $x = c$ является арифметическим. Например, можно написать $x = S(S(\ldots S(0)\ldots))$.
- Полезно такое общее наблюдение: если мы уже установили, что какое-то отношение является арифметическим, то в дальнейшей его можно использовать в формулах, как если бы оно входило в сигнатуру,

поскольку его всегда можно заменить на выражающую его формулу. То же самое относится и к арифметическим функциям. Например, если функция $f(x)$ выражается формулой $A(x,y)$ (то есть, $(f(x)=y) \leftrightarrow A(x,y)$), то формулу $f(x)+z=y$ можно заменить на формулу $\exists u\,(A(x,u) \wedge (u+z=y))$.

- Предикат $x|y$ (число x является делителем числа y), очевидно, арифметичен (формула $\exists z\,(xz=y)$).

- Предикат «x — простое число» арифметичен. В самом деле, число просто, если оно отлично от 1 и любой его делитель равен 1 или самому числу. Это сразу же записывается в виде формулы.

- Операции частного и остатка арифметичны (в том смысле, что трёхместные отношения «q есть частное при делении a на b» и «r есть остаток при делении a на b» арифметичны. Например, первый из них записывается формулой $\exists r\,((a=bq+r) \wedge (r<b))$ (как мы уже говорили, использование арифметического отношения $(r<b)$ не создаёт проблем).

- Этот список можно продолжать: для многих отношений их определение по существу уже является нужной формулой. Например, свойства «быть наибольшим общим делителем», «быть наименьшим общим кратным», «быть взаимно простыми» все относятся к этой категории.

- Предикат «быть степенью двойки» является арифметическим (хотя это и не столь очевидно, как в предыдущих примерах). В самом деле, это свойство можно переформулировать так: любой делитель либо равен единице, либо чётен.

Последнее из наших рассуждений годится для степеней тройки и вообще для степеней любого простого числа. Однако уже для степеней четвёрки оно не проходит,

и, пожалуй, мы подошли к границе, где без некоторого общего метода не обойтись.

Два наиболее известных способа доказывать арифметичность основаны на возможности «кодирования» конечных множеств и последовательностей. Один восходит к Гёделю (так называемая β-функция Гёделя), второй изложен в книге «Теория формальных систем» [2] Р. Смаллиана.

Мы изложим первый способ, как более простой. β-функцией Гёделя называется функция

$$\beta(a,b,i) = \text{остаток от деления } a \text{ на } b(i+1)+1.$$

Поскольку отношение «x есть остаток при делении y на z» записывается формулой $\exists q\,((y=q\cdot z+x) \wedge x<z)$, β-функцией Гёделя арифметична. Основное её свойство заключается в следующей теореме.

Теорема 1. Для любой конечной последовательности натуральных чисел $k_0, k_1, \ldots, k_{l-1}$ существуют такие a, b, что $\beta(a,b,i)=k_i$ для всех $i<k$.

$\lhd$ Сначала докажем, что найдётся натуральное число b, большее всех чисел $k_0, k_1, \ldots, k_{l-1}$, для которого числа $b+1, 2b+1, \ldots, lb+1$ попарно взаимно просты. Положим, например, $b=l!\cdot(\max\{k_0,k_1,\ldots,k_{l-1}\}+1)$. Тогда любой простой общий делитель p двух разных чисел $ib+1$ и $jb+1$ из списка $b+1,\ 2b+1,\ \ldots,\ lb+1$ делит и их разность, следовательно делит $i-j$ или b. Поскольку b кратно $i-j$, в любом случае p делит b. Но тогда p не может делить ни одно из этих чисел.

Осталось применить китайскую теорему об остатках. Её формулировка такова:

- Если натуральные числа $d_0, d_1, \ldots, d_{l-1}$ попарно взаимно просты и $k_0, k_1, \ldots, k_{l-1}$ произвольные натуральные числа, то существует натуральное число a, сравнимое с k_i по модулю d_i для всех $i<l$.

Эта теорема доказывается так. Сначала докажем утверждение для $l=2$: если x, y взаимно просты, а r, s

произвольные натуральные числа, то найдется a, сравнимое с r по модулю x и с s по модулю y. По известной из алгебры теореме найдутся целые u, v, для которых выполнено $ux + vy = 1$. Положим $a = r + (s - r)ux$. Ясно, что a сравнимо с r по модулю x. Поскольку $ux + vy = 1$, число u является обратным элементом к x по модулю y, поэтому $a \equiv r + (s - r) \equiv s \pmod{y}$. Можно и не использовать свойства сравнений, представив a в виде $a = r + (s - r)ux = r + (s - r)(1 - vy) = s + (r - s)vy$.

Далее используем индукцию по j. База индукции: для $j = 1$ утверждение очевидно. Индуктивный переход: пусть a сравнимо с k_i по модулю d_i для всех $i < j$. Положим $c = d_0 \cdot d_1 \cdots d_{j-1}$. Число d_j взаимно просто с каждым из чисел $d_0, d_1, \ldots, d_{j-1}$, поэтому оно взаимно просто и с c, следовательно найдется a', сравнимое с a по модулю c и с k_j по модулю d_j. Ясно, что a' сравнимо с k_i по модулю d_i при всех $i < j$.

Если найденное число a отрицательно, то можно добавить к нему достаточно большое общее кратное $d_0, d_1, \ldots, d_{l-1}$. $\triangleright$

Теперь функцию x^y можно выразить с помощью β-функции Гёделя, например, так: $x^y = z$, если найдутся a и b такие, что, во-первых, $\beta(a, b, 0) = 1$, во-вторых, $\beta(a, b, i + 1) = \beta(a, b, i) \cdot x$ для всех $i < y$ и, в-третьих, $\beta(a, b, y) = z$.

Удобно считать, что кроме индивидных переменных, пробегающих натуральные числа, имеются переменные, пробегающие конечные последовательности натуральных чисел. Будем называть их переменными второго порядка и обозначать греческими буквами. Добавляется новое правило образования термов: если τ терм, а α переменная второго порядка, то выражения $\alpha(\tau)$ и $|\alpha|$ суть термы ($|\alpha|$ обозначает длину последовательности α). А к правилам образования формул добавляется такое: если φ формула, то выражения $\forall\alpha\,\varphi$ и $\exists\alpha\,\varphi$ суть формулы. Любую формулу в расширенном таким образом языке можно перевести в равносильную формулу

первого порядка исходной сигнатуры. Для этого надо сопоставить с каждой переменной второго порядка α тройку индивидных переменных a, b, l (разным переменным второго порядка должны соответствовать непересекающиеся тройки). Затем надо заменить вхождения выражений $\alpha(\tau)$, $|\alpha|$, $\forall\alpha$, $\exists\alpha$ на выражения $\beta(a, b, \tau)$, l, $\forall l\,\forall a\,\forall b$, $\exists l\,\exists a\,\exists b$, соответственно.

Функция $f\colon \mathbb{N}^k \to \mathbb{N}$ называется *вычислимой*, если есть алгоритм, который по произвольным натуральным числам $n_1, \ldots, n_k$ находит $f(n_1, \ldots, n_k)$. С помощью β-функции Гёделя нетрудно доказать, что любая вычислимая функция арифметична.

Теорема 2. Любая вычислимая функция арифметична.

$\triangleleft$ Пусть функция $f\colon \mathbb{N}^k \to \mathbb{N}$ вычислима. Нам нужно написать формулу с параметрами $n_1, \ldots, n_k, m$, истинную тогда и только тогда, когда $f(n_1, \ldots, n_k) = m$. По условию существует машина Тьюринга, вычисляющая функцию f. То есть, получив $n_1, \ldots, n_k$ на вход машина должна выдать на выход m. Мы будем считать, что лента машины бесконечна только вправо, и ячейки нумеруются натуральными числами. Будем считать, что числа $n_1, \ldots, n_k$ даются машине в виде k последовательностей из единиц длин $n_1, \ldots, n_k$, разделённых нулями, написанных в начале ленты, а все остальные ячейки ленты заполнены нулями. Будем считать, что выход должен быть написан в той же форме. То есть, начав работу в состоянии 1 (будем считать, что состояниями являются натуральные числа) на ленте с указанным содержимым, через какое-то количество шагов машина должна остановиться. После остановки в клетках с номерами от 0 до $m - 1$ должны быть записаны единицы, а в клетке с номером m записан 0. Будем считать, что машина останавливается, как только она приходит в состояние 0. Перенумеруем ленточные символы так, что символам 0, 1 присвоены номера 0, 1, соответственно.

Пусть машина остановилась на данном входе n_1, …, n_k через t шагов, и пусть s любое число, большее но-

мера самой правой ячейки, в которой побывала машина. Тогда работа машины полностью задаётся двумя последовательностями натуральных чисел длины $t+1$, задающими состояние машины и положение головки в моменты $0,\ldots,t+1$ а также матрицей из натуральных чисел размера $(t+1)\times s$, задающей содержимое первых s клеток ленты в каждый из моментов $0,\ldots,t+1$. Будем называть эти две последовательности и матрицу *протоколом* работы машины на данном входе. Любую матрицу из натуральных чисел также нетрудно задать с помощью последовательности натуральных чисел. Например, можно считать, что матрица размера $(t+1)\times s$ задаётся последовательностью α длины $2(t+1)s$ следующим образом. Элемент, стоящий в строке i и столбце j равен $\beta(\alpha(2i),\alpha(2i+1),j)$. Будем в дальнейшем обозначать последнее выражение через $\alpha(i,j)$.

Итак, будем задавать протокол работы тремя последовательностями St (состояния машины), Pos (положения головки) и Sym (где $Sym(i,j)$ номер символа в j-ой клетке на шаге i). Теперь напишем четыре формулы φ_{gen}, φ_{beg}, φ_{end}, φ_{step}. Формула φ_{gen} имеет параметры $n_1,\ldots,n_k,m,s,t,Sym,Pos,St$ и утверждает что s больше m и больше номеров всех ячеек, в которых побывала машина (т.е., $Pos(i)<m$ для всех $i\leqslant t$), и что состояния машины в моменты $1,\ldots,t-1$ отличны от 0 (т.е., $St(i)\neq 0$ для всех $0<i<t$). Формула φ_{beg} имеет параметры $n_1,\ldots,n_k,Sym$ и утверждает, что начальное содержимое первых s клеток ленты соответствует данному входу $n_1,\ldots,n_k$ (т.е., $Sym(0,j)=1$ для всех $0<j<n_1$, $Sym(0,n_1)=0$, $Sym(0,j+n_1)=1$ для всех $0<j<n_2$ и т. д.), состояние машины в момент 0 равно 1, и головка в начальный момент находится в нулевой клетке ($Pos(0)=0$). Формула φ_{end} имеет параметры m,Sym,St и утверждает, что в момент t состояние машины равно 0, в клетках с номерами от 0 до $m-1$ записаны единицы, а в клетке с номером m записан 0. Формула φ_{step} имеет параметры s,t,Sym,Pos,St и имеет вид $(\forall i<t)\,\psi_{step}$,

где формула ψ_{step} утверждает, что состояние машины в момент $i+1$ получается из состояния и обозреваемого символа в момент i в соответствии с программой машины, и то же самое для положения головки. Кроме того, формула ψ_{step} говорит, какими должны быть символы на ленте в момент $i+1$: все символы, кроме символа обозреваемого головкой в момент $i+1$ те же, что и в момент i, а этот символ получается в соответствии с программой машины. Чтобы написать формулу ψ_{step} надо, конечно, знать программу машины: формула как-бы содержит в себе эту программу. Например, если в программе машины имеется команда: «находясь в состоянии 3 и видя на ленте символ 1, заменить 1 на 0, сдвинуть головку вправо и перейти в состояние 2», то в формулу ψ_{step} добавляется конъюнктивный член

$$\begin{gathered}(St(i)=\overline{3}\wedge Sym(i,Pos(i))=\overline{1})\to\\ \to(Sym(i+1,Pos(i)))=0\wedge\\ \wedge St(i+1)=\overline{2}\wedge Pos(i+1)=Pos(i)+1\wedge(\forall j<s)\\ (j\neq Pos(i)\to Sym(i+1,j)=Sym(i,j)).\end{gathered}$$

Формула ψ_{step} равна конъюнкции всех таких членов.

Формула $\tau(n_1,\ldots,n_k,m)$, полученная из формулы $\varphi_{\text{gen}}\wedge\varphi_{\text{beg}}\wedge\varphi_{\text{end}}\wedge\varphi_{\text{step}}$ навешиванием кванторов существования по всем параметрам, кроме $n_1,\ldots,n_k,m$, и выражает функцию f. Докажем аккуратно, что это действительно так. Это доказательство нам пригодится в будущем.

Нам нужно доказать, что

$$\forall m\,(\tau(n_1,\ldots,n_k,m)\leftrightarrow m=f(n_1,\ldots,n_k)).$$

Докажем сначала импликацию справа налево. Пусть $m=f(n_1,\ldots,n_k)$. Тогда наша машина выдает m на входе $n_1,\ldots,n_k$. Запустим машину на этом входе и запишем протокол её работы. Определим значения параметров s,t,Sym,Pos,St так, чтобы они описанным выше

образом задавали этот протокол. Тогда без труда проверяется, что все четыре формулы φ_{gen}, φ_{beg}, φ_{end} и φ_{step} истинны.

Докажем импликацию слева направо. Пусть для некоторых s, t, Sym, Pos, St истинны все четыре формулы φ_{gen}, φ_{beg}, φ_{end}, φ_{step}. Последнее означает, что формула ψ_{step} истинна для всех $i < t$. Нам надо доказать, что тогда m равно выходу машины при работе на входе $n_1, \ldots, n_k$. Для этого докажем, что s, t, Sym, Pos, St правильно кодируют вычисление машины на входе $n_1, \ldots, n_k$.

Одновременной индукцией по $i = 0, \ldots, t$ докажем следующие утверждения: (1) $St(i)$ равно состоянию машины на шаге i, (2) $Pos(i)$ равно номеру клетки, обозреваемой головкой на шаге i, (3) $Sym(i, j)$ равно номеру символа, содержащегося в клетке номер j на шаге i (для всех $j < s$). База индукции: формула φ_{beg} как раз и содержит утверждения (1), (2) и (3) для $i = 0$. Индуктивный переход. Пусть (1), (2) и (3) верны для некоторого $i < t$. Докажем, что они верны для $i{+}1$. Пусть на шаге i головка находится в состоянии q и обозревает ячейку номер c, в которой записан символ номер h. По индуктивному предположению мы имеем $q = St(i)$, $c = Pos(i)$, $h = Sym(i, c)$, а из формулы φ_{gen} следует, что $q \neq 0$. Найдём в программе ту команду, которая в данный момент выполняется. Пусть, скажем, машина должна записать в обозреваемую клетку символ с номером 5, сдвинуться влево и перейти в состояние 4. Поскольку соответствующий этой команде конъюнктивный член и его посылка

$$\begin{gathered}(St(i) = \overline{q} \wedge Sym(i, Pos(i)) = \overline{h}) \to \\ \to (Sym(i+1, Pos(i)) = \overline{5} \wedge \\ \wedge St(i+1) = \overline{4} \wedge Pos(i+1) = Pos(i) - 1 \wedge (\forall j < s) \\ (j \neq Pos(i) \to Sym(i+1,) = Sym(i, j))\end{gathered}$$

формулы φ_{step} истинны, мы заключаем, что $St(i+1) = 4$ (т. е. $St(i+1)$ равно состоянию машины на шаге $i+1$), $Pos(i{+}1) = c{-}1$ (т. е. $Pos(i{+}1)$ равно номеру клетки, обозреваемой на шаге $i{+}1$). Осталось доказать, что $Sym(i{+}1, j)$ равно номеру символа, содержащегося в клетке j на шаге $i+1$. Для $j = c$ это следует из истинности $Sym(i{+}1, Pos(i))$, а для остальных $j < s$ из $(j \neq Pos(i) \to Sym(i+1,) = Sym(i, j))$ и индуктивного предположения.

В формуле φ_{end} записано, что $Sym(t, j) = 1$ для всех $j < m$ и $Sym(t, m) = 0$. С другой стороны мы доказали, что $Sym(t, j) = 1$ равно номеру символа, содержащегося в клетке номер j на шаге t для всех $j < s$. Поскольку $m < s$ (что записано в формуле φ_{gen}), в момент остановки машины в первых m клетках написаны единицы, а в m-ой клетке 0, что и требовалось доказать. $\triangleright$

Отношение $R \subset N^k$ называется *разрешимым*, если есть алгоритм, который по произвольным натуральным числам $n_1, \ldots, n_k$ определяет, принадлежит ли кортеж $\langle n_1, \ldots, n_k \rangle$ множеству R. По-другому можно сказать, что предикат, соответствующий отношению, вычислим. Из доказанной теоремы легко следует, что любое разрешимое отношение арифметично. Действительно, предикат, соответствующий разрешимому k-местному отношению R выражается некоторой формулой с $k+1$ параметром. Подставив вместо последнего параметра $\overline{1}$, мы получим формулу, выражающую R.

Теперь сформулируем теорему Тарского о неарифметичности множества номеров истинных формул. Для этого перенумеруем множество всех формул любым способом, но так, чтобы по n можно было найти формулу с номером n (с помощью некоторого алгоритма). Будем обозначать n-ую формулу через ψ_n.

Теорема 3. Множество $\{n \mid$ формула ψ_n замкнута и истинна$\}$ не является арифметическим.

$\triangleleft$ Пусть A произвольное арифметическое множество. Нам достаточно построить замкнутую формулу φ такую, что

$$\varphi \text{ истинна } \Leftrightarrow (\text{номер } \varphi) \notin A$$

Иными словами φ должна утверждать, что её номер не

принадлежит множеству A. Это делается с помощью такого трюка.

Пусть $\overline{k}$ обозначает терм $S(S(\dots S(0)\dots))$, где S повторяется k раз. Рассмотрим функцию Subst, отображающую число n в номер формулы, получающейся из ψ_n подстановкой терма $\overline{n}$ вместо её параметра (если у ψ_n несколько параметров или вообще нет параметров, положим, например, $\mathrm{Subst}(n) = 0$). Эта функция очевидно вычислима. Напишем формулу $\mathrm{Subst}(n, m)$, выражающую эту функцию, так, как это было сделано в доказательстве теоремы 2. Пусть $A(x)$ обозначает формулу, выражающую отношение $x \in A$. Рассмотрим формулу

$$\neg\exists k\,(\mathrm{Subst}(n, k) \wedge A(k)),$$

обозначим её через $\eta(n)$, а её номер через N. По построению, она обладает таким свойством: для любой формулы ψ_n с одним параметром формула $\eta(\overline{n})$ истинна тогда и только тогда, когда номер формулы $\psi_n(\overline{n})$ не принадлежит A. Следовательно, формула $\eta(\overline{N})$ истинна тогда и только тогда, когда её номер не принадлежит A. Поэтому формулу $\eta(\overline{N})$ можно взять в качестве искомой формулы φ. $\triangleright$

1.2. Первая теорема Гёделя о неполноте

Вернёмся теперь к нашей цели — аксиоматизировать натуральные числа формулами языка первого порядка. Системой аксиом мы будем называть произвольное множество истинных замкнутых формул сигнатуры $\{0, S, =, \leqslant, +, \cdot\}$. Чего мы хотим от системы аксиом? Во-первых, чтобы у неё было поменьше моделей (понятие модели будет дано ниже). В идеале, любая модель должна быть изоморфна натуральному ряду. Если это так, то мы говорим что натуральный ряд аксиоматизирован с точностью до изоморфизма. Во-вторых, мы хотим чтобы побольше истинных формул следовало из аксиом. По определению, формула φ следует из системы аксиом T, если φ

истинна во всех моделях T. Поэтому второе требование к системе аксиом связано с первым: чем меньше моделей у системы аксиом, тем больше формул из неё следует. В идеале, любая истинная формула должна следовать из T. Если это выполнено, то система аксиом называется *полной*. Например, система аксиом полна, если она аксиоматизирует натуральный ряд с точностью до изоморфизма. По известной теореме Гёделя о полноте формула φ следует из T, тогда и только тогда, когда φ выводится из T в исчислении предикатов. Поэтому второе требование к T можно переформулировать так: мы хотим чтобы побольше истинных формул выводилось из T в исчислении предикатов.

Перейдём к определению модели данной системы аксиом и определению понятия изоморфизма. Для этого определим понятие *интерпретации* сигнатуры $\{0, S, =, \leqslant, +, \cdot\}$. Двуместным отношением на множестве M назовём произвольное подмножество M^2.

Чтобы задать интерпретацию сигнатуры $\{0, S, =, \leqslant, +, \cdot\}$, необходимо:

- указать некоторое непустое множество M, называемое *носителем* интерпретации;
- указать два двуместных отношения на множестве M; эти отношения интерпретируют символы $=, \leqslant$;
- указать некоторый элемент множества M, он интерпретирует символ 0;
- указать одноместную функцию с аргументами и значениями из M и две двуместных функции с аргументами и значениями из M; они интерпретируют символы $S, +, \cdot$.

Если символ равенства $=$ интерпретируется как совпадение элементов множества M (то есть отношением

$\{\langle x, x\rangle \mid x \in M\}$), то интерпретация называется *нормальной*. Интерпретация, носитель которой есть множество натуральных чисел, а символы $0, S, =, \leqslant, +, \cdot$ интерпретируются обычным образом, называется *стандартной интерпретацией* сигнатуры $\{0, S, =, \leqslant, +, \cdot\}$.

Теперь мы хотим определить понятие формулы, истинной при данных значениях параметров в данной интерпретации. Технически проще считать, что всем индивидным переменным приписаны какие-то значения, а потом доказать, что переменные, не являющиеся параметрами, не влияют на истинность формулы.

Итак, *оценкой* назовём отображение, которое ставит в соответствие каждой индивидной переменной некоторый элемент M. Этот элемент будем называть *значением переменной* при данной оценке. Определим индуктивно *значение терма* t при данной оценке π, которое мы будем обозначать $[t](\pi)$.

- Для переменных оно уже определено.
- Если t есть символ 0, то $[t](\pi)$ не зависит от π и равно элементу, интерпретирующему символ 0.
- Если t имеет вид $S(t_1)$, где t_1 — терм, то $[t](\pi)$ есть $[S](\pi)$, где $[S]$ обозначает функцию, интерпретирующую символ S.
- Если t имеет вид $(t_1 + t_2)$, где t_1, t_2 — термы, то $[t](\pi)$ есть $([t_1](\pi))[+]([t_2](\pi))$, где $[+]$ обозначает функцию, интерпретирующую символ $[+]$ (по традиции мы написали значок $[+]$ между аргументами, а не перед ними). Аналогично определяется $[t](\pi)$ для t, равного $(t_1 \cdot t_2)$.

Теперь можно определить *значение формулы* φ при данной оценке π в данной интерпретации, которое обозначается $[\varphi](\pi)$ и может быть равно **И** или **Л**; в первом случае формула называется *истинной*, во втором — *ложной*. Это определение также индуктивно:

- Значение атомарной формулы $(t_1 = t_2)$ равно **И**, если пара $\langle [t_1](\pi), [t_2](\pi)\rangle$ принадлежит отношению, интерпретирующему символ $=$, и **Л** иначе. Аналогично определяется значение атомарной формулы $(t_1 \leqslant t_2)$
- $[\neg\varphi](\pi)$ определяется как $\neg[\varphi(\pi)]$, где $\neg$ понимается как операция в $\{\mathbf{И}, \mathbf{Л}\}$, определённая правилом $\neg\mathbf{И} = \mathbf{Л}, \neg\mathbf{Л} = \mathbf{И}$. Другими словами, формула $\neg\varphi$ истинна при оценке π тогда и только тогда, когда формула φ ложна при этой оценке.
- $[\varphi \wedge \psi](\pi)$ определяется как $[\varphi](\pi) \wedge [\psi](\pi)$, где $\wedge$ в правой части понимается как операция в $\{\mathbf{И}, \mathbf{Л}\}$: $\mathbf{И}\wedge\mathbf{И} = \mathbf{И}, \mathbf{И}\wedge\mathbf{Л} = \mathbf{Л}\wedge\mathbf{И} = \mathbf{Л}\wedge\mathbf{Л} = \mathbf{Л}$. (Другими словами, формула $(\varphi \wedge \psi)$ истинна при оценке π тогда и только тогда, когда обе формулы φ и ψ истинны при этой оценке.) Аналогичным образом $[\varphi \vee \psi](\pi)$ определяется как $[\varphi](\pi) \vee [\psi](\pi)$, а $[\varphi \to \psi](\pi)$ — как $[\varphi](\pi) \to [\psi](\pi)$, где $\mathbf{И} \vee \mathbf{И} = \mathbf{И} \vee \mathbf{Л} = \mathbf{Л} \vee \mathbf{И} = \mathbf{И}$, $\mathbf{Л} \vee \mathbf{Л} = \mathbf{Л}$; $(\mathbf{И} \to \mathbf{И}) = (\mathbf{Л} \to \mathbf{И}) = (\mathbf{Л} \to \mathbf{Л}) = \mathbf{И}$, $(\mathbf{И} \to \mathbf{Л}) = \mathbf{Л}$.
- Формула $\forall\xi\,\varphi$ истинна на оценке π тогда и только тогда, когда формула φ истинна на любой оценке π', которая совпадает с π всюду, кроме значения переменной ξ (которое в оценке π' может быть любым). В противном случае формула $\forall\xi\,\varphi$ ложна на оценке π.
- Формула $\exists\xi\,\varphi$ истинна на оценке π тогда и только тогда, когда формула φ истинна на некоторой оценке π', которая совпадает с π всюду, кроме значения переменной ξ (которое в оценке π' может быть любым). В противном случае формула $\exists\xi\,\varphi$ ложна на оценке π.

Заметим, что в двух последних пунктах значение переменной ξ в оценке π не играет роли. Это позволяет лег-

ко доказать (индукцией по построению формулы) такое утверждение: если две оценки π_1 и π_2 придают одинаковые значения всем параметрам формулы φ, то $[\varphi](\pi_1) = [\varphi](\pi_2)$. Другими словами, истинность формулы определяется значениями её параметров.

Интерпретация называется *моделью* множества замкнутых формул T, если все формулы из T истинны в ней.

Изоморфизмом интерпретаций называется биекция f между их носителями M_1 и M_2, сохраняющая элементы, функции и отношения, сопоставленные сигнатурным символам. Это означает следующее. Пусть $\lfloor 0\rfloor$, $\lfloor S\rfloor$, $\lfloor +\rfloor$, $\lfloor\cdot\rfloor$, $\lfloor =\rfloor$, $\lfloor\leqslant\rfloor$ обозначают интерпретации сигнатурных символов при первой интерпретации, а $\lceil 0\rceil$, $\lceil S\rceil$, $\lceil +\rceil$, $\lceil\cdot\rceil$, $\lceil =\rceil$, $\lceil\leqslant\rceil$ обозначают интерпретации этих же символов при второй интерпретации. Тогда должно быть выполнено

$$f(\lfloor 0\rfloor) = \lceil 0\rceil,$$
$$y = \lfloor S\rfloor(x) \leftrightarrow f(y) = \lceil S\rceil(f(x)),$$
$$(z = x\lfloor +\rfloor y) \leftrightarrow (f(z) = f(x)\lceil +\rceil f(y)),$$
$$(z = x\lfloor\cdot\rfloor y) \leftrightarrow (f(z) = f(x)\lceil\cdot\rceil f(y)),$$
$$(x\lfloor =\rfloor y)) \leftrightarrow (f(x)\lceil =\rceil f(y)),$$
$$(x\lfloor\leqslant\rfloor y) \leftrightarrow (f(x)\lceil\leqslant\rceil f(y)).$$

(По традиции мы вместо $\langle x, y\rangle \in \lfloor =\rfloor$ пишем $x\lfloor =\rfloor y$.)

Теорема 4. Любое множество предложений, истинных в стандартной интерпретации, имеет нормальную модель, не изоморфную стандартной интерпретации.

$\lhd$ Добавим в сигнатуру новый символ c. При интерпретации ему должен сопоставляться некоторый элемент носителя интерпретации. Соответственно изменяется и определение терма. А именно, символ c также считается термом (и тем самым может входить в другие термы). А в определение значения терма в данной интерпретации на данной оценке добавляется пункт:

- Если t есть символ c, то $[t](\pi)$ не зависит от π и равно элементу, интерпретирующему символ c.

Пусть T — произвольное множество предложений, истинных в стандартной интерпретации. Добавим к T такие формулы: $\neg(c = 0)$, $\neg(c = S(0))$, $\neg(c = S(S(0)))$ и т. д.. Обозначим полученное множество формул (языка первого порядка сигнатуры $\{0, c, S, =, \leqslant, +, \cdot\}$) через T'. Докажем, что множество T' имеет модель. Для этого воспользуемся теоремой компактности (см., напр., [1]): если любое конечное подмножество данного множества формул имеет нормальную модель, то и само множество имеет нормальную модель. Для этот докажем, что любое конечное подмножество $T'' \subset T'$ имеет модель. Действительно, в T'' входит лишь конечное множество формул вида $\neg(c = 0)$, $\neg(c = S(0))$, $\neg(c = S(S(0)))$, $\ldots$. Пусть n любое число, для которого формула $\neg(c = S(\ldots S(0))$ (n раз) не входит в T''. Тогда модель T'' можно получить, взяв стандартную интерпретацию и сопоставив символу c число n.

Итак, пусть M любая модель T'. Будем рассматривать M как интерпретацию исходной сигнатуры $\{0, S, =, \leqslant, +, \cdot\}$. Поскольку T является частью T', интерпретация M является моделью и T. Осталось доказать, что M не изоморфна стандартной интерпретации. Допустим, что биекция f из $\mathbb{N}$ в носитель M осуществляет изоморфизм стандартной интерпретации и M. Тогда $f(0)$ должно быть равно $[0]$ — интерпретации символа 0 в M. Поскольку f сохраняет интерпретацию символа S, мы можем заключить, что для всех $n, m \in \mathbb{N}$ выполнено $m = n + 1 \leftrightarrow f(m) = [S](f(n))$, где $[S]$ — интерпретация символа S в M. То есть $f(1) = [S]([0])$, $f(2) = [S](f(1))$ и т. д.. Поэтому множество значений функции f совпадает с множеством элементов $\{[0], [S]([0]), [S]([S]([0])), \ldots\}$. Но это множество строго меньше, чем носитель M, так как носитель M должен содержать интерпретацию символа c. А поскольку каждая из формул $c \neq 0$, $c \neq S(0)$,

$c \neq S(S(0)), \ldots$ истинна в M, интерпретация символа c отлична от всех элементов $[0], [S]([0]), [S]([S]([0])), \ldots$. $\triangleright$

Итак, даже если в качестве аксиом взять *все* истинные в стандартной интерпретации формулы, мы не получим аксиоматизации натурального ряда с точностью до изоморфизма. Остаётся надежда найти полную систему аксиом. Полную аксиоматизацию можно получить тривиальным образом: достаточно в качестве аксиом взять все истинные в стандартной интерпретации формулы. Однако естественно искать полное *разрешимое* множество аксиом (напомним, что это означает существование алгоритма, который по произвольной формуле определяет, является ли она аксиомой).

Теорема 5 (Первая теорема Гёделя о неполноте). Не существует разрешимого множества формул T такого, что множество формул, выводимых из T в исчислении предикатов, совпадает с множеством формул, истинных в стандартной интерпретации.

$\triangleleft$ Допустим такое множество T существует. Перенумеруем множество всех формул так, чтобы по номеру можно было найти формулу с этим номером (с помощью некоторого алгоритма). Перенумеруем все выводы так, чтобы по номеру вывода можно было восстановить сам вывод. Будем обозначать n-ую формулу через ψ_n, а m-ый вывод p_m. Рассмотрим множество

$$\{\langle n, m\rangle \mid p_m \text{ есть вывод замкнутой формулы } \psi_n \text{ из } T\}.$$

Поскольку T разрешимо, это множество также разрешимо, а следовательно арифметично. Но тогда и множество номеров истинных замкнутых формул арифметично, поскольку получается из этого множества проекцией. А это противоречит теореме Тарского. $\triangleright$

1.3. Аксиоматизация арифметики для бедных языков

Как мы видели, не существует разрешимой аксиоматизации для множества формул, истинных в стандартной интерпретации. В этом параграфе мы рассмотрим обеднённые сигнатуры, получающиеся из исходной удалением одной или нескольких функций или отношений. А именно, мы рассмотрим следующие три сигнатуры $\{0, S, =\}$, $\{0, S, \leqslant, =\}$ и $\{0, S, +, \leqslant, =\}$. Для этих трёх сигнатур существуют полные аксиоматизации и мы их построим. Заметим, что аксиоматизировать натуральный ряд с точностью до изоморфизма ни в одном из обеднённых языков невозможно, поскольку этого нельзя сделать в исходном языке. Впрочем мы ещё предъявим для каждой из трёх сигнатур интерпретацию, элементарно эквивалентную стандартной, но не изоморфную ей. (Интерпретации называются элементарно эквивалентными в данном языке, если в них истинны одни и те же замкнутые формулы первого порядка данного языка.) Большинство утверждений этого параграфа приводятся без доказательства.

1. Сигнатура $\{0, S, =\}$

В этом случае в качестве аксиом естественно взять такие формулы $\forall x\,(S(x) \neq 0)$, $\forall y\,(y \neq 0 \to \exists x\, S(x) = y)$, $\forall x \forall y (S(x) = S(y) \to x = y)$. Однако только этих трёх формул недостаточно: например, из них не следует, что $S(x) \neq x$ для всех x. (В качестве контр-модели можно взять натуральный ряд и добавить к нему новый элемент a, положив $S(a) = a$; легко проверить, что все три аксиомы выполнены, а формула $\forall x\,(S(x) \neq x)$ — нет.) Но добавлением одной только формулы $\forall x\,(S(x) \neq x)$ дела не исправить, поскольку из расширенной этой формулой системы аксиом не будет следовать формула $\forall x\,(S(S(x)) \neq x)$. (В качестве контр-модели можно взять натуральный ряд и добавить к нему два новых элемента a, b, положив $S(a) = b$, $S(b) = a$; легко проверить, что все три аксиомы и формула $\forall x\,(S(x) \neq x)$ выполнены, а формула $\forall x\,(S(S(x)) \neq x)$ — нет.) Поэтому мы вынуждены добавить для каждого натурального n формулу $\forall x\,(S(S(\ldots S(x)\ldots)) \neq x)$ (n раз). Полученное множество

формул T является полным. Доказательство этого факта можно прочитать в книге [1, стр. 216]. Точнее, там построена полная система аксиом для целых чисел (то есть добавляются ещё и отрицательные числа) в сигнатуре $\{0, S, =\}$ и доказана её полнота. Доказательство легко изменить применительно к нашему случаю.

Интересно представить устройство моделей теории T. Для произвольного множества A можно рассмотреть следующую модель T. Её носитель — объединение множеств $\mathbb{N}$ и $A \times \mathbb{Z}$. Символ S интерпретируется так: на $\mathbb{N}$ это обычное добавление 1, а на элементах $A \times \mathbb{Z}$ — добавление 1 ко второму компоненту пары. Легко проверить, что все аксиомы выполнены. Эта модель обозначается через $\mathbb{N} + A \times \mathbb{Z}$. Ясно, что при любом непустом A получается модель, не изоморфная натуральному ряду. Тем самым мы можем явно указать интерпретацию элементарно эквивалентную, но не изоморфную натуральному ряду в нашей сигнатуре.

Можно показать, что любая модель изоморфна модели вида $\mathbb{N} + A \times \mathbb{Z}$ (для некоторого A). Пусть M произвольная модель T. Скажем, что два элемента x, y из её носителя эквивалентны, если $S(S(\dots S(x)\dots)) = y$ или наоборот $S(S(\dots S(y)\dots)) = x$. Аксиомы гарантируют нам, что это отношение транзитивно (рефлексивность и симметричность очевидны). Классы эквивалентных элементов будем называть галактиками. Галактика, содержащая 0, очевидно, изоморфна натуральному ряду, а остальные галактики изоморфны множеству целых чисел. Обозначим через A множество галактик. Ясно, что M изоморфна интерпретации $\mathbb{N} + A \times \mathbb{Z}$.

2. Сигнатура $\{0, S, \leqslant, =\}$

В качестве аксиом возьмём аксиомы, утверждающие, что $\leqslant$ есть отношение нестрогого линейного порядка, то есть $\forall x\,(x \leqslant x)$ и $\forall x\,\forall y\,(x \leqslant y \wedge y \leqslant x \to x = y)$, $\forall x\,\forall y\,\forall z\,(x \leqslant y \wedge y \leqslant z \to x \leqslant z)$, $\forall x\,\forall y\,(x \leqslant y \vee y \leqslant x)$. Добавим к ним аксиому, утверждающую, что 0 есть

наименьший элемент: $\forall x\,(0 \leqslant x)$ и аксиому, говорящую, что $S(x)$ есть непосредственно следующий за x элемент: $\forall x\,(x < S(x) \wedge \forall y\,(x < y \to S(x) \leqslant y))$ (в этой формуле и далее $x < y$ означает $(x \leqslant y \wedge x \neq y)$). Больше никаких аксиом не нужно: построенная система аксиом полна. Мы опускаем доказательство этого факта, отсылая читателя к книге [1, стр. 217], где доказана полнота аналогичной системы аксиом для целых чисел.

Модели полученной теории устроены так. Для произвольного линейно упорядоченного множества A рассмотрим следующую модель T. Её носитель — объединение множеств $\mathbb{N}$ и $A \times \mathbb{Z}$. Символ S интерпретируется так: на $\mathbb{N}$ это обычное добавление 1, а на элементах $A \times \mathbb{Z}$ — добавление 1 ко второму компоненту пары. Символ $\leqslant$ интерпретируется так: любой элемент $\mathbb{N}$ меньше любого элемента из $A \times \mathbb{Z}$. Элементы из $\mathbb{N}$ сравниваются обычным образом, а на элементах $A \times \mathbb{Z}$ порядок лексикографический: пара $\langle a, n\rangle$ меньше или равна пары $\langle b, m\rangle$, если $a < b$ или $a = b$ и $m \leqslant n$. Легко проверить, что все аксиомы выполнены. Эта модель также обозначается $\mathbb{N} + A \times \mathbb{Z}$. Ясно, что при любом непустом A получается модель, не изоморфная натуральному ряду. Тем самым мы можем явно указать интерпретацию элементарно эквивалентную, но не изоморфную натуральному ряду в нашей сигнатуре.

Точно так же, как и в предыдущем случае, можно доказать, что любая модель нашей теории изоморфна модели вида $\mathbb{N} + A \times \mathbb{Z}$ (для некоторого линейно упорядоченного множества A).

3. Сигнатура $\{0, S, +, \leqslant, =\}$

В качестве аксиом возьмём все аксиомы из предыдущего пункта и добавим следующие аксиомы: ассоциативность, коммутативность сложения, нейтральность 0 относительно сложения ($\forall x\,(x + 0 = x)$), согласованность сложения и порядка: $\forall x\,\forall y\,(x \leqslant y \leftrightarrow \exists z\,(x + z = y))$. (Мы используем запись $A \leftrightarrow B$ как сокращение для формулы $(A \to B) \wedge (B \to A)$.) Кроме того напишем аксиомы,

утверждающие возможность разделить с остатком любое число на любое положительное число (для каждого делителя n будет своя аксиома): $\forall x\,\exists y\,(x = y + y \vee x = y+y+S(0))$, $\forall x\,\exists y\,(x = y+y+y \vee x = y+y+y+S(0) \vee x = y+y+y+S(S(0)))$ и так далее. Получится полная бесконечная система аксиом. Её полнота доказана в [1]. Точнее в [1, стр. 219] строится полная система аксиом для целых чисел в сигнатуре $\{0, S, +, \leqslant, =\}$ и доказывается её полнота.

Модели полученной теории устроены так. Для произвольной упорядоченной коммутативной делимой группы[1] G рассмотрим следующую модель теории T. Её носитель — объединение множеств $\mathbb{N}$ и $G \times \mathbb{Z}$. Символ S интерпретируется так: на $\mathbb{N}$ это обычное добавление 1, а на элементах $G \times \mathbb{Z}$ — добавление 1 ко второму компоненту пары. Символ $\leqslant$ интерпретируется так: любой элемент $\mathbb{N}$ меньше любого элемента из $G \times \mathbb{Z}$. Элементы из $\mathbb{N}$ сравниваются обычным образом, а на элементах $G \times \mathbb{Z}$ порядок лексикографический. Наконец символ $+$ интерпретируется так: $\langle a, n\rangle + \langle b, m\rangle = \langle a + b, m + n\rangle$, $n + \langle a, m\rangle = \langle a, m\rangle + n = \langle a, m + n\rangle$. Можно доказать, что описанная интерпретация является моделью теории T и любая модель T изоморфна модели такого вида (для некоторой упорядоченной коммутативной делимой группы G). Простейшим примером упорядоченной коммутативной делимой группы является группа, состоящая из одного нуля. Ясно, что уже при $G = \{0\}$ получается модель, не изоморфная натуральному ряду.

1.4. Аксиомы формальной арифметики

Мы видели, что невозможно написать разрешимое множество формул языка первого порядка сигнатуры

[1] Группа G называется упорядоченной, если на её элементах введено отношение линейного порядка, удовлетворяющее аксиоме $x \leqslant y \to x + z \leqslant y + z$ для всех $x, y, z \in G$, и делимой, если для любого целого положительного n для всех $x \in G$ найдётся $y \in G$, для которого $x = y + y + \cdots + y$ (n раз).

$\{0, S, +, \cdot, =, \leqslant\}$ такое, что из них выводятся все истинные (в стандартной интерпретации) формулы и только они. Тем не менее мы рассмотрим некоторую разрешимую систему аксиом для натуральных чисел, называемую *арифметикой Пеано* (PA). Мы сократим сигнатуру, удалив отношение порядка. При этом мы ничего не потеряем, поскольку оно выразимо формулой $\exists z\,(x + z = y)$. Будем далее называть *арифметическими формулами* формулы языка первого порядка полученной сигнатуры. В качестве аксиом возьмём аксиомы равенства, к ним добавим аксиомы Пеано 3 и 4 и принцип индукции для арифметических множеств. Кроме того в качестве аксиом возьмём индуктивные определения сложения и умножения. Получится следующее множество аксиом. Записывая аксиомы, мы сокращаем $S(x)$ как Sx, а также опускаем все кванторы всеобщности, написанные в начале формулы, так что первую аксиому следует читать, как $\forall x\,\neg(S(x) = 0)$.

1) $Sx \neq 0$,
2) $Sx = Sy \to x = y$,
3) $x + 0 = x$,
4) $x + Sy = S(x + y)$,
5) $x \cdot 0 = 0$,
6) $x \cdot Sy = x \cdot y + x$,
7) $A(0) \wedge \forall x\,(A(x) \to A(Sx)) \to \forall x\,A(x)$, где $A(x)$ — произвольная арифметическая формула.

Все аксиомы, кроме последней, являются конкретными формулами, в то время, как в последней строчке написана *схема аксиом* (для каждой формулы $A(x)$ получается своя аксиома). Эта схема называется также *принципом индукции*. Она слабее, чем пятая аксиома Пеано, поскольку в ней утверждается лишь, что любое *арифметическое*

множество, содержащее 0 и вместе с каждым числом x содержащее $S(x)$, содержит все натуральные числа.

Указанная система аксиом называется формальной арифметикой и обычно обозначается через PA, что является аббревиатурой Peano Arithmetic. Мы говорим, что формула φ следует из PA, $\mathrm{PA} \models \varphi$, если φ истинна в любой нормальной модели PA при всех значениях своих параметров. По теореме Гёделя о полноте, $\mathrm{PA} \models \varphi$ тогда и только тогда, когда формула φ выводима в исчислении предикатов из аксиом PA и аксиом равенства:

- $x = x$,
- $x = y \to y = x$,
- $x = y \wedge y = z \to x = z$,
- $x = y \to S(x) = S(y)$,
- $x = y \wedge u = v \to x + u = y + v$,
- $x = y \wedge u = v \to x \cdot u = y \cdot v$.

Выводимость φ в исчислении предикатов из аксиом PA и аксиом равенства обозначается как $\mathrm{PA} \vdash \varphi$.

Схема аксиом 7 используется для выводов формул вида $\forall x\, A(x)$ так же, как в неформальных рассуждениях. Сначала мы выводим формулу $A(0)$ (база индукции). Затем выводим формулу $\forall x\,(A(x) \to A(Sx))$ (индуктивный переход). После этого, применяя аксиому 7, получаем $\forall x\, A(x)$.

Нетрудно проверить, что все аксиомы PA истинны в стандартной интерпретации. Как следствие мы получаем непротиворечивость теории PA. С другой стороны, легко видеть, что множество аксиом PA разрешимо. По первой теореме Геделя о неполноте, существует истинная формула, не доказуемая в PA. Итак, имеет место следующая

Теорема 6. Все доказуемые в PA предложения истинны в стандартной интерпретации; обратное неверно.

Разобравшись в доказательстве теоремы Гёделя о неполноте, можно найти конкретную истинную в стандартной интерпретации, но недоказуемую формулу φ. (Позже, на стр. 53, мы укажем такую формулу.) Значит математические методы, использованные нами при доказательстве истинности формулы φ, выходят за рамки PA. Настоящая глава посвящена как раз прояснению того, какие рассуждения формализуются в PA, а какие нет.

Мы начнем с выводов в PA простейших суждений, выражаемых бескванторными формулами. Поскольку формальные выводы в исчислении предикатов довольно громоздки, мы не будем их приводить целиком. Вместо этого мы будем доказывать выводимость в PA нужных формул, явно указывая использование аксиом PA и неявно используя аксиомы и правила вывода исчисления предикатов. Приведённые ниже рассуждения можно также понимать и как неформальные доказательства того, что данная формула истинна в любой модели PA.

1.5. Выводы в PA истинных суждений, записываемых формулами без кванторов

Как, например, вывести в PA утверждение “два плюс два равно четырём”: $\overline{2} + \overline{2} = \overline{4}$, или в развёрнутом виде: $S(S(0)) + S(S(0)) = S(S(S(S(0))))$? (Напомним, что $\overline{k}$ обозначает терм $S(S(\ldots S(0)\ldots))$, где S повторяется k раз.) Для этого достаточно применить аксиому $x + 0 = x$ и аксиому $x + Sy = S(x + y)$ для $y = 0$ и $y = S(0)$. Получим формулу $x + S(S(0)) = S(S(x))$. Подставив $x = S(S(0))$, мы докажем искомую формулу. Совершенно аналогично можно доказать в PA формулу $\overline{m} + \overline{n} = \overline{m + n}$ для любых конкретных натуральных чисел m, n.

Как доказать в PA, что дважды два равно четырём: $\overline{2} \cdot \overline{2} = \overline{4}$, или в развёрнутом виде: $S(S(0)) \cdot S(S(0)) = S(S(S(S(0))))$? Для этого достаточно применить аксиому $x \cdot 0 = 0$ и дважды аксиому $x \cdot S(y) = (x \cdot y) + x$ для $y = S(0), S(S(0))$. Мы получим формулы $x \cdot S(0) = (x \cdot 0) + x$,

$x \cdot S(S(0)) = (x \cdot S(0)) + x$, из которых следует, что $x \cdot S(S(0)) = ((0+x)+x)$. Подставив $x = \overline{2}$, мы получим $\overline{2}\cdot\overline{2} = ((0 + \overline{2}) + \overline{2})$. Поскольку мы уже научились доказывать, что $0+\overline{2} = \overline{2}$ и $\overline{2}+\overline{2} = \overline{4}$, мы можем заключить, что $\overline{2}\cdot\overline{2} = \overline{4}$. Аналогично можно доказать в PA формулу $\overline{m} \cdot \overline{n} = \overline{m \cdot n}$ для любых конкретных натуральных чисел m, n.

Докажем теперь, что для любых $m \neq n$ в PA доказуема формула $\neg(\overline{m} = \overline{n})$. Пусть, например, $m = 2, n = 4$ (для остальных m, n доказательство аналогично). Рассуждая от противного, допустим, что $S(S(0)) = S(S(S(S(0))))$. По аксиоме 2 отсюда следует $S(0) = S(S(S(0)))$. Ещё раз применив эту аксиому, получим $0 = S(S(0))$, что противоречит аксиоме 1.

Из доказанного следует, что любая истинная замкнутая формула без кванторов выводима в PA (без применения принципа индукции).

3. Докажите это.

1.6. Выводы в PA основных свойств натуральных чисел

Заметим, что число аксиом не включена коммутативность и ассоциативность сложения. Начнём с вывода этих законов.

Итак, следующие формулы доказуемы в PA:

1) $0 + x = x$.
   Воспользуемся принципом индукции для формулы $A(x)$ равной $0 + x = x$. База индукции: формула $0+0 = 0$ выводится в исчислении предикатов из аксиомы 3. Индуктивный переход: формула $\forall x\,(0+x = x \to 0+Sx = Sx)$ выводится с помощью аксиомы 4, поскольку из $0 + x = x$ следует $0 + Sx = S(0 + x) = Sx$.

2) $Sx + y = S(x + y)$.
   Воспользуемся принципом индукции для формулы $A(y)$, равной $Sx + y = S(x + y)$. База индукции: из аксиомы 3 следует $Sx+0 = Sx = S(x+0)$. Индуктивный переход: чтобы вывести формулу $\forall y\,(Sx + y = S(x + y) \to Sx + Sy = S(x + Sy))$, используем аксиому 4: из $Sx + y = S(x + y)$ следует $Sx + Sy = S(Sx + y) = S(S(x + y)) = S(x + Sy)$.

3) $x + y = y + x$.
   Докажем эту формулу индукцией по y. База индукции: в силу пункта 1) и аксиомы 3, $x+0 = x = 0+x$. Индуктивный переход: пусть $x + y = y + x$, тогда $x + Sy = S(x + y) = Sy + x$ (последнее равенство верно в силу предыдущего пункта).

4) $(x + y) + z = x + (y + z)$. Докажем эту формулу индукцией по z. При $z = 0$ имеем $(x + y) + 0 = x+y = x+(y+0)$. Индуктивный переход: допустим $(x+y)+z = x+(y+z)$. Тогда $(x+y)+Sz = S((x+y)+z) = S(x+(y+z)) = x+S(y+z) = x+(y+Sz)$.

Аналогично предыдущему доказывается выводимость в PA следующих формул, выражающих элементарные свойства сложения и умножения натуральных чисел:

1) $0 \cdot x = 0$,
2) $Sx \cdot y = x \cdot y + y$,
3) $x \cdot y = y \cdot x$,
4) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
5) $(x + y) \cdot z = x \cdot z + y \cdot z$,
6) $x \cdot \overline{1} = x$,
7) $x + z = y + z \to x = y$,
8) $x \neq 0 \to \exists y\, x = Sy$,
9) $x + y = 0 \to x = 0 \wedge y = 0$,
10) $x \cdot y = 0 \to x = 0 \vee y = 0$,

11) $x \cdot z = y \cdot z \wedge z \neq 0 \to x = y$.

Докажем последнюю формулу. Фиксируем произвольное $z \neq 0$ и докажем индукцией по x, что $x \cdot z = y \cdot z \to x = y$ для всех y. При $x = 0$ утверждается, что $0 = y \cdot z \to 0 = y$, что является следствием предыдущего пункта. Докажем теперь, что $Sx \cdot z = y \cdot z \to Sx = y$, предположив, что для всех u выполнено $x \cdot z = u \cdot z \to x = u$. Пусть $Sx \cdot z = y \cdot z$, то есть $x \cdot z + z = y \cdot z$. Если $y = 0$, то $x \cdot z + z = 0$, и по пункту 9 получаем $z = 0$. Поэтому $y \neq 0$, следовательно, $y = Su$ для некоторого u. Тогда $x \cdot z + z = u \cdot z + z$ и по пункту 7 получаем $x \cdot z = u \cdot z$. По индуктивному предположению $x = u$, следовательно, $Sx = Su = y$.

Напомним, что запись $x \leqslant y$ обозначает формулу $\exists z\, x + z = y$. Следующие свойства формулы $x \leqslant y$, выводимы в PA (доказательство предлагается в качестве упражнения). Они означают, что формула $x \leqslant y$ задает линейный порядок с наименьшим элементом 0, при котором $S(x)$ является непосредственно следующим элементом за x, а также другие свойства этого порядка.

1) $x \leqslant x$,

2) $x \leqslant y \wedge y \leqslant x \to x = y$,

3) $x \leqslant y \wedge y \leqslant z \to x \leqslant z$,

4) $x \leqslant y \vee y \leqslant x$,

5) $0 \leqslant x$,

6) $x < Sx$,

7) $x < y \to Sx \leqslant y$,

8) $x \leqslant y \to x + z \leqslant y + z$,

9) $x \leqslant y \wedge z \neq 0 \to x \cdot z \leqslant y \cdot z$.

Будем в дальнейшем понимать $(\forall i < l)\, A$, где A — некоторая формула, как сокращение для формулы $\forall i\, (i < l \to A)$.

В формальной арифметике можно говорить и о целых числах. Именно, целое число x представляется любой парой натуральных чисел a, b, для которой $x = a - b$. Тогда формула $a + c + f = b + d + e$ выражает то, что сумма чисел, представленных парами a, b и c, d, равна числу, представленному парой e, f. Аналогично можно написать формулу для представления умножения целых чисел и доказать в PA формулы, утверждающие, что полученная система есть коммутативное кольцо с единицей. Точно так же можно определить рациональные числа, арифметические операции с рациональными числами и доказать в PA их основные свойства.

1.7. Финитные доказательства и тезис арифметичности

1. Полная математическая индукция и принцип наименьшего числа

Докажем, что в формальной арифметике можно использовать *полную математическую индукцию*. Чтобы доказать некоторое утверждение $\forall x\, A(x)$ методом полной математической индукции, мы сначала доказываем, что если для всех y, меньших x, выполнено $A(y)$, то выполнено и $A(x)$ (заметим, что $A(0)$ приходится доказывать без всяких предположений, поскольку y, меньших 0, нет). Затем мы заключаем, что $A(x)$ выполнено для всех x. Для обоснования этого принципа нам надо доказать, что для любой формулы $A(x)$ формула

- $\forall x\, ((\forall y < x) A(y) \to A(x)) \to \forall x\, A(x)$

является теоремой PA. Пусть $\forall x\, ((\forall y < x) A(y) \to A(x))$. Применим (обычную) индукцию к формуле $B(x) = (\forall y < x) A(y)$. База индукции $(\forall y < 0) A(y)$ очевидна, поскольку нет натуральных чисел, меньших 0. Индуктив-

ный переход: пусть $B(x)$, то есть $(\forall y < x)A(y)$. Тогда по условию выполнено $A(x)$, следовательно $(\forall y \leqslant x)A(y)$, то есть $B(Sx)$. Поэтому для всех x выполнено $B(x)$, из чего мгновенно следует, что и $A(x)$ выполнено при всех x.

Переходом к контрапозиции из принципа полной математической индукции мы получаем *принцип наименьшего числа* — если существует число с некоторым свойством, то и существует и наименьшее число с этим свойством:

- $\exists x\, A(x) \to \exists x\, (A(x) \wedge (\forall y < x)\neg A(y))$.

2. Принцип свёртывания

В формулировках многих арифметических теорем используется понятие конечной последовательности. Такова, например, теорема о разложении натуральных чисел на простые множители. Как и утверждения о целых числах, эти теоремы не формулируются непосредственно как утверждения первого порядка арифметической сигнатуры. Для их формулировки на арифметическом языке мы будем, как и раньше, использовать β-функцию Геделя $\beta(a,b,i)$. Мы доказали (теорема 1), что для любой последовательности натуральных чисел $k_0, k_1, \ldots, k_{l-1}$ существуют такие a, b, что $\beta(a,b,i) = k_i$ для всех $i < l$. Поэтому будем в дальнейшем при записи на арифметическом языке утверждений, содержащих понятие (конечной) последовательности, под последовательностью понимать тройку натуральных чисел a, b, l. При этом l — это длина последовательности, а $\beta(a,b,i)$ ее i-ый член. Вот как записать, скажем, теорему о возможности разложения натуральных чисел на простые множители. Сначала надо выразить утверждение о том, что произведение членов последовательности, задаваемой тройкой a, b, l, равно x. Для этого напишем, что существует последовательность длины $l+1$, нулевой член которой равен 1, последний равен x, и $i+1$-ый член который получается из её i-ого члена умножением на $\beta(a,b,i)$ (для всех $i = 0, \ldots, l-1$). Теперь утверждение о разложении чисел

на простые множители можно записать, например, так: для всех $x \neq 0$ существует l и последовательность длины l, состоящая из простых чисел, произведение которых равно x.

При таком способе представления конечных последовательностях все математические рассуждения, использующие натуральные числа и конечные последовательности натуральных чисел, могут быть естественным образом переведены в теории PA. Чтобы обосновать этот тезис, докажем что в PA выводимы все свойства последовательностей, используемые в обычных рассуждениях. Например, что к любой последовательности можно дописать справа любое число: $\forall a\, \forall b\, \forall l\, \forall x\, \exists c\, \exists d\, \Big(\forall i\, (i < l \to \beta(a,b,i) = \beta(c,d,i)) \wedge \beta(c,d,l) = x\Big)$. Нужные свойства последовательностей выводятся в PA из следующих двух свойств.

- $\forall a\, \forall b\, \forall i\, \exists! k\ \beta(a,b,i) = k$ (здесь и далее выражение $\exists! k A(k)$ означает, что существует единственное k, для которого $A(k)$, его можно можно записать, например, формулой $\exists k(A(k) \wedge \forall m\, (A(m) \to A(k)))$.
- *Принцип свёртывания.* Пусть $A(i,k)$ произвольная формула арифметической сигнатуры, не содержащая свободно переменных a, b (но, возможно, содержащая, кроме i, k, другие свободные переменные). Пусть l произвольное натуральное число. Если для всех $i < l$ существует k, для которого $A(i,k)$, то существуют a, b, для которых $A(i, \beta(a,b,i))$ для всех $i < l$.

Чтобы доказать первое свойство, выведем в PA более общий факт — существование и единственность остатка от деления на положительное число:

$$\forall a\, \forall b\, (b > 0 \to \exists! r\ \exists q\, (a = qb + r \wedge r < b)).$$

Пусть $b > 0$. Докажем сначала существование r. При всех достаточно больших q (скажем при $q > a$) выполнено

$qb > a$. Пусть q наибольшее такое число, что $qb \leqslant a$. Тогда $(q+1)b > a$, следовательно, $a - qb < b$. Положим $r = a - qb$. Теперь докажем единственность r. Пусть $a = qb + r = q'b + r'$, где $r, r' < b$. Пусть для определённости $r > r'$. Тогда $b > r - r' = (q - q')b \geqslant b$. Полученное противоречие доказывает невозможность $r > r'$. Аналогично доказывается невозможность $r < r'$.

Доказать в PA принцип свёртывания значительно сложнее. Его истинность вытекает из теоремы 1. Доказательство этой теоремы основывается на китайской теореме об остатках, в обычном доказательстве которой нужен принцип свёртывания. Чтобы разорвать получающийся порочный круг мы непосредственно (т.е. без использования принципа свёртывания) докажем в PA теорему 1.

Доказательство принципа свёртывания

Мы уже отмечали, что на арифметическом языке можно естественным образом выразить следующие понятия:

- $z = \text{НОД}(x, y)$. Напомним, что число z является наибольшим общим делителем чисел x и y, если x делит как y, так и z, и больше всех остальных чисел с этим свойством; $\text{НОД}(x, y)$ определён, если хотя бы одно из чисел x и y отлично от нуля;
- x, y взаимно просты — $\text{НОД}(x, y) = 1$;
- $z = \text{НОК}(x, y)$. Напомним, что число z является наименьшим общим кратным x и y, если $z \neq 0$, z делится на x и на y и z меньше всех остальных чисел с этим свойством; наименьшее общее кратное определено, если хотя бы одно из чисел x и y отлично от нуля.

Нетрудно доказать в PA, что если хотя бы одно из чисел x, y отлично от нуля, то существует единственное

такое z, что $z = \text{НОД}(x, y)$ и единственное такое z, что $z = \text{НОК}(x, y)$.

Итак, начнем доказательство принципа свёртывания. Пусть для всех $i < l$ найдется такое k, что выполнено $A(i, k)$. Обозначим наименьшее такое k через k_i. Сначала докажем в PA такое утверждение.

Лемма 1. Можно найти натуральное число b такое, что $k_i < b$ при всех $i < l$ и числа $b(i+1)+1$, $b(j+1)+1$ взаимно просты при всех $i < j < l$.

Вспомним доказательство этого факта, приведённое на странице 8: любой общий простой делитель чисел $bi + 1, bj + 1$ будет делителем числа $b(i - j)$; взяв b кратным $l!$, мы гарантируем, что он будет делителем числа b, но все числа $b(i+1)+1$ взаимно просты с b. Таким образом, можно взять $b = l!(\max(k_0, \ldots, k_{l-1}) + 1)$.

При формализации этого доказательства в PA возникает следующая проблема. Для арифметической формулы, выражающей равенство $n = k!$ с помощью β-функции Геделя, мы не можем без принципа свёртывания доказать в PA, что $\forall k \exists n\, (n = k!)$, т.е. что для всех k найдутся a, b, n такие, что $\beta(a, b, 0) = 1$, $\beta(a, b, k) = n$ и $\beta(a, b, i+1) = \beta(a, b, i) \cdot (i+1)$ при всех $i = 0, 1, \ldots, k-1$. Выход прост: нам достаточно только доказать существование числа, кратного всем положительные числам, меньшим l. Это легко доказать индукцией по l. Аналогично, вместо $\max(k_0, \ldots, k_{l-1}) + 1$ мы можем использовать любое число, больше всех k_i при $i < l$. Для доказательства существования такого числа мы можем индукцией по j доказать формулу $\exists m\, (\forall i < j)(k_i < m)$. (Кроме того, мы можем непосредственно, т. е. без помощи β-функции, определить, что значит $m = \max(k_0, \ldots, k_{l-1})$, и доказать существование такого m.)

Кроме того, нам нужно доказать в PA следующие арифметические факты.

- *Любое число, большее 1, имеет простой делитель (лемма Евклида).* Обычное доказательство этого

факта легко переводится в вывод в PA. Напомним его. Пусть $x > 1$. Положим p равным наименьшему неединичному делителю x. Докажем, что p простое. Допустим $p = ab$, где $a, b \neq p$. Тогда a, b отличны от 1, следовательно больше 1. Ясно, что $b < p$, так как иначе $p = ab \geqslant ap > 1 \cdot p = p$. Таким образом, b является неединичным делителем p (следовательно и делителем x), меньшим p. Полученное противоречие доказывает простоту p.

- *Если простое число делит произведение двух чисел, то оно делит одно из этих чисел.* Это мгновенно следует из следующего утверждения.

- *Если x, y взаимно просты и x делит yz, то x делит z.* Доказательство этого факта основано на теореме о том, что для любых взаимно простых натуральных x, y найдутся целые a, b, для которых $ax + by = 1$. Обычное доказательство этого факта использует алгоритм Евклида, не формализуемый непосредственно PA. К счастью, можно обойтись без алгоритма Евклида, использовав индукцию по $\max(x, y)$. Действительно, если $\max(x, y) = 1$, то утверждение очевидно. Индуктивный переход: пусть $\max(x, y) > 1$. Ясно, что $x \neq y$, пусть, скажем $x > y$. Положим $z = x - y$. Легко доказать, что $\text{НОД}(z, y) = \text{НОД}(x, y) = 1$. По предположению индукции $az + by = 1$ для некоторых целых a, b. Следовательно, $ax + (b - a)y = 1$. (В доказательстве мы использовали принцип полной математической индукции, который обосновали ранее. Кроме того, мы использовали целые числа. Как отмечалось ранее, их можно представлять парами натуральных чисел и пользоваться основными свойствами.)

  Итак, пусть x делит yz. Умножив равенство $ax + by = 1$ на z получим $axz + byz = z$. Поскольку x делит оба слагаемых левой части этого равенства,

x делит z.

Далее в доказательстве на стр. 8 мы использовали китайскую теорему об остатках. Нам достаточно доказать в PA эту теорему в следующей форме.

Лемма 2. Пусть $d_i = b(i + 1) + 1$. Если числа d_0, d_1, $\ldots$, d_{l-1} попарно взаимно просты, то существует целое a, сравнимое с k_i по модулю d_i для всех $i < l$.

На самом деле нам совершенно не важно, какой именно арифметической формулой задаются числа d_i; важно лишь, чтобы была такая формула, так как иначе условие леммы невозможно было бы записать на арифметическом языке. (На всякий случай напомним, что k_i также задаются с помощью некоторой формулы.)

Мы уже доказывали это утверждение на стр. 8, не заботясь о том, чтобы доказательство можно было провести в PA. Сейчас мы немного изменим доказательство так, чтобы оно непосредственно формализовывалось в PA. Мы начинали с доказательства такого утверждения: если x, y взаимно просты, а r, s произвольные натуральные числа, то найдётся целое a, сравнимое с r по модулю x и с s по модулю y. Это доказательство непосредственно формализуется в PA. Далее мы доказывали индукцией по j, что существует натуральное число a, сравнимое с k_i по модулю d_i для всех $i < l$. База индукции (для $j = 1$) доказывается в PA непосредственно. Индуктивный переход: пусть a сравнимо с k_i по модулю d_i для всех $i < j$, надо доказать существование a', сравнимого с k_i по модулю d_i для всех $i \leqslant j$. Для этого мы определяли вспомогательное число $c = d_0 \cdot d_1 \cdots d_{j-1}$ и с помощью уже доказанного утверждения находили a', сравнимое с a по модулю c и с k_j по модулю d_j. Поскольку в PA мы пока не можем доказать существования произведения чисел $d_0, d_1, \ldots, d_{j-1}$, будем определять c как наименьшее общее кратное $d_0, d_1, \ldots, d_{j-1}$, а не как их произведение (поскольку числа взаимно просты, произведение равно наименьшему общему кратному, хотя это и не важно).

Наименьшее общее кратное этих чисел выражается непосредственно (без β-функции), как наименьшее ненулевое число, которое делится на все эти числа. Существование какого-нибудь общего кратного $d_0, d_1, \dots, d_{j-1}$ легко доказывается индукцией по j. Тем самым мы можем доказать и существование $\mathrm{НОК}(d_0, d_1, \dots, d_{j-1})$.

Далее нам нужно доказать в PA, что c взаимно просто с d_j. Это следует из такого общего факта, выводимого в PA:

- Если число x взаимно просто с попарно взаимно простыми числами $d_0, d_1, \dots, d_{j-1}$, то x взаимно просто с их наименьшим общим кратным.
  В PA этот факт доказывается индукцией по j. При $j = 1$ утверждение очевидно. Докажем в PA индуктивный переход (от j к $j+1$). Сначала покажем, что наименьшее общее кратное $d_0, d_1, \dots, d_j$ делит любое другое общее кратное $d_0, d_1, \dots, d_j$. Действительно, пусть z есть общее кратное $d_0, d_1, \dots, d_j$. Пусть z' есть остаток от деления z на
  $$c = \mathrm{НОК}(d_0, d_1, \dots, d_j).$$
  Тогда $z' < c$ и z' делится на $d_0, d_1, \dots, d_j$. Следовательно, $z' = 0$.
  Итак, допустим, что x и c не взаимно просты. Тогда существует простое число p, делящее x и c. Легко проверить, что число $\mathrm{НОК}(\mathrm{НОК}(d_0, d_1, \dots, d_{j-1}), d_j)$ делится на d_0, d_1, …, d_j, следовательно, кратно c. Поэтому это число делится на p. Но если наименьшее общее кратное двух чисел r, s делится на простое число p, то хотя бы одно из них делится на p. (Это доказывается почти так же, как аналогичный факт для произведения чисел: предположим, что r не делится на p, тогда для некоторых целых u, v выполнено $up + vr = 1$. Следовательно, $ups + vrs = s$. Число rs кратно $\mathrm{НОК}(r, s)$, поэтому rs делится на p, следовательно и s делится на p.) Следовательно, $\mathrm{НОК}(d_0, d_1, \dots, d_{j-1})$ делится на p или d_j делится на p. По индуктивному предположению первое невозможно. Второе невозможно в силу взаимной простоты x и d_j.

Итак, пусть a удовлетворяет лемме 2. Положим $a' = a + |a|c$. Число a' натуральное и даёт остаток k_i при делении на d_i при всех $i < j$. Действительно, $a' - k_i$ делится на d_i, то есть $a' = qd_i + k_i$ для некоторого целого q. Поскольку $k_i < d_i$, число q натуральное, следовательно k_i есть остаток при делении a' на d_i. Эти рассуждения без труда формализуются в PA.

3. Следствия принципа свёртывания

Приведём несколько часто применяемых следствий принципа свёртывания.

1) В PA можно доказать, что для любой последовательности α и любого числа c существует последовательность β, получающаяся приписыванием x в конец α. Действительно, пусть α задается тройкой a, b, l. Применяем принцип свёртывания к формуле $A(i, k)$, равной $i < l \wedge k = \beta(a, b, i) \ \vee \ i = l \wedge k = x$.

   Забавно, что принцип свёртывания легко выводится из этого своего следствия. Действительно, используя это следствие, нетрудно доказать индукцией по j, что найдется последовательность, задающая j первых членов последовательности, определяемой данной формулой $A(i, k)$.

2) В PA можно доказать, что для любых последовательностей σ, τ существует последовательность π, равная конкатенации последовательностей σ, τ. Действительно, пусть σ, τ задаются соответственно тройками a, b, l и c, d, n. Применяем принцип свёртывания к к формуле $A(i, k)$, равной $((i < l) \wedge (k = \tau(a, b, i))) \vee ((l \leqslant i < l + n) \wedge (k = \tau(c, d, i - l)))$.

3) Рекурсивные определения. Пусть $A(i,x,y)$ — произвольная формула. Будем говорить, что последовательность α длины l согласована с рекурсивным правилом $A(i,x,y)$, если для всех $i<l-1$ выполнено $A(i,\alpha(i),\alpha(i+1))$. Тогда в PA можно доказать такое утверждение: для всех l,c, если для всех $i<l-1$ для всех x существует y, для которого $A(x,y)$, то существует последовательность длины l, начальный член которой равен c, согласованная с рекурсивным правилом $A(i,x,y)$.

   Это доказывается индукцией по l. При $l=1$ утверждение очевидно. Индуктивный переход (от l к $l+1$): пусть $(\forall i<l)\,\forall x\,\exists y\ A(i,x,y)$. По индуктивному предположению существует последовательность α длины l с нулевым членом c, согласованная с рекурсивным правилом $A(i,x,y)$. Возьмём любое y, для которого $A(i,\alpha(l-1),y)$. По пункту 1) существует последовательность, получающаяся приписыванием y в конец последовательности, задаваемой тройкой α. Эта последовательность и есть искомая.

4. Понятие финитного доказательства

Мы будем называть *финитными* доказательства на естественном языке, не использующие бесконечных объектов. Например, любой вывод в PA естественным образом преобразуется в финитное доказательство своей последней формулы. Понятие финитного доказательства не является формальным. Для пояснения различия между финитным и нефинитным доказательством, приведем два доказательства, финитное и нефинитное, неограниченности множества простых чисел (для каждого n существует простое число, большее n).

Финитное доказательство.

Сначала доказываем по индукции (как это было сделано выше), что любое число, большее 1, имеет простой

делитель. Пусть теперь n произвольное натуральное число. Число $n!+1$ больше 1, пусть p — любой его простой делитель. Предположим, что $p\leqslant n$. Тогда p совпадает с одним из чисел $1,2,3,\ldots,n$, а следовательно p делит их произведение $n!$. Но тогда p делит $n!+1-n!=1$, что невозможно. Полученное противоречие показывает, что $p>n$.

Нефинитное доказательство.

Допустим, все простые числа не превосходят некоторого натурального n. Пусть тогда $p_1,\ldots,p_k$ — список всех простых чисел. Любое положительное число единственным образом представимо в виде $p_1^{n_1}\cdots p_k^{n_k}$ (используем основную теорему арифметики), поэтому

$$\frac{1}{(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k})}=$$
$$=\Big(1+\frac{1}{p_1}+\frac{1}{p_1^2}+\ldots\Big)\cdots\Big(1+\frac{1}{p_k}+\frac{1}{p_k^2}+\ldots\Big)=$$
$$=1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\ldots$$

Поскольку гармонический ряд расходится, мы получаем противоречие.

Это доказательство не финитно, поскольку в нем используются ряды. Правда, оно легко может быть переделано в финитное, но это типичная картина: большинство нефинитных доказательств ценой некоторого усложнения переделываются в финитные.

5. Тезис арифметичности

Тезис арифметичности гласит: *любая арифметическая формула, имеющая финитное доказательство, выводима в PA*.

В самом деле, конечные объекты — это натуральные числа, конечные последовательности натуральных чисел, конечные множества натуральных чисел, конечные

функции с натуральными аргументами и значениями, конечные последовательности конечных множеств натуральных чисел и т. д. Все эти объекты представимы натуральными числами: способ представления конечных последовательностей натуральных чисел уже излагался, конечные множества натуральных чисел могут быть представлены как множества значений конечных последовательностей натуральных чисел и т. д. При таком представлении все свойства конечных объектов, используемые в математических рассуждениях, следуют из принципа свёртывания. Потому математические рассуждения, использующие только конечные объекты, естественным образом переводимы в формальные выводы в PA.

Во многом тезис арифметичности аналогичен тезису Черча. Он также имеет неформальный характер, поэтому недоказуем и неопровержим. Схема его применения такова: если нам нужно установить выводимость в PA конкретной арифметической формулы (а сам вывод не нужен), то достаточно привести финитное доказательство формулы. Это сильно упрощает многие рассуждения о выводимых в PA формулах (так же, как и тезис Черча упрощает рассуждения о вычислимых на машинах Тьюринга функциях).

Наша вера в тезис арифметичности основана на двух эмпирических фактах: 1) все известные арифметические формулы, имеющие финитное доказательство, выводимы в PA, 2) все известные исчисления, уточняющие понятие финитных рассуждений, эквивалентны PA (т. е. в них выводимы в точности те же арифметические формулы, что и в PA). В одном из следующих параграфов мы приведем два таких исчисления.

6. Пример формализации в PA финитного доказательства: доказательство основной теоремы арифметики

Чтобы продемонстрировать, как финитные доказательства формализуются в PA, разберем в качестве

примера доказательство основной теоремы арифметики. Как всегда, мы не будем строить формальный вывод, а лишь изложим доказательство в форме, легко преобразуемой в такой вывод.

Напомним, что основная теорема арифметики гласит, что любое натуральное число, большее единицы, единственным образом раскладывается в произведение простых сомножителей. Итак, надо доказать два утверждения

1) если $x > 1$, то существует последовательность $p_1, p_2, \ldots, p_k$ простых чисел такая, что выполнено $x = p_1 p_2 \cdots p_k$;

2) если $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, где p_1, p_2, …, p_n и q_1, q_2, …, q_m неубывающие последовательности простых чисел, то эти последовательности совпадают.

Докажем 1). Мы доказывали, что у каждого числа, большего 1, есть простой делитель. Определим по рекурсии последовательность α длины x так, что $\alpha(0) = x$ и $\alpha(i+1)$ равно $\alpha(i)/p_i$, где p_i наименьший простой делитель $\alpha(i)$, если $\alpha(i) > 1$, и $\alpha(i+1) = \alpha(i)$ иначе. Легко по индукции доказать, что $1 \leqslant \alpha(i) \leqslant x - i$ для всех $i < x$, следовательно $\alpha(x-1) = 1$. Пусть l наименьшее такое число, что $\alpha(l) = 1$. По принципу свёртывания существует такая последовательность γ длины l, что $\gamma(i) = \alpha(i)/\alpha(i+1)$ для всех $i < l$. Тогда все члены этой последовательности — простые числа. Надо еще доказать, что их произведение равно x, т. е. доказать существование последовательности длины $l+1$, первый член которой равен 1, последний член равен x, и $(i+1)$-ый член равен i-ому члену, умноженному на $\gamma(i)$ (при всех $i = 0, 1, \ldots, l-1$). Ясно, что первые $l+1$ членов последовательности α, взятые в обратном порядке, и составляют искомую последовательность (существование такой последовательности следует опять-таки из принципа свёртывания).

Докажем 2). Здесь нам уже не понадобится принцип

свёртывания. Применим индукцию по n. База индукции: $n = 1$. Нам дано, что $p_1 = q_1 q_2 \cdots q_m$. Значит существует последовательность α длины $m+1$, первый член которой равен 1, последний член равен p_1, и i-ый член равен предыдущему, умноженному на q_i (при всех $i = 1, 2, \ldots, m$). В частности, $\alpha(m) = \alpha(m-1)q_m$. Так как $\alpha(m) = p_1$ и p_1, q_m просты, получаем, что $\alpha(m-1) = 1$ и $q_m = p_1$. Отсюда $m = 1$, так как все члены последовательности α, начиная с $\alpha(1)$, больше единицы.

Индуктивный переход. Пусть $n > 1$, $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, где p_1, p_2, $\ldots$, p_n, q_1, q_2, $\ldots$, q_m простые числа и $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_n$, $q_1 \leqslant q_2 \leqslant \ldots \leqslant q_m$.

Индукцией по длине последовательности, докажем, что если простое число делит произведение членов последовательности, состоящей из простых чисел, то оно совпадает с одним из них. Действительно, если простое p делит $s_1 s_2 \cdots s_k$, то p делит $s_1 s_2 \cdots s_{k-1}$ или делит s_k. Во втором случае $p = s_k$, в первом случае утверждение следует из индуктивного предположения.

Положим $x = p_1 p_2 \cdots p_{n-1}$, $y = q_1 q_2 \cdots q_{m-1}$. Тогда $xp_n = q_1 q_2 \cdots q_m$, следовательно p_n делит произведение чисел $q_1, q_2, \ldots, q_m$, значит $p_n = q_i$ для некоторого $i \leqslant m$. Аналогично $q_m = p_j$ для некоторого $j \leqslant n$. Отсюда следует $p_n = q_i \leqslant q_m = p_j \leqslant p_n$, поэтому $p_n = q_m$. Значит $x = y$. По индуктивному предположению $n - 1 = m - 1$ и $p_1 = q_1$, $\ldots$, $p_{n-1} = q_{n-1}$. Поскольку $p_n = q_m$, это завершает доказательство.

7. Два консервативных расширения PA

Примитивно рекурсивная арифметика.

В PA входят аксиомы, определяющие сложение и умножение. но нет аксиом, определяющих возведение в степень. Почему? Давайте добавим в сигнатуру двуместный функциональный символ x^y и две аксиомы: $x^0 = 1$, $x^{y+1} = x^y \cdot x$, Ясно, что все доказательства в таком расширении PA финитны. Более того, для *каждой* примитивно рекурсивной функции h добавим в сигнатуру

новый функциональный символ и аксиомы, определяющие эту функцию. То есть, если h определяется по рекурсии

$$h(x_1, \ldots, x_k, 0) = f(x_1, \ldots, x_k),$$
$$h(x_1, \ldots, x_k, y+1) = g(x_1, \ldots, x_k, y, h(x_1, \ldots, x_k, y)),$$

то эти две формулы и добавим в качестве аксиом, а если h определяется подстановкой

$$h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n)),$$

то эту формулу и добавим в качестве аксиомы. Кроме того, разрешим в принципе индукции использовать формулы, содержащие добавленные символы.

Полученная теория первого порядка обозначается PrA. Докажем, что она является консервативным расширением PA, т. е. любая арифметическая формула (без добавленных символов), выводимая в PrA, выводима и в PA. Для этого перенумеруем все примитивно рекурсивные функции в таком порядке, что функции, участвующие в определении i-ой функции h_i, имеют меньшие, чем i, номера. Определим последовательность теорий первого порядка T_i: $T_0 =$ PA, а T_i получается из T_{i-1} добавлением аксиом, определяющих h_i. Нам достаточно доказать, что T_i есть консервативное расширение T_{i-1} (для всех i).

Известная теорема о консервативных расширениях (см. напр. [3, стр. 93]) утверждает, что если в теории T выводима формула

$$\forall x_1 \ldots \forall x_n \exists! y \; A(x_1, \ldots, x_n, y),$$

то расширение, полученное добавлением к T функционального символа f и аксиомы

$$\forall x_1 \ldots \forall x_n \, A(x_1, \ldots, x_n, f(x_1, \ldots, x_n)),$$

консервативно. Последняя формула называется определяющей аксиомой для f. Поэтому нам достаточно показать, что T_i можно получить из T_{i-1} таким образом.

Если $h = h_i$ определяется подстановкой

$$h(x_1, \dots, x_n) = f(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n)), \tag{1.1}$$

то это почти очевидно, так как в T_{i-1} выводима формула

$$\forall x_1 \dots \forall x_n \exists! y \ (y = f(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n))).$$

Небольшая проблема в том, что T_i получается из T_{i-1} добавлением не только формулы (1.1), но и аксиом индукции для формул, содержащих символ h. Эта проблема решается просто: в каждой аксиоме индукции $A(0) \wedge \forall x\,(A(x) \to A(Sx)) \to \forall x\,A(x)$, где $A(x)$ содержит символ h, заменим $A(x)$ на эквивалентную формулу $A'(x)$, не содержащую h, пользуясь равенством (1.1). Полученная аксиома индукции относится к аксиомам T_{i-1}.

Пусть теперь T_i получается добавлением аксиом

$$h(x_1, \dots, x_k, 0) = f(x_1, \dots, x_k), \tag{1.2}$$

$$h(x_1, \dots, x_k, y+1) = g(x_1, \dots, x_k, y, h(x_1, \dots, x_k, y)). \tag{1.3}$$

В этом случае мы не можем непосредственно воспользоваться консервативностью расширений с помощью добавления определяемых символов, поскольку (1.2) и (1.3) не определяют явно h. Докажем, что неявное индуктивное определение h с помощью (1.2) и (1.3) можно заменить на явное определение формулой:

$$\begin{aligned} \exists a\, \exists b \Big(&\beta(a,b,0) = f(x_1, \dots, x_k) \ \wedge \\ \wedge, &\beta(a,b,y) = h(x_1, \dots, x_k, y) \ \wedge \ (\forall z < y) \\ &(\beta(a,b,z+1) = g(x_1, \dots, x_k, z, \beta(a,b,z))) \Big). \end{aligned} \tag{1.4}$$

Сначала выведем в T_i формулу (1.4). Очевидно, в T_i выводим принцип свёртывания для формул, содержащих символы $h_1, \dots, h_i$. По принципу свёртывания для всех $x_1, \dots, x_k, y$ существуют a, b такие, что $\beta(a,b,z) = h(x_1, \dots, x_k, z)$ для всех $z \leqslant y$. Из аксиом (1.2) и (1.3) следует, что эти a, b удовлетворяют (1.4).

Обратно, докажем, что (1.2) и (1.3) выводимы в теории, получающейся добавлением к T_{i-1} формулы (1.4). Подставив в (1.4) $y = 0$ мы получим что для некоторых a, b выполнено $\beta(a,b,0) = f(x_1, \dots, x_k) \ \wedge \ \beta(a,b,0) = h(x_1, \dots, x_k, 0)$, из чего следует (1.2). Докажем (1.3). В силу (1.4) существуют a, b, c, d, для которых

$$\begin{aligned} &\beta(a,b,0) = f(x_1, \dots, x_k), \\ &\beta(a,b,y) = h(x_1, \dots, x_k, y), \\ &(\forall z < y)\, \beta(a,b,z+1) = g(x_1, \dots, x_k, z, \beta(a,b,z)), \\ &\beta(c,d,0) = f(x_1, \dots, x_k), \\ &\beta(c,d,y+1) = h(x_1, \dots, x_k, y+1), \\ &(\forall z < y+1)\, \beta(c,d,z+1) = g(x_1, \dots, x_k, z, \beta(c,d,z)). \end{aligned}$$

Индукцией по z легко доказать, что $\beta(a,b,z) = \beta(c,d,z)$ для всех $z \leqslant y$. Следовательно,

$$\begin{gathered} h(x_1, \dots, x_k, y+1) = \beta(c,d,y+1) = \\ = g(x_1, \dots, x_k, y, \beta(c,d,y)) = g(x_1, \dots, x_k, y, \beta(a,b,y)) = \\ = g(x_1, \dots, x_k, h(x_1, \dots, x_k, y)). \end{gathered}$$

Итак, нам достаточно доказать, что расширение, полученное добавлением (1.4) к теории T_{i-1}, консервативно. Для этого достаточно доказать в T_{i-1}, что для всех $x_1, \dots, x_k, y$ существует единственное u, для которого

$$\begin{aligned} \exists a\, \exists b \Big(&\beta(a,b,0) = f(x_1, \dots, x_k) \wedge \\ \wedge\, &(\forall i < y)\, \beta(a,b,z+1) = g(x_1, \dots, x_k, z, \beta(a,b,z)) \wedge \\ \wedge\, &\beta(a,b,y) = u \Big). \end{aligned}$$

Существование следует из принципа свёртывания (см. следствие о рекурсивных определениях). Единственность доказывается так: пусть u_1, u_2 удовлетворяют указанной формуле, и пусть a_1, b_1 и a_2, b_2 — соответствующие a, b. Тогда индукцией по z легко доказать, что $\beta(a_1, b_1, z) = \beta(a_2, b_2, z)$ для всех $z \leqslant y$. Поэтому $u_1 = \beta(a_1, b_1, y) = \beta(a_2, b_2, y) = u_2$.

Расширение PA с помощью добавления конечных множеств.

Кроме конечных последовательностей финитные рассуждения могут использовать конечные множества. Одно сводится к другому, поскольку конечное множество можно отождествить с последовательностью, перечисляющей элементы множества в возрастающем порядке. Обратно, каждая конечная последовательность есть конечное множество пар чисел, а любая пара чисел $\langle a, b\rangle$ может быть отождествлена с множеством $\{\{a\}, \{a, b\}\}$ (нетрудно доказать, что определяющее свойство пары $\langle a, b\rangle = \langle c, d\rangle \to a = c \wedge b = d$ выполнено при таком понимании пары). Таким образом, правдоподобным выглядит отождествление финитных рассуждений с доказательствами в расширении PA, получающимся добавлением символа принадлежности $\in$, константы $\emptyset$ и основных свойств конечных множеств.

Точнее, добавим к PA следующие четыре аксиомы:

1) $\forall z\,(z \in x \leftrightarrow z \in y) \to x = y$,

2) $\forall z\,\neg(z \in \emptyset)$,

3) $\forall x\,\forall y\,\exists z\,\forall w\,(w \in z \leftrightarrow w = x \vee w = y)$,

4) $\forall x\,\forall y\,\exists z\,\forall w\,(w \in z \leftrightarrow w \in x \vee w \in y)$.

Аксиома 1) называется аксиомой объемности и говорит, что два множества совпадают, если они состоят из одинаковых элементов. Аксиома 3) утверждает существование неупорядоченной пары $\{x, y\}$. В частности, положив

$x = y$ получаем существование множества $\{x\}$. Поэтому из аксиомы 3) следует существование (упорядоченной) пары $\langle a, b\rangle =_{\text{def}} \{\{a\}, \{a, b\}\}$. Аксиома 4) говорит, что для любых множеств x, y существует их объединение $x \cup y$.

Кроме этих четырех аксиом, добавим аксиомы индукции с формулами, содержащими новые символы $\in, \emptyset$. Получившаяся теория первого порядка будет обозначаться через Z. Недостатком этой теории является смешение натуральных чисел и множеств: каждое натуральное число понимается еще и как некоторое конечное множество. Чтобы устранить этот недостаток, можно было бы ввести специальные переменные для множеств, однако получившаяся бы таким образом теория была бы эквивалентна Z, поэтому мы этого не делаем.

Подразумеваемая интерпретация теории Z следующая. Носитель — множество натуральных чисел, знаки $S, +, \cdot$ понимаются стандартным образом. Чтобы интерпретировать символ $\in$, перенумеруем произвольным образом конечные множества (так, чтобы каждое множество имело ровно один номер). Тогда $x \in y$ будет означать, что x принадлежит множеству с номером y, а $\emptyset$ интерпретируется как номер пустого множества.

Представляется весьма правдоподобным, что все финитные рассуждения формализуемы в Z. Мы утверждаем, что Z есть консервативное расширение PA. Действительно, рассмотрим следующую нумерацию конечных множеств:

$$\emptyset,\ \{0\},\ \{1\},\ \{1,0\},\ \{2\},\ \{2,0\},\ \{2,1\},\ \{2,1,0\},\ldots$$

Множество с номером x состоит из тех i, для которых i-ый разряд двоичной записи x равен 1 (разряды нумеруются числами 0,1,..., начиная с младших разрядов). Обозначим через M получающуюся таким образом интерпретацию языка теории Z. С помощью β-функции Геделя мы можем написать арифметическую формулу, выражающую то, что x принадлежит множеству с номером y, и таким образом сопоставить каждой формуле A

языка теории Z арифметическую формулу A', истинную тогда и только тогда, когда A истинна в M. При этом для любой аксиомы A теории Z ее перевод A' выводим в PA (что проверяется непосредственно), следовательно выводимы и переводы всех теорем. Это завершает доказательство консервативности.

Можно и по-другому переводить формулы языка теории Z на арифметический язык. А именно, конечное множество представляется множеством значений возрастающей конечной последовательности, последняя представляется тройкой чисел с помощью β-функции, а тройки чисел представляются одним числом с помощью какой-нибудь формульной биекции $\mathbb{N}^3$ и $\mathbb{N}$.

1.8. Вторая теорема Геделя о неполноте

1. Формулировка второй теоремы о неполноте

Вторая теорема Геделя о неполноте гласит, что утверждение о непротиворечивости PA недоказуемо в самой PA. По тезису арифметичности это означает, что нет финитного доказательства непротиворечивости PA. В частности, обычное доказательство этого факта должно использовать бесконечные множества. И действительно, обычное доказательство основано на существовании стандартной модели PA, которая бесконечна.

Здесь требуется небольшое уточнение. Поскольку непосредственно в PA можно выразить только утверждения о натуральных числах, в формулировке теоремы следует уточнить, как именно утверждение о непротиворечивости PA записывается в виде арифметической формулы. Раньше, говоря о доказуемости того или иного утверждения в PA, мы всегда указывали, как именно оно записывается в виде арифметической формулы. Сделаем это и сейчас.

Перенумеруем все арифметические формулы так, чтобы существовал алгоритм, который по номеру формулы находит саму формулу. Номер формулы φ будем

обозначать через $\ulcorner\varphi\urcorner$. Таким образом, терм $\overline{\ulcorner\varphi\urcorner}$ будет представлять формулу φ на арифметическом языке. (Напомним, что $\overline{k}$ обозначает терм $SS\ldots S0$, где S повторяется k раз.) Перенумеруем все выводы в PA так, чтобы существовал алгоритм, который по номеру вывода находит сам вывод. Рассмотрим отношение "p есть номер вывода формулы номер x". Очевидно, что этот отношение разрешимо. Запишем формулу параметрами p, x, выражающую это отношение так, как это было сделано в доказательстве теоремы 2. Обозначим эту формулу через $\mathrm{Proof}(p,x)$ и обозначим через $\mathrm{Pr}(x)$ формулу $\exists p\,\mathrm{Proof}(p,x)$. В качестве формализации утверждения о непротиворечивости PA возьмем формулу $\neg\mathrm{Pr}(\overline{\ulcorner\bot\urcorner})$, где $\bot$ есть какая-нибудь формула, отрицание которой выводимо в PA, например $0=1$.

Можно записать формулу $\mathrm{Proof}(p,x)$ и, не используя машины Тьюринга (но, конечно, используя β-функцию). Для этого надо выбрать какой-нибудь удобный способ нумерации формул и выводов и затем записать определение вывода в PA в виде формулы. Если это сделано естественным образом, то теорема Гёделя будет верна.

Теорема 7 (Вторая теорема Гёделя о неполноте). Формула $\neg\mathrm{Pr}(\overline{\ulcorner\bot\urcorner})$ невыводима в PA.

2. Доказательство второй теоремы о неполноте

Доказательство второй теоремы о неполноте использует так называемый принцип отражения, являющийся формальным аналогом теоремы Тарского.

Теорема 8 (Принцип отражения). Для любой арифметической формулы $A(x)$ с одним параметром существует арифметическое суждение φ, для которого в PA выводима формула

$$\varphi \leftrightarrow \neg A(\overline{\ulcorner\varphi\urcorner}). \tag{1.5}$$

Заметим, что в формулировке принципа отражения можно убрать отрицание перед формулой $A(\overline{\ulcorner\varphi\urcorner})$. Мы

этого не сделали, чтобы была аналогия с теоремой Тарского.

$\lhd$ Вспомним доказательство теоремы Тарского. В нём определялась конкретная формула φ, для которой истинно утверждение (1.5). А именно φ есть $\eta(\overline{N})$, где $\eta(n)$ обозначает формулу

$$\neg\exists k\,(\mathrm{Subst}(n,k)\wedge A(k)),$$

а $N=\ulcorner\eta(n)\urcorner$. Здесь $\mathrm{Subst}(n,k)$ обозначает формулу, выражающую вычислимую функцию $n\mapsto$ (номер формулы, получающейся из ψ_n подстановкой терма $\overline{n}$ вместо её параметра). Существование такой формулы следует из теоремы 2 (стр. 10). То, что построенная в доказательстве теоремы 2 формула действительно выражает данную вычислимую функцию, было доказано финитно (в чём легко убедиться, вспомнив доказательство). Применительно к нашему случаю, это означает, что мы можем доказать финитно формулу

$$\forall k\,(\mathrm{Subst}(\overline{N},k)\leftrightarrow k=\overline{\ulcorner\varphi\urcorner}).$$

Поскольку формула φ есть

$$\neg\exists k\,(\mathrm{Subst}(\overline{N},k)\wedge A(k)),$$

из этого следует равносильность φ и $\neg A(\overline{\ulcorner\varphi\urcorner})$. Таким образом, мы имеем финитное доказательство утверждения (1.5). По тезису арифметичности это утверждение выводимо в PA. $\rhd$

Теперь приступим к доказательству второй теоремы о неполноте. По принципу отражения существует формула φ для которой

$$\mathrm{PA}\vdash(\varphi\leftrightarrow\neg\mathrm{Pr}(\overline{\ulcorner\varphi\urcorner})). \tag{1.6}$$

Сначала приведём финитное доказательство такого утверждения: если PA непротиворечива, то формула φ недоказуема в PA. В виде формулы это утверждение записывается так:

$$\neg\mathrm{Pr}(\overline{\ulcorner\bot\urcorner})\to\neg\mathrm{Pr}(\overline{\ulcorner\varphi\urcorner}). \tag{1.7}$$

Рассуждая от противного, допустим, что формула φ выводима в PA. Докажем, что тогда PA противоречива. Утверждение о выводимости φ в PA, $\mathrm{Pr}(\overline{\ulcorner\varphi\urcorner})$, имеет финитное доказательство. Действительно, формула $\mathrm{Pr}(x)$ имеет вид $\exists p\,\mathrm{Proof}(p,x)$. Финитное доказательство $\mathrm{Pr}(\overline{\ulcorner\varphi\urcorner})$ состоит в предъявлении p, для которого $\mathrm{Proof}(\overline{p},\overline{\ulcorner\varphi\urcorner})$ истинно, и финитном доказательстве $\mathrm{Proof}(\overline{p},\overline{\ulcorner\varphi\urcorner})$. В том, что формула $\mathrm{Proof}(\overline{p},\overline{\ulcorner\varphi\urcorner})$ имеет финитное доказательство, можно убедиться, например, так. Разберёмся, что представляет из себя формула $\mathrm{Proof}(p,x)$. По построению, она равна $A(p,x,\overline{1})$, где $A(p,x,y)$ — формула, построенная в доказательстве теоремы 2 для выражения предиката «p есть номер вывода формулы номер x». Доказательство того, что построенная в доказательстве теоремы 2 формула действительно выражает данную вычислимую функцию, финитно. Следовательно, для любых p,x, для которых $\mathrm{Proof}(p,x)$ истинно, мы можем финитно доказать, что $\forall y\,(A(\overline{p},\overline{x},y)\leftrightarrow y=\overline{1})$. Следовательно, для таких p,x мы можем финитно доказать $A(\overline{p},\overline{x},\overline{1})$, что и требовалось обосновать.

По тезису арифметичности $\mathrm{PA}\vdash\mathrm{Pr}(\overline{\ulcorner\varphi\urcorner})$. Поэтому и в силу (1.6) получаем $\mathrm{PA}\vdash\neg\varphi$. Следовательно, PA противоречива. Итак, мы финитно доказали утверждение (1.7). По тезису арифметичности оно доказуемо в PA. Поэтому, если бы формула $\neg\mathrm{Pr}(\overline{\ulcorner\bot\urcorner})$ была доказуема в PA, то была бы доказуема и формула $\neg\mathrm{Pr}(\overline{\ulcorner\varphi\urcorner})$, а значит и формула φ. А мы знаем, что формула φ недоказуема. Вторая теорема о неполноте доказана.

Замечание 1. Изложенное доказательство не является финитным, поскольку в последнем абзаце мы использовали недоказуемость φ. Поскольку недоказуемость φ финитно следует из непротиворечивости PA, мы имеем финитное доказательство импликации «если PA непротиворечива, то ее непротиворечивость доказуема в PA»:

$$\mathrm{PA}\vdash\neg\mathrm{Pr}(\overline{\ulcorner\bot\urcorner})\to\neg\mathrm{Pr}(\overline{\ulcorner\neg\mathrm{Pr}(\overline{\ulcorner\bot\urcorner})\urcorner}) \tag{1.8}$$

Иногда вторую теорему о неполноте формулируют именно в такой ослабленной форме.

Замечание 2. В доказательстве имеется следующее сомнительное место. Дело в том, что при записи формулы $\mathrm{Proof}(p,n)$ имеется свобода: мы можем выбирать произвольным образом машину M, вычисляющую предикат "p есть номер вывода формулы номер n" (также мы можем выбирать нумерацию формул и доказательств, но это не важно). Учитывая зависимость формул $\mathrm{Proof}(p,n)$, $\mathrm{Pr}(n)$ от M, мы будем писать $\mathrm{Proof}^M(p,n)$, $\mathrm{Pr}^M(n)$. Оказывается можно построить «нечестную» программу M вычисления этого предиката, для которой формула $\neg\mathrm{Pr}^M(\overline{\ulcorner\bot\urcorner})$ доказуема в PA. Действительно, пусть программа M на входах p,n сначала проверяет, равно ли n номеру формулы $\bot$, и если окажется, что это так, то выдает 0. В противном случае программа «по-честному» вычисляет значение предиката. Поскольку формула $\bot$ не имеет доказательства в PA, программа M действительно вычисляет предикат "p есть номер вывода формулы номер n" (однако этот факт не имеет финитного доказательства). Нетрудно финитно доказать, что не существует такого p, для которого построенная программа на входах $p, \ulcorner\bot\urcorner$ выдает 1. Следовательно, формула $\neg\mathrm{Pr}^M(\overline{\ulcorner\bot\urcorner})$ доказуема в PA. Но ведь в доказательстве второй теоремы о неполноте мы не конкретизировали, какая именно программа выбрана для вычисления указанного предиката!

Внимательно просмотрев доказательство, нетрудно найти то место, в котором неявно используется тот факт, что машина M «честная». Из существования финитного доказательства утверждения

> «если PA непротиворечива, то формула φ невыводима в PA»

мы вывели доказуемость в PA формулы

$$\bigl(\neg\mathrm{Pr}(\overline{\ulcorner\bot\urcorner}) \to \neg\mathrm{Pr}(\overline{\ulcorner\varphi\urcorner})\bigr).$$

При этом мы неявно предполагали, что для $n = \overline{\ulcorner\bot\urcorner}$ и $n = \overline{\ulcorner\varphi\urcorner}$ мы можем финитно доказать равносильность утверждений «ψ_n доказуемо в PA» и $\mathrm{Pr}(n)$. Если M — нечестная машина, описанная выше, то для предиката $\mathrm{Pr}(n) = \mathrm{Pr}^M(n)$ это неверно. Действительно, утверждение $\mathrm{Pr}^M(n)$ формулируется как утверждение о том, что для некоторого p машина M на входе p,n выдаёт 1. Но для машины M мы не можем финитно доказать равносильность утверждений «для некоторого p машина M на входе $p, \overline{\ulcorner\bot\urcorner}$ выдаёт 1» и «формула $\bot$ не доказуема в PA». Действительно, первое из этих утверждений доказуемо финитно, а второе нет.

Если формула Proof построена с помощью построенной обычным образом машины, «честно» вычисляющей предикат "p есть номер вывода формулы номер n", то изложенное доказательство корректно. Возникает однако проблема строго определения понятия честного вычисления указанного предиката. Говоря неформально, программа M честно вычисляет функцию f, если утверждение «M вычисляет f» финитно доказуемо. Для того, чтобы было возможно формализовать это определение, надо, чтобы M и f определялись арифметическими формулами. Тогда формальное определение «честного вычисления» состоит в том, что формула «M вычисляет f» доказуема в PA. Но для того, чтобы применить это определение в нашем случае, надо сначала перевести понятие "p есть номер вывода формулы номер n" на арифметический язык, т. е. возникает порочный круг.

Таким образом, если мы хотим, чтобы формулировка второй теоремы о неполноте была строгой, не остается ничего иного, как явно определить, программу M, вычисляющую предикат "p есть номер вывода формулы номер n" (предварительно зафиксировав нумерации формул и доказательств), или как-нибудь по-иному явно определить формулу доказуемости. Однако нам не очень хочется это делать по следующей причине. Ведь явное определение формулы доказуемости имеет смысл только,

если потом мы без применения тезиса арифметичности докажем выводимость формулы

$$\neg\mathrm{Pr}(\overline{\lceil\bot\rceil}) \to \neg\mathrm{Pr}(\overline{\lceil\varphi\rceil}).$$

Это доказательство займет несколько страниц рутинных выкладок, разобраться в которых под силу только сверхусердному читателю. Ситуация здесь аналогична ситуации с теоремой о существовании универсальной машины Тьюринга (проще убедиться самому в существовании универсальной машины, чем разбираться в чужой конструкции). Читателю, не удовлетворенному этими разговорами, рекомендуется самому написать явную формулу доказуемости и убедиться в том, что предыдущее доказательство в самом деле можно дополнить до совершенно формального доказательства.

3. Аксиомы Бернайса

Как мы уже указывали, существуют способы записи свойства "формула ψ_n доказуема в PA", при котором вторая теорема Гёделя о неполноте неверна. В этом параграфе мы сформулируем свойства формулы $\mathrm{Pr}(x)$, достаточные для истинности теоремы Гёделя о неполноте. Эти свойства принято называть аксиомами Бернайса.

А именно, пусть $n \mapsto \psi_n$ — некоторая вычислимая нумерация арифметических формул и пусть формула $\mathrm{Pr}(n)$ выражает свойство "формула ψ_n доказуема в PA". Для произвольной замкнутой формулы ψ будем обозначать формулу $\mathrm{Pr}(\overline{\lceil\psi\rceil})$ через $\Box\psi$. Формула $\mathrm{Pr}(x)$ удовлетворяет *аксиомам Бернайса*, если для любых замкнутых арифметические формул η, ψ выполнено следующее.

1) Если $\mathrm{PA} \vdash \eta$, то $\mathrm{PA} \vdash \Box\eta$;

2) $\mathrm{PA} \vdash (\Box\eta \to \Box\Box\eta)$;

3) $\mathrm{PA} \vdash (\Box\eta \wedge \Box(\eta \to \psi) \to \Box\psi)$, в эквивалентной форме: $\mathrm{PA} \vdash (\Box(\eta \to \psi) \to (\Box\eta \to \Box\psi))$.

Теорема 9. Если формула $\mathrm{Pr}(x)$ удовлетворяет аксиомам Бернайса, то в PA выводима формула $\neg\Box\bot \to \neg\Box\neg\Box\bot$.

Поскольку все выводимые формулы истинны и PA непротиворечива, указанная формула и её посылка истинны, поэтому истинно и заключение, то есть формула $\neg\Box\bot$ невыводима в PA.

$\lhd$ По принципу отражения существует формула φ, для которой в PA выводимо $\varphi \leftrightarrow \neg\Box\varphi$. Далее убеждаемся в выводимости в PA следующих формул:
1. $\Box\varphi \to \neg\varphi$.
2. $\Box(\Box\varphi \to \neg\varphi)$ (из 1 по первой аксиоме Бернайса).
3. $\Box\Box\varphi \to \Box\neg\varphi$ (из 2 по третьей аксиоме Бернайса).
4. $\Box\varphi \to \Box\Box\varphi$ (по второй аксиоме Бернайса).
5. $\Box\varphi \to \Box\neg\varphi$ (из 3 и 4).
6. $\varphi \to (\neg\varphi \to \bot)$.
7. $\Box\varphi \to (\Box\neg\varphi \to \Box\bot)$ (из 6 по первой и третьей аксиомам Бернайса).
8. $\Box\varphi \to \Box\bot$ (из 5 и 7).
9. $\neg\varphi \to \Box\varphi$.
10. $\neg\Box\bot \to \varphi$ (из 8 и 9).
11. $\Box\neg\Box\bot \to \Box\varphi$ (из 10 по первой и третьей аксиомам Бернайса).
12. $\neg\Box\bot \to \neg\Box\neg\Box\bot$ (из 8 и 11).

Нетрудно проверить, что это рассуждение повторяет доказательство второй теоремы о полноте, изложенное ранее. $\rhd$

4. Вторая теорема о неполноте для расширений PA

Раз утверждение о непротиворечивости PA недоказуемо в PA, то почему бы не добавить его к PA в качестве новой аксиомы? Оказывается, непротиворечивость новой теории опять будет недоказуема в ней самой. Это следует из следующего простого обобщения второй теоремы о неполноте.

Пусть S некоторая разрешимая теория арифметической сигнатуры, содержащая все аксиомы PA. Постро-

им обычным образом машину Тьюринга M, разрешающую предикат «p есть номер доказательства в S формулы номер n». Запишем формулу доказуемости в S, заменив в формуле доказуемости для PA формулу $\mathrm{Proof}(p,n)$ на формулу, выражающую этот предикат. Обозначим полученную формулу через $\mathrm{Pr}_S(x)$. Нетрудно проверить, что формула $\mathrm{Pr}_S(x)$ удовлетворяет всем трем аксиомам Бернайса. Откуда получаем:

Теорема 10 (Вторая теорема о полноте для расширений PA). Если S непротиворечива, то формула $\neg\mathrm{Pr}_S(\overline{\lceil\bot\rceil})$ невыводима в S. Это утверждение доказуемо финитно.

5. Программа Гильберта

В этом параграфе мы расскажем о программе Гильберта обоснования математики, которая не была осуществлена и не могла быть осуществлена, что выяснилось почти одновременно с её опубликованием. Тем не менее знакомство с идеями Гильберта представляет интерес и сейчас. Изложение в этом параграфе будет совсем неформальным; таковым оно было и у Гильберта.

Целью программы Гильберта являлось обоснование применения идеальных объектов (таких, как бесконечные множества) в математических рассуждениях. Проблема обоснования математики возникла на рубеже XIX и XX веков, когда в теории множеств были обнаружены различные парадоксы. Другими словами, было обнаружено, что теория множеств противоречива. Эти парадоксы используют используют идеальные объекты, скажем очень большие бесконечные множества. Затем в 1908 г. Цермело и Френкель предложили аксиоматическую теорию множеств, достаточную для построения современной математики. До сих пор в ней не обнаружено парадоксов, поэтому есть надежда, что она непротиворечива. Хотя непротиворечивость системы Цермело — Френкеля не доказана (и не может быть доказана, если она действительно непротиворечива), для большинства математиков она является приемлемым решением проблемы обоснования математики.

Гильберт предлагал программу более надежного обоснования математики. По Гильберту математические утверждения делятся на *финитно осмысленные*, или *реальные*, и *идеальные*. Первые имеют содержательный смысл, вторые могут его и не иметь, однако ими можно манипулировать абстрактно по правилам некоторого исчисления. Гильберт не разъяснял четко смысл понятия реального утверждения. Заведомо реальными являются суждения типа

$$\forall x\,(f(x)=g(x)), \tag{1.9}$$

где $f(x), g(x)$ — примитивно рекурсивные функции. Например, реальными является основная теорема арифметики, постулат Бертрана (для всех $n>1$ интервал $(n,2n)$ содержит простое число), большая теорема Ферма и утверждение о непротиворечивости PA. Заведомо идеальными являются суждения, в формулировке которых присутствуют бесконечные объекты, например теорема о равномерной непрерывности непрерывной на отрезке функции и основная теорема алгебры.

В первую очередь нас интересуют доказательства финитно осмысленных утверждений. Среди них выделяются так называемые *финитные* доказательства. Гильберт использовал этот термин в значительно более ограничительном смысле, чем мы делали это в предыдущих параграфах. В этом параграфе (и только в нём) «финитный» будет значить «финитный по Гильберту». В финитных доказательствах могут использоваться только реальные утверждения. Например, изложенное ранее нами доказательство того, что каждое число, большее 1, имеет простой делитель, финитно. Финитно доказанные суждения считаются надежно обоснованными. Большинство же математических доказательств реальных суждений не являются финитными. Хотя, как правило, они могут быть переделаны в финитные. В таких случаях нефинитные рассуждения могут рассматриваться как важное

интуитивное средство получения новых истин, которые затем обосновываются надёжно. Приведем поясняющий пример. Требуется разложить многочлен x^4+4 в произведение двух многочленов с целыми коэффициентами. Без использования идеальных объектов не приходит в голову ничего лучше, чем искать разложение перебором. Вместо этого будем использовать комплексные числа. Находим корни нашего многочлена: $x = \pm 1 \pm i$. Затем пишем

$$x^4 + 4 = (x - 1 - i)(x - 1 + i)(x + 1 - i)(x + 1 + i) =$$

$$= (x^2 - 2x + 2)(x^2 + 2x + 2).$$

Мы оперировали идеальными утверждениями, однако получили равенство, обосновать которое можно обычным раскрытием скобок и приведением подобных членов.

Использование в математических рассуждениях идеальных утверждений, не имеющих смысла, таит угрозу доказать ложное реальное утверждение. Целью программы Гильберта было показать, что последнее невозможно. Точнее, требовалось установить консервативность математических теорий, оперирующих идеальными суждениями, т. е. доказать, что любое реальное утверждение, выводимое с использованием идеальных суждений, имеет финитное доказательство. Успех программы программы полностью реабилитировал бы использование идеальных утверждений: все, что доказано с их помощью может быть доказано и финитно (только быть может длиннее).

Будем говорить чуть более формально. Будем обозначать теорию финитных доказательств через R, а аксиоматическую теорию, оперирующую идеальными утверждениями, через S (мы предполагаем, что S содержит R). Консервативность S над R означает, что любое суждение языка R, выводимое в S, выводимо и в R. Отождествим реальные утверждения с утверждениями вида (1.9) (мы предполагаем, что утверждения этого типа можно записывать в языке теории R) и будем считать,

что в R доказуемы утверждения только такого вида.

Как же можно доказать консервативность S над R? Оказывается для этого достаточно доказать в R утверждение о непротиворечивости S (легко проверить, что это утверждение имеет вид (1.9)). Действительно, пусть суждение $\forall x\,(f(x) = g(x))$ доказуемо в S. Тогда истинность $\forall x\,(f(x) = g(x))$ устанавливается следующим финитным рассуждением: допустим для некоторого a выполнено $f(a) \neq g(a)$; этот факт, будучи финитно проверяемым, доказуем в R, следовательно и в S; кроме того в S доказуемо $f(a) = g(a)$, следовательно S противоречива, а мы знаем, что это не так.

Кроме того, непротиворечивость формальной теории есть её необходимое свойство, поэтому утверждение о непротиворечивости S должно быть установлено надежными (финитными) средствами.

Итак, программа Гильберта заключалась в доказательстве непротиворечивости идеальных теорий финитными средствами. Из теорем Гёделя о неполноте следует неосуществимость этой программы. А именно, из второй теоремы о неполноте следует, что даже непротиворечивость PA не имеет финитного доказательства (мы предполагаем, что все финитные доказательства проводятся в PA). Следовательно, непротиворечивость более сильных теорий также не доказуема финитно. Можно и не использовать второй теоремы о неполноте, ограничившись только принципом отражения. А именно, формула, утверждающая собственную недоказуемость в PA, является реальным суждением (в чём легко убедиться). Она истинна, но не выводима в PA. Её истинность доказана обычными математическими средствами (в качестве идеального утверждения использовалось утверждение об истинности выводимых формул), надёжность использования которых и была призвана обосновать программа Гильберта.

Литература

[1] Н.К.Верещагин. А.Шень. Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления. Москва: МЦНМО. 2000.

[2] Р. Смальян. *Теория формальных систем*, перевод с англ. Н. К. Косовского под редакцией Н. А. Шанина. М.: Наука, главная редакция физико-математической литературы, 1981. 207 с. (Серия: Математическая логика и основания математики.)

[3] Дж. Шенфилд. Математическая логика. М.: Наука, главная редакция физико-математической литературы, 1975. — 527 с.