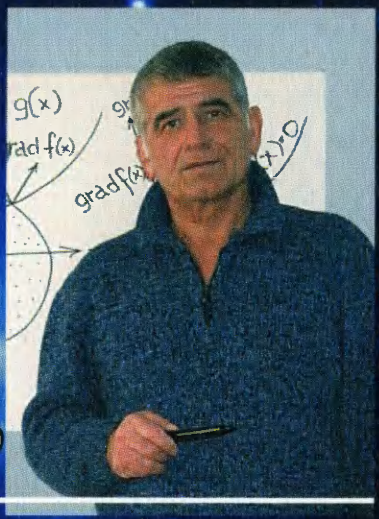
В. Босс



ЛЕКЦИИ *по* МАТЕМАТИКЕ

ТОМ 6

От Диофанта до Тьюринга

Краткое и ясное изложение предмета

URSS

В. Босс

ЛЕКЦИИ *по* МАТЕМАТИКЕ

ТОМ 6

От Диофанта до Тьюринга

МОСКВА

URSS

ББК 22.12 22.18 22.1я73

Босс В.

Лекции по математике. Т. 6: **От Диофанта до Тьюринга:** Учебное пособие. М.: КомКнига, 2006. — 208 с.

ISBN 5–484–00463–2

Книга посвящена основаниям математики, проблемам вычислимости и доказуемости. Машины Тьюринга, рекурсивные функции, логика, теория моделей, неразрешимость и неаксиоматизируемость арифметики, десятая проблема Гильберта — вот рассматриваемый круг вопросов. Изложение отличается краткостью и прозрачностью. Значительное внимание уделяется мотивации результатов и прикладным аспектам. Классическая проблематика в значительной мере переосмыслена и представлена в удобном для восприятия виде. Теоремы Гёделя, например, доказываются в несколько строчек.

Для студентов, преподавателей, инженеров и научных работников.

Издательство «КомКнига». 117312, г. Москва, пр-т 60-летия Октября, 9.
Подписано к печати 15.02.2006 г. Формат 60×90/16. Бумага офсетная. Печ. л. 13. Зак. № 463.
Отпечатано в ООО «ЛЕНАНД». 117312, г. Москва, пр-т 60-летия Октября, д. 11А, стр. 11.

ISBN 5–484–00463–2

НАУЧНАЯ И УЧЕБНАЯ ЛИТЕРАТУРА
E-mail: URSS@URSS.ru
Каталог изданий в Интернете:
http://URSS.ru
Тел./факс: 7 (495) 135–42–16
URSS Тел./факс: 7 (495) 135–42–46

3798 ID 35004
9 785484 004638 >

Оглавление

Предисловие к «Лекциям»

Отвлекаясь по дороге в баню на поездку в Сочи, забываешь куда идешь.

Для нормального изучения любого математического предмета необходимы, по крайней мере, 4 ингредиента:

1) *живой учитель*;
2) *обыкновенный подробный учебник*;
3) *рядовой задачник*;
4) *учебник, освобожденный от рутины, но дающий общую картину, мотивы, связи, «что зачем».*

До четвертого пункта у системы образования руки не доходили. Конечно, подобная задача иногда ставилась и решалась, но в большинстве случаев — при параллельном исполнении функций обыкновенного учебника. Акценты из-за перегрузки менялись, и намерения со второй-третьей главы начинали дрейфовать, не достигая результата. В виртуальном пространстве так бывает. Аналог объединения гантели с теннисной ракеткой перестает решать обе задачи, хотя это не сразу бросается в глаза.

«Лекции» ставят 4-й пункт своей главной целью. Сопутствующая идея — экономия слов и средств. Правда, на фоне деклараций о краткости и ясности изложения предполагаемое издание около 20 томов может показаться тяжеловесным, но это связано с обширностью математики, а не с перегрузкой деталями.

Необходимо сказать, на кого рассчитано. Ответ «на всех» выглядит наивно, но он в какой-то мере отражает суть дела. Обозримый вид, обнаженные конструкции доказательств, — такого сорта книги удобно иметь под рукой. Не секрет, что специалисты самой высокой категории тратят массу сил и времени на освоение математических секторов, лежащих за рамками собственной специализации. Здесь же ко многим проблемам предлагается короткая дорога, позволяющая быстро освоить новые области и освежить

старые. Для начинающих «короткие дороги» тем более полезны, поскольку облегчают движение любыми другими путями.

В вопросе «на кого рассчитано», — есть и другой аспект. На сильных или слабых? На средний вуз или физтех? Опять-таки выходит «на всех». Звучит странно, но речь не идет о регламентации кругозора. Простым языком, коротко и прозрачно описывается предмет. Из этого каждый извлечет свое и двинется дальше.

Наконец, последнее. В условиях информационного наводнения инструменты вчерашнего дня перестают работать. Не потому, что изучаемые дисциплины чересчур разрослись, а потому, что новых секторов жизни стало слишком много. И в этих условиях мало кто готов уделять много времени чему-то одному. Поэтому учить всему — надо как-то иначе. «Лекции» дают пример. Плохой ли, хороший — покажет время. Но в любом случае, это продукт нового поколения. Те же «колеса», тот же «руль», та же математическая суть, — но по-другому.

Предисловие к шестому то́му

Фундамент нужен не потому,
что в подвале жить хорошо.

Диапазон «от Диофанта до Тьюринга» подразумевается смысловой. Короче, речь идет о дискретной математике в той ее части, которая касается «оснований». Вычислимость, доказуемость, теоремы Гёделя, неразрешимые проблемы, — вот круг вопросов, определяющих русло изложения.

Что касается мотивации, то в обычном понимании ее нет, поскольку основания математики то и дело натыкаются на непреодолимые преграды, оставаясь, как говорится, при своих. Но чего, собственно, ожидать на краю? На грани, где возможное переходит в невозможное, жизнь — в смерть, теорема — в парадокс. По сути — ожидать нечего. Однако, как и в поиске смысла жизни, основную роль здесь играют побочные эффекты.

Глава 1

Алгоритмы и вычислимость

В главе рассматривается ядро проблематики *алгоритмической неразрешимости*. Изложение обходится без математической логики[1], — что рассеивает туман и позволяет выделить главное.

1.1. Универсальные вычисления

До каких-то пор игра в шахматы, сочинение музыки и решение уравнений — казались задачами разной природы. Потом было осознано, что любая информация может *кодироваться* и записываться в виде чисел, после чего механизмы решения приобретают форму арифметических и логических действий.

Кодирование представляет собой отождествление — по избранным правилам соответствия — символов или групп символов одного алфавита с символами или группами символов другого алфавита. В вычислительных машинах «на микроуровне» используется посимвольное двоичное восьмибитовое кодирование[2]. Восемь двоичных разрядов позволяют кодировать (пересчитывать) $2^8 = 256$ различных символов.

Хитросплетения теории кодирования [3, т. 4] в данном контексте не играют роли. Здесь существенна лишь сама возможность кодирования — возможность перехода к желаемому алфавиту, как правило, двоичному.

Двоичная система счисления является частным случаем p-ичной системы, в которой числа представляются в виде

$$\alpha_k p^k + \alpha_{k-1} p^{k-1} + \ldots + \alpha_1 p + \alpha_0, \quad \textit{все} \quad \alpha_j < p, \tag{1.1}$$

и записываются в *позиционной форме*

$$\alpha_k \alpha_{k-1} \ldots \alpha_1 \alpha_0.$$

---

[1] Если не считать эпизодического использования *кванторов общности и существования*, $\forall x$, $\exists x$.

[2] Windows-код 1251.

Представление (1.1) любого числа A однозначно. При делении нацело A на p в остатке получается α_0. При делении частного (полученного в результате предыдущего деления) снова на p — в остатке получается α_1. И так далее.

В случае $p = 2$ делить надо все время пополам — остатки будут нулями и единицами. Например, $33 = 2^5 + 1$, т. е. в двоичной системе

$$33 = 100001.$$

Двоичный алфавит $\{0, 1\}$ используется в компьютерах, хотя снаружи это незаметно. Однако языки программирования высокого уровня при дезинтеграции «рассыпаются» постепенно в коды машины, где мелькание нулей и единиц уже не напоминает заложенную в программу целесообразность.

На «микроуровне» имеется срез, в котором ясно, что машина всего лишь умеет выполнять четыре арифметические операции и простейшие логические. Остальное — это уже системные эффекты, чему полезно удивляться, ра́вно как и тому, что Вселенная построена из сотни химических элементов.

Таким образом, все решаемое, — вычисляется на базе арифметики и элементарной логики. Взбираясь по лестнице технического образования, важно добиться ощущения этого факта. Не умом понять, а именно ощутить. Это приходит постепенно. Знакомство с различными алгоритмами (распознавания, поиска, анализа, моделирования) и их обдумывание шаг за шагом убеждает, что любой метод в конечном итоге сводится к выполнению простейших операций.

1.2. Что такое алгоритм

Общее определение алгоритма как *рецепта достижения результата с помощью однозначной последовательности действий* — страдает определенной расплывчатостью. Какими средствами может выражаться «рецепт»; кто судит об «однозначности»; как быть, если «все хорошо», а результат не достигается? Эти вопросы снимает следующее определение.

1.2.1. *Алгоритм — это программа на любом универсальном языке программирования (например, на фортране).*

Для понимания сути определения знать программирование нет необходимости. Достаточно понимать, что *программа* — это некий

текст, определяющий работу компьютера. Никакой идеи «правильности» вычислений алгоритм не предполагает. Допускается написание программы с любыми ошибками (в пределах избранного алфавита). Компьютер, наличие которого предполагать необязательно, имеет право программу не понимать, зависать и зацикливаться на всех либо некоторых *входах*, каковыми считаются исходные данные, т. е. параметры задачи.

Может ли алгоритм доказывать теоремы? Может. Идея заключается в поиске цепочек, ведущих от исходных аксиом к формулировкам теорем. Все это кодируется, и перебором любая конечная цепочка рано или поздно будет найдена, *если существует*. Конечно, для исполнения могут потребоваться миллиарды лет, но трудоемкость алгоритма в данном случае остается вне поля зрения.

Важно понимать также, что наряду с «правильными» алгоритмами, ведущими поиск цепочек, есть «неправильные», дающие ложные заключения. Отделять зерна от плевел — задача стоящего за кадром, если таковой имеется, и у него есть желание понять, что происходит.

Существует ли, скажем, алгоритм для нерешенной *проблемы Гольдбаха*, предполагающей возможность представления любого четного числа $n > 2$ в виде суммы двух простых? Существует. Это, например, один из двух алгоритмов, первый — всегда говорит «да», второй — «нет». Один из них дает правильный ответ, какой — неясно. И это не насмешка над здравым смыслом, а обнаженная характеристика проблемы. Алгоритм — это абсолютно тупая и бездушная вещь, — так проводится граница. Понятия смысла и соответствия остаются за бортом. Если вычисления обнаруживают признаки интеллекта, то это результат интерпретации и «сопровождения».

Другое дело, что за счет *массовости*, о чем будет сказано далее, удается отсеять алгоритмы, которые дают правильные ответы по недоразумению (случайно).

1.3. Вычислимость

1.3.1. Определение. *Целочисленную функцию* $f(n)$ *целочисленного аргумента называют вычислимой, если существует алгоритм, вычис-*

ляющий значения $f(n)$, но необязательно приводящий к результату. Множество вычислимых функций обозначается через $\mathbb{F}$.

Заметим, что аргумент может быть также векторным, $n = \{n_1, \ldots, n_k\}$. Функцию $f(n_1, \ldots, n_k)$ в этом случае называют ***k*-местной.** *Включение запятых в алфавит с последующей перекодировкой цифрами — позволяет все функции считать одноместными.*

Как уже отмечалось, *процедура вычислений* отождествляется с программой работы компьютера[3)], представляющей собой запись алгоритма на некотором языке в некотором алфавите $\mathbb{A}$,

$$P = a_1 a_2 \ldots a_N, \quad \textit{все} \quad a_j \in \mathbb{A}. \tag{1.2}$$

Программа применяется к различным *входным словам*. Если входные и выходные данные кодируются числами, программа определяет *вычислимую функцию*. С точностью до педантизма к такому определению сводятся все подходы.

Известны многочисленные попытки определения вычислимой функции. В 1936 году Тьюринг ввел функции, вычислимые конечной машиной, известной ныне как *машина Тьюринга*. В том же году Гёдель, Эрбран, Клини ввели *рекурсивные функции*. Затем Чёрч, Пост, Марков — выделяли иные классы функций. Но все пути, как выяснилось, «ведут в Рим» — приводят к одному и тому же классу вычислимых функций.

Запись программы вычислений в виде (1.2) позволяет *все вычислимые функции перенумеровать*[4)],

$$f_1(n), \ldots, f_k(n), \ldots . \tag{1.3}$$

Сначала перечисляются все программы из одной буквы, потом из двух, потом из трех и так далее.

Нумеруются таким образом не функции, а программы, и возникает естественная мысль изгнать функции из лексикона, оставив

[3)] Технократы давно свыклись с мыслью, что любой алгоритм реализуем на вычислительной машине. Решение уравнений, лингвистические задачи, игра в шахматы, аудио- и видео-приложения, — все это программируется, кодируется, вычисляется, и результат выдается в любой желаемой форме.

[4)] Независимо от предположения о наличии такого инструмента, как компьютер. Важно существование самого рецепта (1.2).

алгоритмы. Но принято говорить о функциях, иначе потеряется возможность в простых ситуациях типа $f(n) = n!$ обходиться без упоминания конкретных программ. Поэтому о вычислимой функции говорят как о функции в обычном понимании, но за кадром подразумевается наличие алгоритма. В простых ситуациях это не приводит к недоразумениям.

В то же время возникает потребность в обременительных уточнениях. Каждая функция в перечислении (1.3) получает бесконечное количество номеров, поскольку разнообразие алгоритмов неисчерпаемо. Что-нибудь по ходу делится пополам, потом умножается на 2, — вот уже и другой алгоритм. Далее. Если две разные программы вычислений дают одинаковые результаты при различных n, они определяют разные функции или одну и ту же? Ответ неоднозначен, потому что вопрос плохо поставлен. Ситуации $f(n) \equiv g(n)$ бывают разные, от тривиальных до недоказуемых. Поэтому возникает соблазн сказать так. Функции $f(n)$ и $g(n)$ различны, если вычисляются принципиально разными алгоритмами. Но это уже совсем плохо. Если программа перепроверяет себя семь раз, — это алгоритм другой, но — принципиально или непринципиально?

Чем глубже вдумываешься, тем сильнее меняется фокус понимания[5]. Для хорошего ответа чем-то приходится жертвовать. Тут бы, конечно, прибегнуть к транквилизатору педагогической лжи, обходя острые углы. Но в обнажении слабых мест есть свои плюсы. Проясняется мотивация более громоздких, но менее зыбких теорий. В то же время некоторая расплывчатость определения не влияет на строгость приводимых далее выводов. Внимательный анализ доказательств показывает: несмотря на приговаривание о функциях, манипулирование всегда идет алгоритмами.

Ситуация чем-то напоминает ряды Фурье, где пишут

$$f(x) = \sum^{\infty} \dots .$$

И хотя равенство не всегда выполняется, — жонглируют рядами, но говорят о функциях [3, т. 1].

[5] Здоровье, как говорила Раневская, это когда каждый день болит в другом месте. Понимание в этом смысле имеет другую природу.

Строгое уточнение определения 1.3.1 *на данном этапе заключается в следующем. Вычислимая функция — это множество эквивалентных алгоритмов, дающих на любом входе* n *один и тот же результат — определенный или неопределенный. В нумерации* (1.3) *каждая функция имеет бесконечное число своих представителей (номеров).*

В этом случае все становится на свои места, правда, появляются трудности с другой стороны — при необходимости гуманитарно судить о вычислимости некоторых «аномальных» функций. Что касается двух разных программ, дающих одинаковые результаты при различных n, то в последнем варианте определения — это одна и та же функция. Однако, как выяснится впоследствии, совпадение результатов работы разных алгоритмов — в общем случае неразрешимая проблема.

Напомним далее, что определение алгоритма допускает *любые программы*, в том числе: синтаксически неправильные либо зацикливающиеся на всех или некоторых входах. Поэтому среди вычислимых функций обязательно есть — неопределенные на всех или каких-то аргументах. Неопределенность, $f(n) =?$, возникает в двух случаях: алгоритм работает безостановочно либо останавливается, не зная, что дальше делать. В случае «нормальной» остановки — по завершению вычислений — можно предусмотреть печать специального знака. Либо, наоборот, при зависании предусмотреть вхождение алгоритма в цикл, чтобы неопределенность возникала лишь в одном случае (безостановочной работы).

На осознание проблематики имеет смысл потратить какое-то время, рассматривая задачу с разных сторон. Возьмем в качестве входного и выходного алфавита — латинские и русские буквы, цифры и всевозможные математические знаки. Кодирование позволяет все это перевести в двоичные числа. Далее все тексты упорядочим, пронумеруем. В последовательности текстов $\{P_n\}$ найдутся осмысленные компьютерные программы P_n. Найдется также роман «Идиот», текст из точек и запятых, и вообще все, что было и не было когда-либо написано. Тем не менее любые тексты будем считать программами P_n, — благо, по данному выше определению, они не обязаны работать.

Вот что такое нумерация (1.3). «Интерпретатор» будет, конечно, диву даваться, но время от времени ему будут попадаться осмысленные программы P_n на оговоренном заранее алгоритмическом языке.

Многочисленные попытки регламентировать описание алгоритмов (*машины Тьюринга*, *МНР*, *рекурсивные функции* — см. далее) позволяют исключить из поля зрения непрофильные тексты, но с точки зрения рассматриваемой проблематики — это не имеет большого значения.

1.4. Примеры и комментарии

Решение целочисленных задач, например, *коммивояжера или линейного программирования*, *поиск наибольшего общего делителя либо корней диофантова уравнения*, — все это вычислимые функции, за которыми стоят различные алгоритмы. Здесь вполне очевидно, почему удобнее говорить о функциях, а не о программах. Используется ли для задачи коммивояжера один из переборных алгоритмов [6] или динамического программирования, — весь этот куст рецептов имеет общий корень и направлен на решение одной смысловой задачи. Предложение отвлечься от семантики и спуститься на уровень синтаксиса здесь едва ли привлекательно.

Возьмем кочующий из книги в книгу пример

$$f(n) = \begin{cases} 1, & \textit{если в десятичной записи числа } \pi \textit{ есть ровно } n \\ & \textit{идущих подряд нулей;} \\ 0, & \textit{в противном случае,} \end{cases} \tag{1.4}$$

где напрашивается процедура последовательного определения цифр десятичного разложения числа π. Если на каком-то шаге появляется n соседних нулей, процесс останавливается, $f(n) = 1$. Но в случае $f(n) = 0$ для некоторого n — указанная процедура никогда не остановится. И не ясно, существует ли эффективная процедура. Поэтому не ясно, вычислима $f(n)$ или нет. Причем большинство думает — невычислима. Так пишется в одной книжке.

Другой автор занимает иную позицию. Очевидно, либо $f(n) \equiv 1$, либо $f(n > n_0) \equiv 0$. В любом из этих случаев существует подходящий алгоритм, выдающий — вне смысловой связи с $f(n)$ — либо одни единицы, либо нули после n_0, — поэтому функция $f(n)$ вычислима.

В третьей книжке с тем же успехом можно возразить, что алгоритм существует, но его невозможно эффективно указать.

---

[6] Каковых есть «миллион», с различной организацией порядка перебора.

Вопрос «где правда» — не имеет ответа. Дело не в том, «кто прав», а в том, что описание $f(n)$ использует недопустимую конструкцию языка, и это выводит ситуацию за пределы «правового поля». Регламентация средств будет проводиться в главе 5.

Заведомо вычислима другая функция

$$g(n) = \begin{cases} 1, & \textit{если в десятичной записи числа } \pi \textit{ есть ровно } n \\ & \textit{идущих подряд нулей;} \\ ?, & \textit{в противном случае.} \end{cases}$$

Значения $g(n)$ вычисляет та же бесхитростная процедура определения цифр десятичного разложения числа π, не обязанная теперь останавливаться «в противном случае».

Конечно, возможно $f(n) \equiv g(n)$, что может быть как доказуемо, так и не доказуемо. Но к вопросу о вычислимости это не имеет отношения, разве что становится в принципе ясно, что та же самая программа вычисляет и $f(n)$, потому что случай $f(n) = 0$ ей не встретится. Расплывчатость проблемы опять-таки проистекает из наличия «философского» зазора и отсутствия фактического — между функцией и программой. И здесь легко утопить картину в деталях, не соблюдая гигиену словоупотребления.

Рассмотрим еще один «плохой пример»,

$$f(n) = \begin{cases} 1, & \textit{если } x^n + y^n = z^n \textit{ разрешимо в целых числах;} \\ 0, & \textit{в противном случае.} \end{cases} \qquad (1.5)$$

Поскольку теорема Ферма, наконец, доказана, то $f(n) \equiv 0$ при $n > 2$. Но точнее сказать, что $f(n)$ и есть функция, равная нулю при $n > 2$, и — единице при $n = 2$, — не упоминая никакую теорему Ферма.

Присутствие в (1.5) неразрешимости $x^n + y^n = z^n$ наводит тень на плетень и уводит задачу совсем в другую область, *доказуемости*. Корень зла — снова в использовании недопустимых конструкций языка.

На фоне сказанного естественно возникает вопрос. Имеет ли право алгоритм пользоваться теоремами типа

$$(n - m)^2 = n^2 - 2nm + m^2 \,?$$

Ведь без аксиом и правил логического вывода утверждения вида «для всех n имеет место то-то и то-то» — установить нельзя.

Тем не менее — имеет. Алгоритм имеет право на все. Положить, например, $2 = 3$ либо $(n - m)^2 = n^2 - m^5$. В результате счета будет получаться какая-то функция, неважно какая. А если наблюдателю хочется, чтобы машина вычисляла «его функцию», то это проблема наблюдателя, а не машины, — установить соответствие алгоритма внешнему описанию функции.

1.5. Проблема неопределенности

Неопределенность некоторых вычислимых функций заключается не только в ошибочных программах, приводящих к зависанию компьютера. Отсеять «мусор» из (1.3) можно введением грамматического фильтра, способного оставить в последовательности (1.3) только те тексты, которые действительно являются программами. Пробелов нумерации легко избежать, нумеруя после фильтрации. Однако никакие меры не могут предотвратить зацикливание некоторых программ на некоторых входах, — и любые усилия в этом направлении бессмысленны.

1.5.1. Теорема. *Любая попытка ввести понятие вычислимой функции $f(n)$ так, чтобы она была определена при любом n, — **неразумна**.*

◀ С помощью нумерации (1.3) определим функцию

$$g(n) = f_n(n) + 1.$$

Она не вычислима, так как при $n = 1$ отличается от f_1, при $n = 2$ — от f_2, и так далее. С другой стороны, она вычислима в любом разумном смысле, поскольку к вычисляемому значению $f_n(n)$ всегда можно прибавить 1. ▶

Это стандартный трюк из категории *диагональных рассуждений*, каковые в рассматриваемой области часто используются. В популярной литературе существование функции $g(n) = f_n(n) + 1$ иногда трактуется как парадокс, что порождает нежелательные заблуждения.

Если какие-то функции в перечислении (1.3) определены не при всех n, конструкция $g(n) = f_n(n) + 1$ к противоречию не приводит. (?)

Формулировка теоремы 1.5.1, конечно, слегка зашкаливает, но здесь важно заострить внимание. Определение вычислимой

функции $f(n)$ при любом n — принципиально обречено на провал. Или получаются слишком узкие классы функций, дискредитирующие понятие вычислимости, или какие-то $f(n)$ перестают вычисляться. А попытка доопределить $f(n)$ «силовым методом» не проходит, иначе получается сказка про белого бычка — возврат к теореме 1.5.1, и — по тому же кругу.

Источник неприятностей имеет много лиц. Вот самое простое. Определение функций с помощью заведомо выполнимых прямых действий (типа сложения, умножения, логических операций) позволяет говорить об уравнениях

$$u(m, n) = 0, \tag{1.6}$$

решение которых $m = f(n)$ естественно относить к вычислимым функциям. В противном случае теория превращается в малополезную игрушку. В то же время (1.6) принципиально не всегда разрешимо, что интуитивно более-менее ясно, и с некоторыми усилиями устанавливается формально (см. далее).

Что касается существования *невычислимых функций*, то это ясно из того, что различных функций $f(n)$ имеется континуум [7], а вычислимых — счетное число (1.3).

Конкретно указать невычислимую функцию тоже просто. Очевидно,

$$h(n) = \begin{cases} f_n(n) + 1, & \textit{если значение } f_n(n) \textit{ определено;} \\ 0, & \textit{если значение } f_n(n) \textit{ не определено} \end{cases} \tag{1.7}$$

невычислима. Для доказательства предположим противное, т. е. $h(n) = f_p(n)$ при некотором p. Но этого не может быть, так как $h(p) \neq f_p(p)$, если значение $f_p(p)$ определено, и $h(p)$ определено, если $f_p(p)$ не определено.

Отсюда вытекает, кстати, существование принципиально недоопределяемых (для любых n) вычислимых функций.

[7] Если функции принимают только значения $0, 1, \ldots, 9$, то каждой функции f соответствует вещественное число $0, f(1)f(2)\ldots \in [0, 1]$.

1.6. Перечислимые множества

Одна из естественных задач вычислительного характера — перечисление элементов множества, каковое считается *перечислимым*, если существует эффективная процедура (алгоритм) порождения его элементов. Элементы перечислимого множества эффективно нумеруются — в порядке появления.

• Характеристика «эффективно» добавляется в тех случаях, когда за кадром подразумевается незацикливающийся и независающий алгоритм, определенный при любом n.

Множество называется *разрешимым*, если существует эффективная процедура для выяснения принадлежности любого n этому множеству. Говорят также, что разрешимое множество *распознаваемо*.

(!) Гуманитарный характер данных определений позволяет им лучше укладываться в голове, но размывает предмет, что становится ясно, когда доходит до дела. Чтобы не усиливать ощущение туманности, эти определения лучше привязать к уже оговоренному источнику.

1.6.1. Определение. *Множество X перечислимо, если оно есть область значений либо область определения вычислимой функции.*

◀ Это уже более однозначно, но не сразу увязывается с предыдущим. Если X — область значений $f(n)$, то как порождать его элементы? Процедура «зависнет» на первом же n, при котором значение $f(n)$ не определено. Для параллельного вычисления $f(n)$ сразу при всех n требуется (вроде бы) бесконечное число компьютеров, что не очень согласуется с представлением о возможной реализации алгоритма.

Однако достаточно одного компьютера. Пусть $P(n, m)$ обозначает реализацию m шагов работы программы по вычислению значения $f(n)$. Пары чисел (n, m) упорядочиваются стандартным образом (нумеруются вдоль стрелочек):

$$\begin{pmatrix} (1,1) & \to & (1,2) & & (1,3) & \to & (1,4) & \dots \\ & \swarrow & & \nearrow & & \swarrow & & \\ (2,1) & & (2,2) & & (2,3) & & (2,4) & \dots \\ \downarrow & \nearrow & & \swarrow & & & & \\ (3,1) & & (3,2) & & (3,3) & & (3,4) & \dots \\ & \swarrow & & & & & & \\ (4,1) & & (4,2) & & (4,3) & & (4,4) & \dots \\ \downarrow & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}, \tag{1.8}$$

после чего программе дается возможность последовательно работать по m шагов, вычисляя $f(n)$, в избранном порядке. Понятно, все значения $f(n)$ будут рано или поздно перечислены.

В пояснении нуждается также другой момент. Определение содержит в себе теорему: *область значений любой вычислимой функции всегда есть область определения другой вычислимой функции, и наоборот*. Устанавливается это с помощью той же процедуры $P(n, m)$, вычисляющей $f(n)$ на протяжении m шагов. Если вычисление $P(n, m)$ приводит к определенному результату, n объявляется значением функции $g(k)$, где k — номер пары (n, m). В результате область определения f становится областью значений g. Обратный трюк еще проще. ►

Формальное определение разрешимого множества остается, по существу, прежним.

1.6.2. Определение. *Множество X разрешимо, если его характеристическая функция,*

$$\theta_X(x) = \begin{cases} 1, & \text{если} \quad x \in X; \\ 0, & \text{в противном случае}, \end{cases}$$

вычислима.

Упражнения

- Если X и Y перечислимые (разрешимые) множества, то объединение $X \cup Y$, пересечение $X \cap Y$ и декартово произведение [8] $X \times Y$ — также перечислимы (разрешимы).
- Множества квадратов n^2; простых чисел; квадратных уравнений с целыми коэффициентами, не имеющих действительных корней, — перечислимы и разрешимы. Множество стозначных чисел, встречающихся в десятичной записи π, — перечислимо, но не ясно, разрешимо ли (несмотря на конечность).
- Непустое множество X перечислимо, если (и только если) оно является областью значений либо нигде, либо всюду определенной вычислимой функции [9].
- Множество $X \subset \mathbb{N}$ перечислимо тогда и только тогда, когда оно является проекцией некоторого разрешимого множества пар $Z \subset \mathbb{N} \times \mathbb{N}$.
  (*Подсказка*. Перечислимость проекции перечислимого (тем более разрешимого) множества — очевидна. Обратно, перечислимое X есть проекция множества Z пар (x, n), где x есть n-й элемент в перечислении X. Разрешимость Z очевидна.)

[8] Множество пар (x, y), где $x \in X$, $y \in Y$.

1.6.3. Теорема Поста. *Для разрешимости X необходимо и достаточно, чтобы X и его дополнение $\overline{X}$ были перечислимы.*

◀ *Необходимость.* Если программа P определяет, принадлежит n множеству X или нет, то ее последовательная работа на $n = 0, 1, 2, \ldots$ разбивает натуральный ряд на два списка X и $\overline{X}$.

Достаточность. Если P перечисляет X, а Q — $\overline{X}$, то попеременная работа программ P и Q рано или поздно любое n внесет в один из списков X или $\overline{X}$, что дает разрешающий алгоритм. ▶

1.6.4. Теорема. *Существует перечислимое, но неразрешимое множество положительных целых чисел.*

◀ Пусть $S_1, S_2, \ldots$ — эффективное перечисление всех перечислимых множеств[10]. Заметим, если бы все S_n были разрешимы, то и все дополнения $\overline{S}_n$ входили бы в перечисление $S_1, S_2, \ldots$ (теорема 1.6.3).

Образуем множество D из тех номеров n, которые принадлежат S_n. Таким образом,

$$n \in D \cap S_n \Leftrightarrow n \in D \cup S_n,$$

откуда следует невозможность[11] $D \cap S_n = \varnothing$ и в то же время $D \cup S_n = \mathbb{N}$. Это означает, что D не совпадает ни с одним $\overline{S}_n$, т. е. не перечислимо, а значит (теорема 1.6.3) и неразрешимо. ▶

Теорема 1.6.4 — краеугольный результат, от которого не так далеко до знаменитых теорем Гёделя. Связующая нить обрисована в разделе 2.1.

Отметим, наконец, два принципиальных, хотя и очень простых по доказательству, утверждения.

1.6.5. *Образ и прообраз перечислимого множества при вычислимом преобразовании — перечислимы.*

1.6.6. *Для вычислимости $f(x)$ необходима и достаточна перечислимость графика, т. е. множества пар $\{x, f(x)\}$.*

---

[10] Существование перечисления перечислимых множеств следует из наличия перечисления (1.3) вычислимых функций, области значений которых и являются множествами $S_1, S_2, \ldots$.

[11] Непустота D при любой организации перечисления $\{S_n\}$ следует хотя бы из того, что $\{S_q = \mathbb{N}\}$ при каком-то q.

1.7. Эффективные процедуры

Аналогом разрешимого множества является понятие *эффективно вычислимой функции* $f(n)$, которая, по определению, вычислима и определена при любом n. В теории рекурсивных функций — это так называемые *общерекурсивные функции*.

1.7.1. Теорема. *Множество эффективно вычислимых функций неперечислимо (не может быть эффективно пронумеровано).*

◄ В данном случае работает та же конструкция, что и в доказательстве теоремы 1.5.1. Если существует нумерация f_n, то функция $g(n) = f_n(n) + 1$ заведомо эффективно вычислима, но не присутствует в списке $\{f_n\}$. ►

Понятно, что рассматриваемые (пока) факты неразрешимости крутятся вокруг одной и той же идеи. Но глубина и простота этой идеи такова, что каждый маленький поворот дает новое освещение. Причем без центрального стержня все эти «повороты» рассыпаются в рой полумистических сентенций, которые, имея общую природу, светятся единой загадкой.

1.8. Машины Тьюринга

Проблематика алгоритмической вычислимости и разрешимости исторически начиналась с машин Тьюринга и рекурсивных функций. Сейчас это уже археология. Начинать издалека теперь необязательно, но и вычеркивать — не вычеркнешь. Кроме того, это язык, который весьма эффективен в определенных секторах.

Машина Тьюринга представляет собой конечный автомат, способный читать и писать на бесконечной ленте. Точнее говоря, лента разбита на ячейки, приспособленные для записи букв из некоторого алфавита $A = \{a_1, \ldots, a_m\}$, например, из $\{0, 1\}$:

...	1	**0**	1	...	0	...

Время дискретно. В каждом такте автомат обозревает содержимое текущей ячейки [12], стирает и записывает в эту ячейку новую букву [13], после чего переходит к соседней ячейке (слева или справа) и меняет свое внутреннее состояние.

[12] На рисунке символ в обозреваемой ячейке выделен жирным шрифтом.

[13] Которая, в том числе, может совпадать с прежней.

Формализованно процесс выглядит так: t — время, $x(t)$ — входной сигнал автомата (буква, которую он читает в момент t), $y(t+1)$ — выходной сигнал (буква, которую автомат записывает в ячейку вместо $x(t)$), $q(t)$ — внутреннее состояние автомата, число которых предполагается конечным, наконец, $d(t+1)$ — направление сдвига головки.

Машина M характеризуется тремя функциями F, G и H, определяющими динамику «вычислений»,

$$y(t+1) = F[q(t), x(t)],$$
$$q(t+1) = G[q(t), x(t)],$$
$$d(t+1) = H[q(t), x(t)],$$

показывающими: F — «что в ячейку писать», G — «в какое состояние переходить», H — «куда сдвигаться, влево или вправо».

В каждом такте работу машины можно описывать также в виде

$$q_i a_j \to q_k a_l L \quad \textit{или} \quad q_i a_j \to q_k a_l R, \tag{1.9}$$

что подразумевает следующее. Если машина, находясь в состоянии q_i видит перед собой a_j, то она стирает a_j, пишет a_l, переходит в состояние q_k и сдвигается влево (Left) или вправо (Right). Список всевозможных (для данной машины) переходов (1.9) задает сразу все функции F, G и H.

Кто знаком с возможностями конечных автоматов, едва ли удивится, что такая машина способна на многое. Достаточно сказать, что современный компьютер — это универсальный конечный автомат. Наращиваемость памяти расширяет его возможности. Такой же эффект обеспечивает бесконечная лента машины Тьюринга [14)].

Традиционно при описании машины Тьюринга упор делается на ее чрезвычайную простоту. Дескать, есть лента и головка, считывающая и записывающая, которая ходит вдоль ленты «влево-вправо». Вот, собственно, и вся машина. Ну разве что, у головки есть несколько внутренних состояний, которые меняются в зависимости от прочитанной буквы.

Такая расстановка акцентов обычно дает эффект, что нужно признать удачным использованием художественных средств для маскировки неограниченного потенциала.

[14)] Всегда предполагается (!), что лента, к работе с которой приступает конечный автомат, имеет лишь **конечное** число заполненных ячеек, остальные пусты. Поэтому можно говорить не о бесконечной, а о наращиваемой ленте.

Богатые возможности машины Тьюринга устанавливаются достаточно просто. Сначала конструируются машины, выполняющие простейшие арифметические и логические операции. Затем выясняется возможность работы таких машин в комбинации друг с другом, что порождает более сложные машины. Те, в комбинации друг с другом, порождают еще более сложные машины. И так далее.

Скрупулезное описание работы отдельных машин Тьюринга, а также конкретных способов их объединения в тандемы, — на данном этапе развития цивилизации стало малоинтересным. Когда все было в новинку, энтузиазма хватало, чтобы вникать в детали. И это было важно, потому что общие рассуждения нередко ведут к ошибкам. Как «от великого до смешного — один шаг», так и от истины — до ереси. Дьявол, прячущийся в деталях, всегда наготове. Поэтому рутинная работа по анализу тьюринговой вычислимости сыграла свою историческую роль, но повторять пройденное уже мало кто хочет. Сегодня для принципиальной ясности достаточно двух-трех примеров и нескольких общих замечаний.

Так или иначе, Тьюринг очертил границы, четко определив «инструмент». Общими усилиями было осознано, что для любого алгоритма, приходящего в голову, существует реализующая машина. Но *тезис Тьюринга*: «*Любой алгоритм, являющийся таковым с интуитивной точки зрения, реализуем машиной Тьюринга*», конечно, может быть справедлив только в «религиозном смысле», поскольку ***интуитивное*** понимание алгоритма — явление внематематическое.

Тезис Тьюринга используется, когда возникает необходимость утверждать существование машины Тьюринга для функции, алгоритмическая вычислимость которой ясна из «посторонних» соображений, проистекающих из опыта.

Естественно, в алгоритмизации возникли альтернативные подходы. В первую очередь заслуживают упоминания *рекурсивные функции*, но об этом будет сказано отдельно (раздел 1.10). В «компьютерном направлении» можно отметить *машины с неограниченными регистрами* (МНР) [15].

Универсальная машина. Машины Тьюринга (в силу конечности описания каждой) можно *эффективно перечислить*, $M_1, \ldots, M_n, \ldots$.

[15] МНР называют также *адресными машинами*, см. раздел 1.12.

Восстановление функций F, G и H по номеру n оказывается при этом достаточно простой операцией, выполнимой некоторой машиной U, на которую — после восстановления M_n — может быть возложена имитация работы M_n на любом входном слове k. В этом случае U называется *универсальной машиной Тьюринга*,

$$U(n, k) = M_n(k).$$

Универсальной машиной иного типа является современный компьютер, где индивидуальный подход к задачам обеспечивается разными программами. Правила изменения внутренних состояний могли бы, конечно, быть запаяны внутрь конструкции, — но тогда для каждой задачи требовался бы свой компьютер. В универсальном варианте перестройка под задачу производится вводом информации извне, с клавиатуры или дисковой памяти.

Похожая картина наблюдается в ситуации с универсальной машиной Тьюринга. Ее подробное описание [12, 20], несмотря на принципиальную ясность вопроса, имеет определенный смысл, поскольку некоторые детали выглядят проблематично. Например, может ли U, имея фиксированное число внутренних состояний, моделировать работу машин Тьюринга M_n, имеющих большее число состояний?

Может. Нехватка состояний компенсируется записями в памяти (на ленте), что иллюстрируется примером обычного компьютера. Шеннон, кстати, показал, что для U достаточно всего двух состояний (!), но тогда нужен «большой» алфавит. Возможен другой вариант. Алфавит двоичный, но требуется «много» состояний. В [20] описана универсальная машина с четырьмя буквами в алфавите и семью внутренними состояниями [16)].

1.9. О «внутренней кухне»

Главный недостаток машин Тьюринга — низкий языковой уровень описания вычислительных процессов, не обеспечивающий наглядную интерпретацию. Но есть и плюсы. В первую очередь — это

[16)] С точки зрения теории вычислимости такие головоломки не представляют интереса, но дают пищу для ума, что время от времени дает всходы.

конкретность и недвусмысленность, что при определенном устройстве воображения играет немаловажную роль. При описании любой машины никакие «посторонние куски текста» не могут встретиться. Это избавляет от необходимости нумеровать всякий «мусор», как было раньше.

Более-менее систематическое изложение машин Тьюринга имеется в [12, 20]. Общее представление можно составить по нижеследующим примерам и замечаниям.

• Среди внутренних состояний машины $q_1, \ldots, q_n$ выделяется начальное — q_1, в котором машина приступает к работе, и конечное — q_n, попадая в которое, машина останавливается.

• Машины легче конструировать при использовании *единичного кода*, в котором число N записывается в виде последовательности N единиц с возможными пропусками — пустыми ячейками, $\varnothing$. Числа отделяются друг от друга оговоренным знаком, например, $*$.

Для сложения двух чисел N_1 и N_2 достаточно, чтобы машина убрала вторую звездочку в *машинном слове*

$$\underbrace{*\,1\,\varnothing\,1\,\ldots\,1}_{N_1\ \text{единиц}}\,*\,\underbrace{1\,1\,\ldots\,\varnothing\,1}_{N_2\ \text{единиц}}.$$

Задача решается следующим образом. Пусть M начинает работу с левой единицы, и в ее списке (1.9) присутствуют операции

$$q_1 1 \to q_1 1 R, \quad q_1 \varnothing \to q_1 \varnothing R.$$

Тогда M будет двигаться вправо, ничего не меняя [17], пока не дойдет до $*$. Здесь в ее списке (1.9) должна присутствовать команда $q_1 * \to q_2 \varnothing L$, приводящая к стиранию звездочки и переходу в новое состояние q_2, которое может быть заключительным. В другом варианте можно организовать возврат головки в исходное положение (к левой единице)

$$q_2 1 \to q_2 1 L, \quad q_2 \varnothing \to q_2 \varnothing L, \quad q_2 * \to q_3 * R,$$

где q_3 — конечное состояние машины в новом исполнении.

• **Преобразование единичного кода в двоичный.** Для определения четности числа N машине требуются два состояния, которые бы она попеременно меняла после чтения каждой единицы, двигаясь все время вправо. Наткнувшись на обозначение конца N, она бы печатала 0 или 1 (после $*$) — в зависимости от состояния.

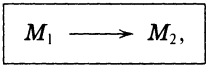
Для перевода N из единичного кода в двоичный — описанный счетчик необходимо немного усложнить. Алгоритм выглядит так. Сначала пересчитываются N единиц и пишется 0 при четном N и 1 — при нечетном. Это дает последний

[17] Поскольку все время стирает единицу и снова ее записывает.

разряд двоичного кода N. При пересчете каждая вторая единица стирается, а также стирается последняя единица, если после нее нет «второй». Оставшиеся единицы в количестве [18] $[N/2]$ пересчитываются аналогичным образом, что дает следующий разряд двоичного кода N. И так далее — до исчерпания всех исходных единиц.

Утрясти детали не так сложно, располагая несколькими дополнительными состояниями. Принципиального решения требуют два вопроса. Стирание четных единиц и сдвиг вправо уже полученных разрядов двоичного кода N перед получением следующего разряда (для освобождения места).

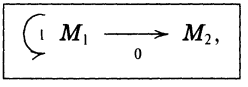
• Решение только что упомянутых вопросов значительно упрощает следующее общее соображение. Если задача распадается на две подзадачи, которые надо решить последовательно, то машины Тьюринга M_1 и M_2 для подзадач можно конструировать независимо, и включать M_2 после завершения работы M_1. Это выглядит как связка двух машин,



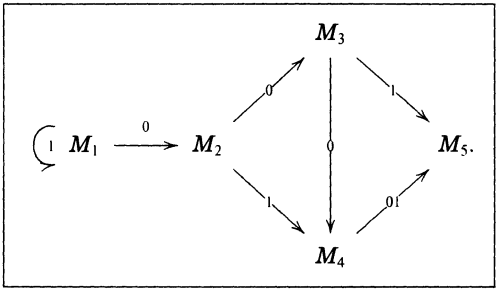
(1.10)

но может рассматриваться как единая машина Тьюринга при отождествлении конечного состояния M_1 и начального M_2, в результате чего возникают единые таблицы функций F, G и H, характеризующие работу блок-схемы (1.10) в целом. Следовательно, композиция (последовательное соединение) машин Тьюринга — есть машина Тьюринга.

Такого же рода консолидация в единую машину возможна и при сложном ветвлении алгоритмов в зависимости, например, от последней напечатанной цифры:



либо



Продумывание таких возможностей довольно быстро продвигает к ощущению «неограниченных» возможностей машин Тьюринга. Тем не менее в фокус внимания надо поместить еще одно обстоятельство.

[18] Квадратные скобки обозначают целую часть числа.

Блок-схемы алгоритмов описывают работу системы *по управлению* (к работе какого блока переходить). Но при переходах блоку необходимо еще указать, где и как искать информацию, его касающуюся. Поэтому устройство блоков (машин Тьюринга) должно предполагать умение искать информацию.

• **Поиск информации.** Допустим, информация на ленте записана в виде слов W_j и признаков S_j (*адресная память*). Пары S_jW_j могут быть отделены друг от друга двумя звездочками, а признаки от слов — одной. Где-то на ленте записан желаемый признак S. Машина ищет сначала ближайшую пару S_jW_j, потом — следующую, и каждый раз челночными проходами осуществляет поразрядное сравнение S и S_j.

Изобретение такой машины — дело нехитрое. Сложная задача — оптимизация поиска, но это совсем другая проблема, в данном контексте не играющая роли.

• **Многомерные состояния.** Конструируя машину Тьюринга, удобно рассуждать, имея в распоряжении *разнородные* состояния. В следующем, например, исполнении. Имеется набор k *опций*, которые можно включать и выключать. Включена опция q_5 — головка движется влево, q_2 — стирание, q_8 — заполнение нулями, q_3 — поиск информации и т. д.

В результате совокупное внутреннее состояние будет характеризоваться двоичным числом $10\ldots0101$ (1 в j-м разряде — опция q_j включена, 0 — выключена).

Другое удобное послабление: добавление в алфавит новых символов по мере размышлений. Этим допустимо пользоваться, поскольку любой алфавит впоследствии всегда можно перевести (опять же машиной Тьюринга) в двоичный код.

• Иногда возникает затруднение при переходе от алфавита $\{1, 0, *\}$ — к чисто двоичному. Трудность — психологическая. Думается, что кодировать надо лишь звездочку, — и тогда все перемешается. Кодировать надо все. Например,

$$0 \leftrightarrow 00, \quad 1 \leftrightarrow 11, \quad * \leftrightarrow 01.$$

Лента в результате становится «блочной» — ячейки объединяются в пары.

1.10. Рекурсивные функции

Другой подход к вычислимости базируется на иной платформе. Все алгоритмы на детальном уровне, как известно, состоят из элементарных арифметических и логических операций и комбинирования «уже определенного». С учетом возможности перевести кодированием все в числа, возникает надежда определить вычислимые функции с помощью конечного числа операций типа «сложить, умножить».

В результате «проб и ошибок» и стремления к компактности список допустимых операций приобрел следующий вид:

$$o(x) = 0 \qquad (\textit{обнуление}), \tag{1.11}$$

$$\sigma(x) = x + 1 \qquad (\textit{следование}), \tag{1.12}$$

$$\theta_m^n(x_1, \ldots, x_n) = x_m \qquad (\textit{проектирование}), \tag{1.13}$$

наконец, *суперпозиция* [19],

$$\omega(x_1, \ldots, x_n) = \psi[\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_m(x_1, \ldots, x_n)], \tag{1.14}$$

и *примитивная рекурсия*,

$$\begin{cases} f(x, 0) = g(x), \\ f(x, y + 1) = h[x, y, f(x, y)], \end{cases} \tag{1.15}$$

где $x = \{x_1, \ldots, x_n\}$.

1.10.1. Определение. *Функция называется* ***примитивно рекурсивной****, если она может быть получена с помощью операций* (1.11)–(1.15).

Понятно, что примитивно рекурсивные функции перечислимы и всюду определены [20], в силу чего не могут исчерпывать вычислимых функций (теоремы 1.5.1, 1.7.1). Не хватает операции, приводящей к «обязательной» неопределенности функций. В качестве такой операции выбирается ***оператор минимизации***

$$\mu y\{\varphi(x; y) = 0\},$$

дающий наименьшее $y \in \mathbb{N}$, которое удовлетворяет уравнению $\varphi(x; y) = 0$, либо неопределенный, если такое y не существует. Аргумент x, вообще говоря, векторный, $x = \{x_1, \ldots, x_n\}$.

Таким образом, оператор минимизации дает одну из неявных функций $y = f(x)$, удовлетворяющую условию $\varphi[x; f(x)] = 0$.

1.10.2. Определение. *Функция называется* ***частично рекурсивной****, если она может быть получена с помощью операций* (1.11)–(1.15) *и оператора минимизации.*

---

[19] Оператор проектирования (1.13) расширяет возможности суперпозиции, позволяя в (1.14) произвольно варьировать число переменных.

[20] Потому что в их конструкцию входят всюду определенные операции.

Довольно быстро выяснилось, что *частично рекурсивные функции — это в точности вычислимые функции по Тьюрингу*[21].

В одну сторону факт устанавливается совсем просто. Для выполнения каждой операции (1.11)–(1.15) и оператора минимизации, — очевидно, существует машина Тьюринга, чего, собственно, достаточно для вычисления любых частично рекурсивных функций машинами Тьюринга. Чуть больше мороки с обратной импликацией.

Предпринимались многочисленные попытки увеличения списка исходных операций, с тем чтобы расширить множество вычислимых (частично рекурсивных) функций. Безрезультатно. В итоге стала крепнуть уверенность, что «все дороги ведут в Рим». Как ни усложняй определение рекурсивных функций либо конструкцию машин Тьюринга, класс вычислимых функций не меняется.

Другое дело, что класс $\mathscr{R}_0$ примитивно рекурсивных функций может быть расширен, — но это не представляет особого интереса. Примитивно рекурсивные функции — всего лишь ступенька на пути к вычислимым функциям. Ее можно сделать чуть выше, но от этого конечный результат не меняется. Если расширение вести с помощью всюду определенных операций, то недостижимым пределом расширения будет класс $\mathscr{R}$ всюду определенных вычислимых функций (их называют *общерекурсивными*[22]). Причина «недостижимости» — в невозможности эффективной нумерации всюду определенных *вычислимых* функций.

Поэтому

$$\mathscr{R}_0 \subset \mathscr{R}, \quad \text{но} \quad \mathscr{R}_0 \neq \mathscr{R}.$$

Быстро растущая *функция Аккермана* (раздел 1.12) служит примером из области $\mathscr{R}\backslash\mathscr{R}_0$. Но с точки зрения теории вычислимости это ничего не меняет.

Рекурсивные множества. Как при переезде из России в Англию вместо «рыбы» приходится говорить «fish», так и на территории рекурсивных функций «*перечислимые*» множества превращаются

[21] Эквивалентом *тезиса Тьюринга* в теории рекурсивных функций является **тезис Чёрча**: «*Интуитивно алгоритмически вычислимая функция — частично рекурсивна*».

[22] А также эффективно вычислимыми, раздел 1.7.

в «*рекурсивно перечислимые*», а «*разрешимые*» — в «*рекурсивные*». Эта ясность, конечно, достигается не сразу, но в итоге получает строгое обоснование, и на нейтральной территории *разрешимые* и *рекурсивные* множества становятся синонимами, рáвно как *перечислимые* и — *рекурсивно перечислимые*.

Что касается внутренних определений, то они остаются прежними после замены вычислимых функций на частично рекурсивные.

1.11. Диофантовы множества

В 1970 году был получен выдающийся результат, отрицательно решающий 10-*ю проблему Гильберта* о распознавании неразрешимых диофантовых уравнений.

Довольно часто решение трудных проблем, которые десятилетиями не поддавались натиску математического авангарда, — связано с использованием сложного аппарата, что мешает непрофессионалам получить удовольствие. Данный случай — исключение. Кроме того, в процессе «решения» было достигнуто понимание ряда сопутствующих вопросов, оказавшихся значительно более интересными. Если говорить о главном, то была установлена связь «диофантовой тематики» с алгоритмизацией и вычислимостью. Именно этот аспект рассматривается ниже, авансом.

Пусть $p(z_1, \ldots, z_n)$ — полином с целыми коэффициентами [23]. *Диофантовы уравнения*

$$p(z_1, \ldots, z_n) = 0 \tag{1.16}$$

подразумевают решение в целых числах.

Часть переменных в (1.16) выделим в качестве параметров и перепишем уравнение в виде $p(a, x) = 0$, т. е.

$$p(a, x_1, \ldots, x_m) = 0, \tag{1.17}$$

где параметр может быть векторным, $a = \{a_1, \ldots, a_k\}$, причем все a_i и x_j принадлежат натуральному ряду

$$\mathbb{N} = \{1, 2, \ldots\}.$$

[23] Например, $p(z_1, z_2) = z_1^5 - 4z_1z_2^3 + 32$.

1.11.1. Определение. *Множество A положительных векторов*

$$a = \{a_1, \ldots, a_k\}$$

***называется** диофантовым, если при любом $a \in A$ и только при $a \in A$ уравнение* (1.17) *разрешимо в целых положительных $x_1, \ldots, x_m$.*

Требование положительности переменных, вообще говоря, не принципиально и связано с техническими причинами. Отрицательные коэффициенты полинома $p(a, x)$ при этом не исключены, например,

$$p(a, x) = x^2 - ax - 1,$$

$$p(a, x) = x_1^2 - x_1x_2 - a_1x_2 + a_2x_1x_2^7.$$

В тех случаях, когда, имея уравнение $p(a, x) = 0$ неразрешимое в целых положительных числах, необходимо указать уравнение неразрешимое в

$$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\},$$

выручает известная *теорема Лагранжа*: *каждое целое положительное число является суммой четырех квадратов*. Поэтому замена $p(a, x) = 0$ на

$$p(a, 1 + p^2 + q^2 + r^2 + s^2) = 0$$

дает «то что надо». В случае $x = \{x_1, \ldots, x_m\}$ теорема Лагранжа применяется к каждому x_j отдельно.

С виду определение 1.11.1 устанавливает жесткие ограничения, и кажется маловероятным, что диофантовыми будут сколько-нибудь нетривиальные множества. Скажем, множество целых чисел π_n, запись которых совпадает с первыми n разрядами в разложении числа π. Не говоря о «загадочном» множестве простых чисел.

Матиясевич [18], поставивший в решении проблемы последнюю точку, вполне мог бы стать миллионером, предлагая до публикации своих результатов вопрос на пари: «диофантово ли множество простых чисел?» Любой, кто был в теме, ответил бы: «нет». Оказалось же, что

диофантовость множества равносильна перечислимости!

Это был шок. Да еще небольшая переформулировка усиливала эффект. Переформулировка на основе очень простого, но тоже неожиданного результата.

1.11.2. Лемма. *Множество $A \subset \mathbb{N}$ диофантово в том и только том случае, когда оно является множеством положительных значений некоторого полинома $P(x_1, \ldots, x_k)$.*

◄ Действительно, если A — множество положительных значений полинома $P(x_1, \ldots, x_k)$, то уравнение

$$p(a, x_1, \ldots, x_k) = a - P(x_1, \ldots, x_k) = 0$$

определяет A как — диофантово.

Обратно. Пусть A — множество тех a, при которых

$$Q(a, x_1, \ldots, x_l) = 0$$

разрешимо. Тогда A — множество положительных значений полинома

$$a[1 - Q^2(a, x_1, \ldots, x_l)]. \quad ►$$

Таким образом, существует полином, множество положительных значений которого в точности совпадает с множеством простых чисел. Более того, его можно конкретно указать (см. раздел 6.2).

Определенный интерес представляет вопрос о том, насколько сложны полиномы, описывающие нетривиальные множества. Тут можно было бы ожидать астрономических размерностей, но ответ в определенной степени удивителен. Каждый полином (1.17) характеризуется степенью n и числом m переменных x. Для любого диофантова множества A можно указать полином (1.17) с $n \leqslant 4$ (но, возможно, большим m) либо $m \leqslant 9$ (но, может быть, большим n). Чисел n и m порядка двух-трех десятков, как правило, достаточно для самых сложных случаев. Такого порядка n и m достаточно и для записи *универсального полинома* (аналог универсальной машины Тьюринга), генерирующего любое диофантово множество по его номеру.

Если $S_1, S_2, \ldots$ — эффективное перечисление всех перечислимых множеств, то существует (глава 6) *универсальный полином* $U(n, s, x_1, \ldots, x_k)$, перечисляющий все S_n,

$$s \in S_n \Leftrightarrow \exists\,(x_1, \ldots, x_k) : U(n, s, x_1, \ldots, x_k) = 0,$$

причем $U(n, s, x)$ строится конструктивно, поскольку все звенья за кадром конкретно определены.

В эквивалентном варианте: *существует полином* $\widehat{U}(n, x_1, \ldots, x_k)$, *множество положительных значений которого при фиксированном n совпадает с* S_n,

$$s \in S_n \Leftrightarrow \exists\,(x_1, \ldots, x_k) : s = \widehat{U}(n, x_1, \ldots, x_k) \wedge s > 0.$$

При этом имеет место удивительный факт (теорема 6.3.1). *Каков бы ни был полином* $P(z_1, \ldots, z_N)$ *(любой размерности), существует полином*

$$\widehat{U}(x_1, \ldots, x_k)$$

фиксированной размерности k*, множество положительных значений которого в точности совпадает с множеством положительных значений полинома* $P(z_1, \ldots, z_N)$.

На фоне открывающихся перспектив 10-*я проблема Гильберта* как-то отходит на второй план. Ее отрицательное решение дает простой перевод на другой язык факта существования перечислимого, но неразрешимого множества. Последнее означает существование такого полинома $P(x_1, \ldots, x_k)$, что разрешимость уравнения

$$P(x_1, \ldots, x_k) - y = 0 \tag{1.18}$$

по $x_1, \ldots, x_k$ при любом положительном y, — алгоритмически непроверяема.

Если смущает некоторая неопределенность приведенной формулировки, то вот совершенно конкретная недоказуемая арифметическая формула,

$$\exists\, n, y \forall\, x_1, \ldots, x_k : U(n, y, x_1, \ldots, x_k) \neq 0, \tag{1.19}$$

где U конкретный универсальный полином (см. раздел 6.3).

О массовых, или «единых», алгоритмах. В данном случае принято говорить об отсутствии единого алгоритма для распознавания неразрешимых уравнений. При этом, как правило, оговаривается, что в каждом конкретном случае — алгоритм может существовать, из чего аудитория делает оптимистический вывод. Дескать, единообразно нельзя, но специфически — можно.

«Специфически» в самом деле можно, но это выглядит совсем не так, как хотелось бы. Правильный ответ в любой задаче распознавания дает один из двух алгоритмов: первый, независимо от решаемой задачи, все время говорит «да», второй — «нет». И выбраться из этой тривиальности не так просто. Как оставить в поле зрения алгоритмы, «осмысленно решающие задачу», а не угадывающие наобум? Понятно, что такие алгоритмы должны правильно работать не на одной задаче, а на разных однотипных. Здесь и возникают оговорки насчет «единых» алгоритмов, называемых еще

массовыми, что приходится делать в данном случае, если говорить о разрешимости уравнений

$$Q(x_1, \ldots, x_k) = 0.$$

Если же говорить о задаче (1.18), то здесь «единость» заменяется оговоркой «для любого y». Иными словами, отрицательное решение десятой проблемы Гильберта получилось сильнее, чем можно было бы ожидать. Не существует единого алгоритма даже для однопараметрического семейства полиномов (1.18). В записи (1.19) это выглядит еще более конкретно.

Что касается связи с *вычислимыми функциями* $y = f(x)$, то *это функции*, *график которых* (*множество*)

$$G = \{x_1, \ldots, x_n,\ y = f(x_1, \ldots, x_n)\},$$

диофантов.

Таким образом, диофантовы уравнения оказываются еще одним вариантом (языком) изучения вычислимости. В каком-то смысле — эквивалентным, в каком-то — более эффективным, в каком-то — менее. Большинство исследований в рассматриваемой области традиционно опирается на машины Тьюринга или на рекурсивные функции. В том и другом случае процесс вычислений — «не дан в ощущениях». Здесь же вычисляются значения обыкновенного полинома, который можно «потрогать». Для некоторых задач это может быть существенно. По крайней мере, к знаменитым *теоремам Гёделя* обеспечивается весьма наглядный путь (раздел 2.1). В любом случае стоит обратить внимание, что «целочисленные» полиномы и диофантовы множества стали полноправными участниками событий, разворачивающихся вокруг вычислимости.

1.12. Комментарии и дополнения

- Функцию (1.4) интересно сопоставить с

$$g(n) = \begin{cases} 1, & \textit{если существует целое } \boldsymbol{k}, \textit{ квадрат которого} \\ & \textit{содержит ровно } \boldsymbol{n} \textit{ идущих подряд семерок}; \\ 0, & \textit{в противном случае}, \end{cases}$$

которая вычислима, поскольку $g(n) \equiv 1$.

Доказательство легко выводится из следующего факта.

1.12.1. Теорема Кронекера. *Для произвольного иррационального числа α и любых x, y $(x < y)$ всегда можно указать целые m и n такие, что*[24]

$$x < m\alpha - n < y. \tag{1.20}$$

◀ Считаем $|x - y| < 1$ — в противном случае x и y можно сблизить, ужесточив требование (1.20), — и $(x, y) \subset (0, 1)$ — иначе для близких x, y (имеющих одинаковые целые части) условию (1.20) можно удовлетворить, меняя n.

Разобьем далее $(0, 1)$ на достаточно большое число равных по длине интервалов $\Delta_1 \ldots, \Delta_N$ так, чтобы какой-то интервал Δ_j попал целиком в промежуток (x, y). Среди $\{m\alpha - n\}$ при всевозможных m и n (где *фигурные скобки обозначают дробную часть числа*) найдутся

$$m_1\alpha - n_1 \quad \text{и} \quad m_2\alpha - n_2 \qquad (m_1 \neq m_2),$$

попадающие в один и тот же интервал Δ_k. Поэтому[25]

$$\gamma = (m_1 - m_2)\alpha - (n_1 - n_2) \in \Delta_1 \Rightarrow j\gamma \in \Delta_j \subset (x, y). \quad ▶$$

◀ Покажем теперь, что всегда существует квадрат целого числа, десятичная запись которого начинается с любой наперед заданной последовательности цифр $A = a_1, \ldots, a_N$. Это означает, что найдутся такие целые k и p, что

$$A \cdot 10^p < k^2 < (A + 1) \cdot 10^p.$$

После логарифмирования неравенство переходит в

$$\lg A < 2 \lg k - p < \lg (A + 1).$$

Полагая $k = 2^m$, $p = 2q$, получаем

$$\lg A < 2m \lg 2 - 2q < \lg (A + 1).$$

Далее остается сослаться на теорему Кронекера. ▶

• Только что проведенное доказательство дает пример использования неарифметической идеологии (иррациональные числа, логарифмы). Однако внешняя картина не гарантирует опоры на что-нибудь существенное за пределами арифметики. Внешние атрибуты могут проектироваться внутрь чисто арифметической системы аксиом, а могут и не проектироваться. Решение такой дилеммы бывает весьма сложным.

• В последнее время некоторое распространение при изучении вычислимых функций получили *машины с неограниченными регистрами* (МНР). МНР-машины по большому счету не так уж сильно отличаются от машин Тьюринга. Та же лента. Ячейки, правда, называются регистрами, в которые можно записывать не одну

[24] Иными словами, множество $m\alpha - n$ $(m, n \in \mathbb{Z})$ плотно на вещественной прямой при любом иррациональном α.

[25] Равенство $(m_1 - m_2)\alpha - (n_1 - n_2) = 0$ невозможно в силу иррациональности α и $m \neq n$.

букву, а любое число. Что касается действий самой машины, то ситуация нагляднее. МНР выполняет всего четыре типа команд: *обнуления*, *прибавления единицы*, *переадресации* (перенос содержимого из одного регистра в другой) и *условного перехода* (переход к выполнению команды не в порядке очереди, вернее, записи). Программа вычислений,

$$P = C_1 C_2 \dots C_n,$$

представляет собой последовательность команд C_j указанных типов, но надо иметь в виду, что команды имеют параметры (номера регистров).

Получается универсальный счетный прибор[26], действия которого относительно легко поддаются интерпретации, в то время как внутренняя кухня машины Тьюринга сильно запутана, хотя внешне копируется поведение человека, решающего задачу (последовательное чтение и запись символов на фоне изменения внутреннего состояния). Однако загадочность ментального процесса не становится обозримее при его переводе на механический язык.

• Соответствие МНР канонам обыденного мышления в свое время вызвало вздох облегчения. Но освободиться от гипнотических чар Тьюринга еще проще, не мудрствуя. Чем МНР лучше обыкновенного компьютера? Безусловно, проще и обозримее, но для теории вычислимости это уже не так важно. Важен сам факт существования конечного описания алгоритма. Если до определенных пор такая формулировка была размыта, то теперь есть возможность сослаться на любой универсальный язык программирования. Эквивалентной заменой машине Тьюринга может служить программа вычислений, скажем, на фортране или бейсике. Все что требуется в плане конкретности и однозначности — обеспечено. Зацикливание и зависание — беда общая. Таким образом, за упоминанием алгоритма сегодня можно подразумевать программу на каком-либо универсальном алгоритмическом языке.

• **Функция Аккермана**

$$A(n) = B(n, n),$$

где B определяется соотношениями[27]

$$\begin{aligned} B(x+1, z+1) &= B[x, B(x+1, z)], \\ B(0, z) &= 2 + z, \\ B(x+1, 0) &= \theta(x), \end{aligned}$$

приобрела известность благодаря превосходству в скорости роста над любой примитивно рекурсивной функцией, откуда будто бы стало ясно, что класс примитивно рекурсивных функций не исчерпывает всюду определенных вычислимых функций. Но это и так ясно (теорема 1.7.1). Поэтому анализ скорости роста здесь больше имеет олимпиадно-развлекательный уклон — подробности есть в [13].

---

[26] Равный по возможностям универсальной машине Тьюринга.

[27] Здесь $\theta(x)$ — «ступенька»: $\theta(0) = 0$, $\theta(x > 0) = 1$.

Существенно больший интерес представляет *двойная рекурсия* построения функции B. Хотя, казалось бы, что здесь может быть интересного? Значения $B(x, z)$ определяются через «предыдущие». Но в том-то и дело, что «предыдущие» не случайно взяты в кавычки, потому что конкретные вычисления вынуждены странно блуждать по аргументам, не обнаруживая признаков упорядоченности. Для определения $B(3, 2)$, например, приходится вычислять по ходу дела $B(2, 4)$, а вычисление $B(3, 4)$ проходит через $B(2, 16)$. И с ростом аргументов в $B(x, z)$ «забегание вперед» становится все больше. На каком-то этапе пробных попыток возникает подозрение, что петля вычислений может вообще не замыкаться, ставя крест на двойной рекурсии как эффективной процедуре.

Подозрения не оправдываются, но разбор ситуации требует определенных усилий.

• **Теорема**[28]. *Любая общерекурсивная функция (одноместная) может быть получена из функций*

$$\sigma(x) = x + 1 \quad и \quad \zeta(x) = x - [\sqrt{x}]^2$$

с помощью конечного числа сложений, суперпозиций и всюду определенных обращений одноместных функций.

[28] *Robinson J.* General recursive functions // Proc. Amer. Math. Soc. 1950. **1**. 703–718.

Глава 2

Неполнота арифметики

2.1. Теоремы Гёделя

Проблема доказуемости с высоты птичьего полета выглядит следующим образом. Заданы аксиомы и правила вывода теорем. При конечном и даже счетном числе аксиом и правил — из отправных точек к теоремам ведут цепочки «рассуждений», именуемые доказательствами. Поскольку любое доказательство конечно, — все они, а значит, и теоремы — могут быть эффективно пересчитаны, т. е. алгоритмически пронумерованы.

> *Возможность алгоритмического перечисления множества всех теорем не исключает в рамках рассматриваемой теории других «истин», которые можно называть недоказуемыми теоремами или как-нибудь еще, в зависимости от договоренности.*

В механизмах регламентации правил вывода есть, конечно, тонкости и нюансы (см. главы 4, 5). Но они для рассматриваемой в данном разделе проблематики не играют *никакой* роли. Единственное, что важно, принципиальное наличие алгоритма перебора доказательств, т. е. теорем. И ни *гёделизация*, ни скрупулезное описание логической подоплеки не добавляют к сказанному ничего существенного.

Другое дело, что всегда находится сомневающаяся часть аудитории, играющая очень важную роль в устройстве Вселенной, но сильно мешающая какому-либо движению. Для нейтрализации обременительного недоверия обычно пишется сотня-другая страниц текста с перечислением правильных, но не меняющих сути формул, что вводит аудиторию в транс и создает иллюзию наличия ответов на все вопросы.

Перейдем теперь к главному. *Теоремы Гёделя* в свободной формулировке звучат так:

• *Какова бы ни была совокупность аксиом, в арифметике, если она непротиворечива, существует такое утверждение A, что ни A, ни его отрицание $(\neg A)$ — не доказуемы.*

• *Если непротиворечивая теория T содержит в себе арифметику, то непротиворечивость T недоказуема в T.*

Сначала о понятии непротиворечивости. *Теория T* называется *непротиворечивой*, если в T не могут быть доказаны две противоположные формулы [1] (теоремы): A и «не A» (что обозначают как $\neg A$). Для ближайших целей под *теорией* достаточно понимать аксиоматику плюс правила вывода, плюс доказуемые формулы. В главе 5 есть уточнения, но сути дела они не меняют.

Приведем вариант *первой теоремы Гёделя о неполноте*, в некотором роде усиливающий классический результат.

2.1.1. Теорема. *Какова бы ни была непротиворечивая теория, содержащая арифметику, существует не имеющий положительных корней полином $Q(x_1, \ldots, x_k)$, отсутствие у которого целых положительных корней недоказуемо.*

◄ *Доказательство.* Пусть алгоритм $\mathscr{A}_1$ перечисляет разрешимые уравнения $P(x_1, \ldots, x_k) = 0$. Неперечисленными остаются утверждения

$$\forall\, x_1, \ldots, x_k : P(x_1, \ldots, x_k) \neq 0. \tag{2.1}$$

Если допустить, что при некоторой непротиворечивой системе аксиом все факты вида (2.1) доказуемы, это будет означать существование алгоритма $\mathscr{A}_2$, перечисляющего теоремы (2.1) [2], т. е. перечисляющего дополнение к множеству $\mathbb{P}$ полиномов, перечисляемых алгоритмом $\mathscr{A}_1$. Отсюда по теореме 1.6.3 будет следовать разрешимость множества $\mathbb{P}$, что вступает в противоречие с отрицательным решением *десятой проблемы Гильберта*. ►

Заметим, что в случае противоречивой системы аксиом, алгоритм $\mathscr{A}_2$ пересекался бы с $\mathscr{A}_1$, и отделить полиномы (2.1) не удалось бы. В то же время требование непротиворечивости в какой-то мере обесценивает результат. Накал противостояния частично снимает дальнейшее усиление теоремы 2.1.1.

---

[1] Такое определение позволяет избежать проблематичного понятия истины.

[2] Алгоритм $\mathscr{A}_2$ перечисляет те самые цепочки доказательств, о которых говорилось выше.

2.1.2. Теорема. *Существует полином* $P(x) = P(x_1, \ldots, x_k)$ *такой, что высказывание*:

«уравнение $P(x) - y = 0$ *неразрешимо по* x *при некоторых* y*»*	(2.2)

истинно, но недоказуемо ни в какой непротиворечивой системе аксиом, включающей ***примитивную*** *арифметику.*

Примитивной арифметикой L_0 мы называем систему, опирающуюся на *диофантов язык* $L_0 = \{+, \times, =, \exists\}$, подробно рассматриваемый в главах 5 и 6. Отрицание, импликация, квантор общности — исключены. И, главное, в L_0 исключена *математическая индукция* — острие *арифметики Пеано*[3] Z. В L_0 ничего нельзя доказать, можно только проверить разрешимость полиномиального уравнения (перебором). Иначе говоря, все верные утверждения $\exists\, x : P(x) = 0$, и только они, в L_0 доказываются. В этом смысле примитивная арифметика непротиворечива.

Всю тяжесть доказательства теоремы 2.1.2 берет на себя истинность (2.2), устанавливаемая в теории диофантовых множеств. Невозможность обойти преграду с помощью какой-нибудь непротиворечивой аксиоматики очевидна. Была бы подходящая аксиоматика, существовал бы алгоритм, ибо в совокупности всех алгоритмов есть алгоритмы, реализующие поиск при любой мыслимой системе аксиом. Система аксиом еще не оговорена, не придумана, — а в списке алгоритмов уже есть соответствующая программа[4]. Поэтому, с натяжкой говоря:

> *Все, что может быть в принципе доказано, — алгоритмически разыскиваемо. Все, что алгоритмически «не обнаруживаемо» — не может быть доказано никогда.*

Заметим, что в теореме 2.1.2 высказывание (2.2) с дополнительным утверждением существования подходящего полинома P можно заменить формулой (1.19), т. е.

$$\exists\, n, y \forall\, x_1, \ldots, x_k : U(n, y, x_1, \ldots, x_k) \neq 0,$$

где U конкретный универсальный полином.

---

[3] Именно арифметику Пеано обычно имеют в виду, когда говорят просто об арифметике — см. главу 8.

[4] Также как в списке всевозможных текстов есть все еще ненаписанные романы.

2.2. Неформализуемость истины

Над понятием *истины* полезно задуматься до изучения логики.

Будем, для определенности, говорить пока о двух типах формул в арифметике:

$$\exists\, \boldsymbol{x} : P(\boldsymbol{x}) = 0 \quad \text{и} \quad \forall\, \boldsymbol{x} : P(\boldsymbol{x}) \neq 0,$$

где $\boldsymbol{x} = \{x_1, \ldots, x_n\}$.

Понятно, что в арифметике L_0 формула $\forall\, \boldsymbol{x} : P(\boldsymbol{x}) \neq 0$ — если правильна — непроверяема в принципе, а $\exists\, \boldsymbol{x} : P(\boldsymbol{x}) = 0$ можно проверить, но только в случае, если $P(\boldsymbol{x}) = 0$ имеет решение [5].

Как в этой ситуации на множестве уравнений $\boxed{P(\boldsymbol{x}) = 0}$ ввести понятие *истины*? При наличии единственного надежного инструмента (перебора) возможность одна: если находится корень, то $\exists\, \boldsymbol{x} : P(\boldsymbol{x}) = 0$ *истинно*, $\forall\, \boldsymbol{x} : P(\boldsymbol{x}) \neq 0$ — *ложно*. *Истинные* утверждения [6] $\forall\, \boldsymbol{x} : P(\boldsymbol{x}) \neq 0$ — «истинные» с точки зрения *Всевидящего Ока* — остаются вне закона.

В *арифметике Пеано* Z есть дополнительные, хотя и менее надежные инструменты: *математическая индукция и правила логического вывода*, с помощью которых часть формул $\forall\, \boldsymbol{x} : P(\boldsymbol{x}) \neq 0$ получают доказательства и могут быть помечены как истинные. Но эта истина все же «второго сорта», потому что *непротиворечивость* средств доказательства не имеет обоснования, кроме интуитивного (см. раздел 2.3).

Тем не менее истины «второго сорта» тоже приходится считать истинами, иначе математика превращается в малоинтересную игру. Причем, если «проверка» квалифицируется как доказательство, то *истиной становится, по определению, все доказуемое, и ничто другое.* Но возникает соблазн оставить *Всевидящее Око* хотя бы в качестве виртуального инструмента, и тогда терминология временами размывается, порождая парадоксов немного больше, чем предусмотрено Создателем.

---

[5] Тогда $\boldsymbol{x}$ гарантированно находится перебором.

[6] Ра́вно как и ложные $\exists\, \boldsymbol{x} : P(\boldsymbol{x}) = 0$, что по сути — одно и то же. Такая оговорка далее везде опускается.

На пути удобного определения истины стоят две преграды: *теоремы Гёделя о неполноте арифметики*. Строгие рамки «истинно то и только то, что имеет доказательство» — не позволяют в достаточно сложных теориях [7] определить истинность всех утверждений [8].

2.3. Непротиворечивость

Непротиворечивость в какой-то степени менее острый вопрос, хотя — «кому как». Одних успокаивает интуиция «здравого смысла», другим не дает покоя *вторая теорема Гёделя*:

2.3.1. Теорема о непротиворечивости [9]. *Если теория T непротиворечива и содержит в себе арифметику, то непротиворечивость T недоказуема в T.*

Разумеется, теорема 2.3.1 не исключает возможности решения проблемы за счет привлечения дополнительных средств (аксиом), и такого сорта утверждения о непротиворечивости арифметики получены, например, *Генценом*. Но гарантировать непротиворечивость *расширенной аксиоматики* опять-таки нельзя в силу теоремы 2.3.1, и необходим следующий акт расширения. Путь ведет в «никуда», и в этом смысле *проблема непротиворечивости* не имеет абсолютного решения.

Тем не менее «усеченные» обоснования непротиворечивости заслуживают определенных реверансов, поскольку, несмотря на изъяны, проясняют ситуацию. Обыкновенная констатация невозможности абсолютного решения не дает ощущения края и представления о глубине пропасти. Расширение аксиоматики показывает ту «малость», которая нужна, чтобы концы сошлись с концами.

Есть еще один аспект, который удобно рассмотреть, пока «шум инструментов» не мешает слышать мелодию.

Как происходит формирование системы аксиом? Отталкиваясь от любой стартовой совокупности, можно утверждать существова-

[7] Критерием «сложности» служит наличие внутри теории — арифметики.

[8] За некоторыми исключениями, к каковым относятся в основном теории, имеющие дело с конечными множествами объектов.

[9] Доказательство в разделе 2.7.

ние недоказуемой истины [10]

$$\forall x > 0 : P(x) \neq 0. \tag{2.3}$$

Но конкретно указать $P(x)$ принципиально нельзя, иначе возникает противоречие [11] с недоказуемостью (2.3). Поэтому у нас могут быть лишь подозрения об истинности утверждений типа (2.3). Присовокупляя их к аксиомам, мы получаем «подозрительную» систему, сидя внутри которой, ничего не можем сказать об истинности фундамента. Разумеется, если аксиомы действительно истинны, но об этом не знает даже Бог. Если же в основании пороховая бочка, — остается ждать, когда «заискрит».

2.4. Неразрешимые уравнения

Для простоты речи в случае неразрешимости диофантова уравнения

$$P(x) = 0, \quad x = \{x_1, \ldots, x_n\},$$

будем говорить о *неразрешимости полинома* $P(x)$.

Пониманию рассматриваемой проблематики в значительной мере способствует «переформулировка» теоремы 2.1.1.

2.4.1. Теорема. *Множество* $\mathcal{P}$ *неразрешимых полиномов* $P(x)$ — *неперечислимо* (*тем более неразрешимо*) [12].

◄ Еще раз. В предположении противного и при учете перечислимости разрешимых полиномов [13], множество $\mathcal{P}$ оказалось бы разрешимо, что гарантировало бы существование распознающего алгоритма, вразрез с отрицательным решением *десятой проблемы Гильберта*. ►

При таком изложении всю сложность обоснования, разумеется, принимает на себя доказательство эквивалентности понятий диофантова и перечислимого множества (см. главы 5, 6). Но сама

[10] Поскольку теория T содержит, по предположению, арифметику, можно говорить о полиномах.

[11] Доказательство неразрешимости (2.3) равносильно доказательству справедливости (2.3).

[12] Необходимо обратить внимание на иерархию: *неразрешимое множество неразрешимых полиномов*.

[13] Перечисление разрешимых полиномов обеспечивает обыкновенный перебор.

по себе теорема 2.4.1 выглядит экспонатом из несколько иного окружения, и будь она доказана независимо — *теоремы Гёделя* (рáвно как и решение *десятой проблемы Гильберта*) вытекали бы из нее совсем просто. Не говоря о дополнительной прозрачности результатов. Например, из сказанного в предыдущем разделе может возникнуть впечатление о неком несоответствии. С одной стороны, утверждается существование *неразрешимых полиномов*, с другой, — такие полиномы (2.3) можно добавить в аксиоматику.

Выход из противоречия дает как раз *неперечислимость* множества $\mathcal{P}$. Включение в аксиоматику любого перечислимого (даже бесконечного) подмножества $\widetilde{\mathcal{P}} \subset \mathcal{P}$ — оставляет непустым множество $\mathcal{P}\backslash\widetilde{\mathcal{P}}$ неразрешимых полиномов. Это указывает на справедливость следующего факта.

2.4.2. Теорема. *Арифметика неаксиоматизируема, даже при включении в систему бесконечного, но конструктивно (перечислимо) задаваемого множества аксиом.*

Интересно, что вместо «$\forall\, x > 0 : P(x) \neq 0$» с неразрешимым полиномом в аксиоматику может быть добавлено противоположное утверждение «$\exists\, x > 0 : P(x) = 0$», причем *без ущерба для арифметики*. Как бы дико это ни казалось, но опровергнуть декларацию разрешимости неразрешимого полинома — невозможно[14]. Разумеется, ни о каком *конкретном* полиноме этого сказать нельзя, но такой полином существует. Поэтому — можно угадать (но нельзя гарантировать, что догадка правильна).

Сказанное дает основание для формулировки следующего результата.

2.4.3. Теорема. *Существуют системы аксиом, «порочность» которых принципиально нельзя обнаружить.*

«Порочность» здесь употреблена по той простой причине, что «противоречивость» уже занята конкретной формулировкой (нельзя доказать A и $\neg A$). Если же под непротиворечивостью понимать недоказуемость ложного утверждения[15], то теорема 2.4.3 как раз

[14] Иначе это было бы обоснованием недоказуемого «$\forall\, x > 0 : P(x) \neq 0$».

[15] Что было бы логичнее, но совершенный индикатор ложности в этом мире не предусмотрен.

решает этот вопрос, причем абсолютно — не оставляя надежды. Другое дело, что о подобной непротиворечивости беспокоиться бессмысленно.

(!) Замечание. Возможность добавить в аксиоматику как утверждение о неразрешимости $P(x)$, так и его отрицание, — может натолкнуть на мысль, что решение знаменитой *гипотезы континуума* (глава 8) имеет тот же корень. Это не совсем так. Полином, который «подходит» как для предположения о его разрешимости, так и неразрешимости, — принципиально нельзя указать, несмотря на его существование. В противном случае возникало бы противоречие. Подходящий полином может быть только неразрешимым, и тогда «$\exists\, x : P(x) = 0$» — заведомо ложно.

Гипотеза же континуума оказалась *конкретным* утверждением, которое можно добавлять к аксиоматике теории множеств, рáвно как и его отрицание. В этом, собственно, и заключалась «неожиданность» решения. В то же время надо признать что соответствующим аналогом в арифметике может служить утверждение (2.2).

2.5. Об арифметических истинах

Полиномы в обосновании теоремы Гёделя дают ощущение психологического комфорта, но их можно заменить вычислимыми функциями, что позволяет получить доказательство без ссылки на диофантовость перечислимых множеств. Вот соответствующее рассуждение.

◀ *Множество S значений вычислимой функции*[16] *$f(x)$ разрешимо, если существует алгоритм, определяющий по любому $y \in \mathbb{N}$, имеет решение уравнение $f(x) = y$ или нет.*

Из существования перечислимого, но неразрешимого множества (теорема 1.6.4) вытекает, что последняя задача при некоторой функции $f(x)$ — алгоритмически неразрешима. Это означает ***недоказуемость*** *разрешимости уравнения $f(x) = y$ при некоторых y (при которых уравнение разрешимо). В противном случае существовал бы алгоритм, распознающий неразрешимые уравнения $f(x) = y$.* ▶

Здесь, собственно, раскручивается та же спираль с заменой полиномов вычислимыми функциями, и не очень ясно, чем это хуже. Строго говоря, ничем. Но уравнение $f(x) = y$ вместо $P(x) = y$ — в значительной степени размывает предмет.

[16] Перечислимое по определению.

Во-первых, под $f(x)$ здесь надо понимать не функцию, а вычислительную программу, если оставаться пока в избранных рамках. В этом, конечно, нет ничего страшного, поскольку ясно, что утверждение $\forall x : f(x) \neq y$ имеет арифметический характер [17]. Но это как-то неуклюже, а если хочется перейти от алгоритмов к функциям, то это длинная песня, связанная с регламентацией языка и привлечением математической логики. Такой путь не очень короток [18].

Во-вторых, имея дело с программами, приходится допускать, что алгоритм в процессе счета может положить $2 = 3$. И что толку тогда говорить о неразрешимости $f(x) = y$, если в $f(x)$ заложено неправильное в арифметике равенство? Оказывается, есть толк. Алгоритм не утверждает «$2 = 3$», а механически заменяет двойку тройкой, — что вполне «арифметично», т. е. допустимо при описании нормальной функции $f(x)$. Но чисто психологически это все же вызывает опасения, что при такой неразберихе истина перепутывается с ложью, и для обретения душевного равновесия требуется все перерисовать в каком-либо виде, удобном для интуиции.

Таким образом, вычислимые функции вместо полиномов — дают больше поводов для разговоров, что иногда скрашивает досуг. В этом — вся разница.

Напомним в заключение, что существование недоказуемого утверждения «$\exists y \forall x : f(x) \neq y$» при алгоритмической неразрешимости имеет абсолютный характер в смысле независимости от принятой системы аксиом. Система аксиом лишь выделяет «законные» алгоритмы и отсеивает «незаконные». Здесь же утверждается неразрешимость при любых мыслимых алгоритмах.

2.6. Можно ли помочь арифметике извне?

Нельзя, — если говорить о ликвидации неразрешимостей. Хотя в литературе встречается мнение, что точки опоры могут найтись вне арифметики [19].

---

[17] На самом деле не так уж ясно. По поводу арифметичности вычислимых функций см. главы 5, 6.

[18] Зато, благодаря утомительности, снимает напряжение у недоверчивой части населения.

[19] К таким заключениям обычно подталкивают неверно понимаемые результаты Генцена о непротиворечивости арифметики, см. главу 8.

Конечно, аппарат других дисциплин часто оказывается полезен в решении конкретных арифметических задач, привлекая в качестве инструментов всякую эквилибристику вплоть до топологической. При этом не всегда ясно, привлекаются ли по сути новые гипотезы или же все опосредованно сводится к удобствам, не выводящим за пределы обычной идеологии.

Использует ли, скажем, доказательство последней *теоремы Ферма* что-либо не принятое до сих пор в классической теории чисел? Внешне — использует. А по сути? Никто пока всерьез таким вопросом не занимался. Но если предположить наличие в решении фундаментально новых моментов, что это может означать для арифметики?

Вообще говоря, целесообразность принятия дополнительных аксиом, которые могут оказаться полезны для решения каких-то теоретико-числовых задач. Однако никакие извне прибывшие рецепты не могут повлиять на существование в арифметике недоказуемых истин. Если все рецептурно осмысленное — программируемо, любые «внешние» аксиомы и правила после кодирования проецируются в арифметику, и не могут расширить круг вычислимых функций. В этом смысле арифметика сильнее любых фантазий в рамках алгоритмической догматики.

2.7. Доказательство второй теоремы Гёделя

Сначала опишем конструкцию, на которую можно «повесить» многие доказательства.

Пусть $S_1, S_2, \ldots$ — эффективное перечисление всех перечислимых множеств. Диагональное множество D образуется из тех номеров n, которые принадлежат S_n, — и оказывается неразрешимым [20].

Далее просматриваем перечень $\{P_k\}$ всех доказательств в арифметике, пока не встретится доказательство либо формулы $\{n \in D\}$, либо $\{n \notin D\}$. В первом случае в конструируемое множество $\mathbf{S}$ вносим *фантом* n^*, во втором — число n. *Фантом* n^* не является элементом $\mathbf{S}$, его роль заключается в том, что при *последующем* по-

[20] См. доказательство теоремы 1.6.4.

явлении доказательства $\{n \notin D\}$ (в случае противоречивости системы) число n не включается в $\mathbf{S}$. Механизм эффективен (дает перечисление элементов из $\mathbb{N}$), и потому $\boxed{\mathbf{S} = S_r}$ при некотором r. Разумеется, по построению S_r лежит в дополнении D, но где лежит r?

Высказывание (формула) $\mathbf{A} = \{r \in D\}$ запускает «карусель», выход из которой в различных точках порождает разные теоремы. Работает это, например, так.

◀ Если **A** доказуемо, то это означает, что $\{r \notin D\}$ в списке $\{P_k\}$ встречается первым, — откуда получается $\{r \notin D\}$. С другой стороны, если **A** доказуемо — то $r \in D$. Противоречие.

Если же «не **A**» доказуемо, — то $\{r \notin D\}$, с одной стороны, и $\{r \in D\}$ — с другой. Опять противоречие. В условиях непротиворечивой аксиоматики выход один. Ни **A**, ни «не **A**» — доказаны быть не могут, что еще раз дает обоснование *первой теоремы Гёделя*. ▶

Далее сценарий сталкивается с *видимостью парадокса*. Незначительная перестановка декораций ведет к другому результату.

◀ Если $r \in D$, то из непротиворечивости арифметики следует $r \notin D$. С другой стороны, условие $r \in D$ эффективно, т. е. доказуемо проверяется. Но тогда (по схеме предыдущего доказательства) $r \notin D$, следовательно, **A** ложно. В результате «не **A**» доказано. ▶

Итак, ни **A**, ни «не **A**» — доказаны быть не могут, но проведенное рассуждение доказывает «не **A**». Возникает второй круг противоречий, уже между теоремами. Сказать, что это *не парадокс*, а — *видимость*, гораздо легче, чем осознать ситуацию. И как принято считать, это самый тонкий момент во всей теории.

◀ «Тонкость» заключается в том, что данное доказательство является **метатеоретическим**. Имеет *надарифметический* характер и не принадлежит списку $\{P_k\}$. В узаконенные рамки не укладывается ссылка в первом предложении на непротиворечивость арифметики. Если последняя имела бы *синтаксический вывод* внутри Z, то данное метадоказательство проектировалось бы в Z и приводило бы к настоящему противоречию. Поэтому непротиворечивость Z не может быть доказана в Z. ▶

Теперь, когда видна конструкция в целом, можно уточнить некоторые детали. Сомнения иногда вызывают манипуляции с перечислимыми множествами. На самом деле всякое бесконечное

множество, если перечислимо, имеет конечное описание (раздел 1.6), и все можно было бы переписать с помощью вычислимых функций, причем конструктивно определяемых. Более того, даже число r конкретно определяемо. Что касается возможных сомнений в арифметичности вычислимых функций, то они (сомнения) развеиваются в разделе 5.10 (теорема 5.10.4).

Несколько странной может показаться возможность указания r. Особенно на фоне разговоров о существовании неразрешимого полинома, который невозможно указать. Дело в том, что конкретно указуема (раздел 1.11) формула, имеющая дело с семейством полиномов:

$$\exists\, y \forall\, x_1, \ldots, x_k : \{P(x_1, \ldots, x_k) - y \neq 0\}.$$

Заслуживает внимания еще один момент. Арифметику Z везде в рассуждениях можно заменить «непротиворечивой» теорией T, содержащей Z. Наличие Z в T необходимо по той причине, что техника используемых манипуляций опирается на нумерации и другие механизмы арифметических вычислений.

2.8. Лингвистические парадоксы

Лингвистические парадоксы типа «заключенное в кавычки — есть ложь» уже порядком надоели. В ту же категорию попадают аналогичные фокусы в математической аранжировке, потому что везде фигурирует одна наскучившая причина: «самообращение» понятий и языков.

Для теории алгоритмов это плохо тем, что контуры совершенно нормальных математических доказательств ассоциируются с классическими рассуждениями *брадобрея*[21]. Дискредитировавшая себя область отбрасывает тень, и возникает червоточинка в связи с арифметическими неразрешимостями. Исподволь думается, не такая ли чепуха лежит в основе знаменитых теорем.

Не такая. Математика в своих основаниях действительно проходит вблизи тривиальных противоречий, но минует их, и по тем же выкройкам создает абсолютно логичные конструкции. Можно сказать и по-другому. Лингвистическое разоблачение *парадокса лжеца*

[21] Приказано: брить тех, кто не бреется сам. Как теперь брить самого себя?

убивает парадокс. Математика же умудряется рассмотреть и сохранить *непротиворечивое ядро*, проецируя которое на игровое поле арифметики, получает эффективный *механизм диагональных рассуждений.*

Представление о *диагональном методе* и владение им — разные вещи. Сопутствующие обстоятельства меняют облик. Поэтому знакомство с возможно бóльшим числом разнородных примеров имеет смысл. Вот еще одно (уже четвертое) доказательство *первой теоремы Гёделя* из той же категории.

◄ Пусть $\{A_n(x)\}$ перечисление всех формул в непротиворечивой теории T с одной свободной переменной x, а $B(n)$ высказывание (формула) о *недоказуемости* $A_n(n)$. Причем $B(n)$ может быть как истинным, так и ложным.

Поскольку мы хотим оставаться внутри T, то $B(n)$ формула из T, и с неизбежностью $B(n) = A_r(n)$ при некотором r. Рассмотрим высказывание

$$B(r) = A_r(r). \tag{2.4}$$

Если $B(r)$ доказуемо, то $A_r(r)$ вместе с $B(r)$, в силу (2.4), — недоказуемо. Противоречие. Если же отрицание $\neg B(r)$ доказуемо, то $A_r(r)$, вместе с $B(r)$, доказуемо. Снова противоречие. Остается предположить либо противоречивость аксиоматики, либо недоказуемость $\neg B(r)$ и $B(r)$. ►

Некоторый дискомфорт в связи с рассмотрением утверждений типа $B(n)$ естествен, но необоснован. Широко распространенные ощущения, что самоссылки, самореферирование и прочие уловки самообращения могут выводить за пределы рассматриваемой области — проистекают как раз из опыта знакомства с наивными парадоксами. В теории алгоритмов все перечислимые множества упорядочиваются, $S_1, S_2, \ldots$, затем образуется диагональное множество $D = \{n : n \in S_n\}$, — и все это обеспечивается *конечным механизмом*, который никуда «не выводит», $D = S_r$ при некотором r.

Парадокс заключенного. Приговор гласил: «Казнить в течение недели. День казни должен быть неожиданным для приговоренного». Заключенный рассудил так. В последний день недели казнить не могут — не будет неожиданно. Но тогда предпоследний день становится последним из возможных, и его надо исключить по той же причине. И так вплоть до понедельника. Поэтому — не казнят. Умение рассуждать успокоило беднягу.

В среду *неожиданно* пришли — и казнили.

Глава 3

Универсальные функции и нумерации

3.1. Универсальные функции

В главе 1 уже шла речь об универсальной машине Тьюринга. С тем же успехом можно говорить об универсальной вычислимой функции, а также об универсальном перечислимом множестве. За кадром здесь стоит возможность эффективной нумерации вычислимых функций,

$$f_1(x), \ldots, f_n(x), \ldots, \tag{3.1}$$

которая позволяет считать двуместную функцию

$$U(n, x) = f_n(x)$$

универсальной.

В обычном анализе операция поднятия индекса в аргумент не требует обоснования, являясь вопросом орфографии. В данном случае ситуация иная. Поднятие индекса означает, что функция $U(n, x)$ *вычислима* в рамках той же самой идеологии. Другими словами, что нумерация (3.1) осуществима программой на фортране (рекурсивной функцией, машиной Тьюринга), т. е. теми же средствами, которые вычисляют сами функции $f_n(x)$.

Далее *подразумевается нумерация программ вычисления — по их длине*, выполнимая, очевидно, любыми средствами из перечисленных. От ощущения тривиальности можно избавиться, рассмотрев *диофантовы множества* как множества положительных значений полиномов. Полиномы с целыми коэффициентами легко упорядочиваются, $P_1(x), P_2(x), \ldots$, но индекс «некуда» поднимать. Функция

$$Q(n, x) = P_n(x)$$

— не полином, и требуется довольно хитрая эквилибристика, чтобы ситуацию «вернуть в русло».

Способов нумерации программ — бесконечно много. Поэтому универсальных функций тоже бесконечно много.

3.1.1. Определение. *Нумерация и функция $U(n, x)$ называются **гёделевскими**, если существует всюду определенная вычислимая функция $s(n)$ такая, что для любой двуместной функции $f(n, x)$ справедливо*

$$f(n, x) = U(s(n), x).$$

◀ В рассматриваемой области понимать определения сложнее (до приобретения навыков), чем доказательства теорем.

При фиксированном n функция $f(n, x)$ — есть некоторая одноместная функция $f_k(x)$ в перечислении (3.1). Соответствие k номеру n — и есть функция $k = s(n)$, которая в общем случае «неизвестно какая». В гёделевском варианте $s(n)$ обязана быть вычислимой и всюду определенной. ▶

(!) *Предостережение.* Допустим,

$$f(n, x) = U(q(n), x), \tag{3.2}$$

где функция $q(n)$ вычислима, но не везде определена. По первому впечатлению из [1]

$$U(q(n), x) = U(s(n), x)$$

вытекает, что $s(n)$ является всюду определенным продолжением функции $q(n)$, чего в общем случае не может быть (теорема 3.1.3).

Впечатление ошибочно. Даже если $q(n)$ всюду определена, функция $s(n)$ не обязана совпадать с $q(n)$, — см. конструкцию обоснования следующего утверждения.

3.1.2. *Упорядочение программ вычисления по их длине [2] дает гёделевскую нумерацию.*

◀ Фиксация n в $f(n, x)$ дает программу вычислений конечной длины, которая в списке (3.1) может быть эффективно найдена. Поэтому функция $s(n)$ вычислима и всюду определена. ▶

Универсальная функция — есть эквивалент эффективного упорядочения программ (3.1), и можно было бы «не изобретать ве-

[1] Если значение $q(n)$ не определено, то $s(n)$ — номер нигде неопределенной функции.

[2] С точностью до непринципиальных оговорок подходящая нумерация по длине программ — есть *нумерация Клини*.

лосипед». Но $U(n, x)$ оказывается удобной категорией мышления, снимающей напряжение ряда головоломок[3].

Первый аргумент в $U(n, x)$ является номером программы в перечислении (3.1), и в этом смысле n — есть сама программа (однозначно восстанавливаемая по номеру). Поэтому универсальную функцию $U(n, x)$ можно трактовать как механизм, позволяющий отвлечься от процесса вычислений и сконцентрироваться на маркировке.

Из сказанного выше следует, например, существование всюду определенной вычислимой функции $\xi(m, n)$, удовлетворяющей тождеству

$$U[m, U(n, x)] = U[\xi(m, n), x].$$

Это означает, что по номерам двух функций

$$g(x) = U(n, x) \quad \text{и} \quad f(x) = U(m, x)$$

сразу определяется номер $q = \xi(m, n)$ композиции $f(g(x))$, минуя хлопоты проникновения в суть дела.

Проблема самоприменимости. *Диагональная функция*

$$u(n) = U(n, n)$$

заведомо не определена при всех n и принципиально недоопределяема, иначе вычислимая функция

$$g(n) = u(n) + 1, \quad \textit{т.е.} \quad g(n) = f_n(n) + 1,$$

не входила бы в перечисление (3.1). Другими словами, существует n, при котором значение $f_n(n)$ не определено, т. е. n-я программа не применима сама к себе[4].

Проблема останова. Другой поворот ситуации заключается в том, что функция

$$g(n) = u(n) + 1$$

[3] С помощью $U(n, x)$ уменьшается необходимая «глубина расчета» многих рассуждений.

[4] Самоприменимость, как и самовлюбленность, штука не очень естественная. Но располагать функцией $f_n(x)$, неопределенной при $x = n$, иногда удобно.

не может быть везде доопределена, иначе ее доопределение $g^*(n)$ не будет входить в перечисление [5] (3.1).

Разумеется, область определения некоторых вычислимых функций может быть расширена, иногда — вплоть до $\mathbb{N}$. Но пример функции $g(n)$ показывает справедливость следующего принципиального факта.

3.1.3. Теорема. *Среди вычислимых — существуют функции, область определения которых не может быть расширена до* $\mathbb{N}$.

Одно из возможных следствий [6] — *неразрешимость проблемы останова*. Если бы существовал алгоритм, дающий ответ на вопрос, определено ли значение $f(n)$ для любых $f \in \mathbb{F}$ и $n \in \mathbb{N}$, то $f(n)$ всегда можно было бы всюду доопределить.

То же самое можно сказать о функции $v(n) = U[n, h(n)]$, где $h(n)$ вычислима и всюду определена, иначе $v(n) + 1$ не будет входить в перечисление (3.1). Следовательно, не существует всюду определенной функции $h(n)$, которая бы обеспечивала вычислимость $f_n[h(n)]$ при любом n. С другой стороны, если значение $f_n(x)$ определено хотя бы при одном x, то это $x = h(n)$ может быть эффективно вычислено — см. комментарий к определению 1.6.1. Тогда подстановка $x = h(n)$ в $f_n(x)$ приводит к противоречию. Отсюда вытекает следующий результат.

3.1.4. Теорема. *Среди вычислимых — обязательно существует нигде не определенная функция.*

Факт может показаться тривиальным, если думать, что причина заключается в существовании плохо написанных неработающих программ. Но, как уже отмечалось, «мусор программирования» может быть отсеян [7]. Тем не менее теорема 3.1.4 гарантирует, что среди всевозможных программ, прошедших грамматические те-

[5] Будет отличаться от $f_n(x)$ в точке $x = n$ — из-за прибавления единицы, если значение $f_n(n)$ определено, либо из-за определенности значения $g^*(n)$ в случае неопределенности $f_n(n) = ?$.

[6] Другое следствие — неразрешимость области определения функции $u(n)$. В противном случае $u(n)$ могла бы быть доопределена. В результате получается еще один пример перечислимого, но неразрешимого множества. Конструкция на данном этапе выглядит намного проще, чем доказательство теоремы 1.6.4.

[7] А для машин Тьюринга и рекурсивных функций проблемы такого отсева даже не возникает.

сты, всегда есть программа, зацикливающаяся на любом входе. Например, ищущая перебором корень неразрешимого уравнения $P(x) = 0$.

- Множество номеров n, при которых гёделевская универсальная функция $U(n, x)$ нигде не определена, — неразрешимо. (?)
- Множество гёделевских номеров n любой вычислимой функции — неразрешимо. (?) (См. *теорему Райса*.)

3.2. Универсальные множества

Пусть $S_1, S_2, \ldots$ — эффективное перечисление всех перечислимых множеств, существование которого вытекает из наличия перечисления (3.1) вычислимых функций, области значений которых (либо области определения) и есть множества $S_1, S_2, \ldots$.

На другом языке это означает существование *перечислимого множества пар* $S = \{n, x \in S_n\}$, дающего S_n в сечении, при фиксированном n. Запись $S = \{n, x \in S_n\}$, конечно, равносильна игре с открытыми картами. В более общем варианте определение выглядит так. Перечислимое множество пар $S \subset \mathbb{N}\times\mathbb{N}$ называется *гёделевским универсальным множеством*, если для любого перечислимого множества $Q \subset \mathbb{N}\times\mathbb{N}$ можно указать такую вычислимую функцию $t(n)$, что

$$(n, x) \in Q \Leftrightarrow (t(n), x) \in S.$$

3.2.1. Теорема. *Область определения универсальной функции $U(n,x)$, а также множество пар $\{n, U(n, x)\}$, — являются гёделевскими универсальными множествами.*

Доказательство, конечно, не требуется. Все сводится к простому сопоставлению определений.

3.3. Изоморфизм гёделевских нумераций

Из определения 3.1.1 нетрудно вывести обоснование следующего факта.

3.3.1. Теорема. *Если $U_1(n, x)$ и $U_2(n, x)$ — две гёделевские универсальные функции, то существует обратимая всюду определенная вычислимая функция $s(n)$ такая, что*

$$U_1(n, x) = U_2(s(n), x), \quad U_2(n, x) = U_1(s^{-1}(n), x).$$

Таким образом, гёделевские универсальные функции *изоморфны* друг другу. Попросту говоря, переход к другой универсальной функции сводится к вычислимой перестановке номеров.

То же самое можно сказать об изоморфизме гёделевских универсальных множеств. Переход от одной гёделевской нумерации перечислимых множеств — к другой всегда определяется вычислимой перестановкой номеров (со взаимно однозначным соответствием).

По поводу изоморфизма хотелось бы заметить следующее. При упоминании многих понятий принято полагаться на контекст, что позволяет игнорировать подробности. С изоморфизмом ситуация несколько хуже. Слово каждый раз настойчиво объясняется — что отвлекает. Поэтому в любой области полезно вырабатывать *чутье контекста*, позволяющее многое читать по диагонали. Изоморфизм — это всегда взаимно однозначное соответствие (в данном случае — номеров), сохраняющее определенные свойства (в данном контексте — универсализм перечисления).

3.4. Теорема о неподвижной точке

Следующий результат удобен при рассмотрении многих вопросов о неразрешимости.

3.4.1. Теорема Клини. *Какова бы ни была вычислимая всюду определенная функция $q(n)$, найдется n, при котором*

$$U(n, x) = U(q(n), x)$$

тождественно по x, где $U(n, x)$ — гёделевская универсальная функция.

Если ввести знак *гёделевской эквивалентности*, $u \sim v$, означающей, что u и v номера одной и той же функции в перечислении (3.1), $f_u(x) \equiv f_v(x)$, — то $n \sim q(n)$ при некотором n. Другими словами, никакая общерекурсивная функция[8] $q(n)$ не позволяет гарантированно перейти от $f_n(x)$ к *другой* функции $f_{q(n)}(x)$ (избежать совпадения). Программа-то может быть другая[9], но при каком-то n функция будет та же самая.

[8] Напомним, что «общерекурсивная» — синоним вычислимой всюду определенной функции, — раздел 1.10.

[9] Например, в случае $q(n) = n + 1$ все программы другие.

Для дальнейшего удобно разрешить переменным в $u \sim v$ принимать неопределенные значения, имея в виду под $? \sim v$ требование, что v — номер нигде не определенной функции.

Прежде чем переходить к рассмотрению доказательства, в данном случае имеет смысл попытаться самостоятельно обосновать теорему 3.4.1. Вероятность успеха, как показывает «статистика», невелика, но неудача здесь дает больше пользы, чем знакомство с готовым рецептом.

◀ *Доказательство.* Рассмотрим вычислимую всюду определенную функцию

$$w(n) \sim u(n) = U(n, n),$$

что означает $f(n, x) = U(u(n), x) = U(w(n), x)$.

Пусть, в предположении противного, $q(n)$ не имеет неподвижной точки, т. е. $q(n) \nsim n$ при любом n. Тогда

$$u(n) \sim w(n) \nsim q(w(n))$$

при любом n, что влечет за собой $u(n) \neq q(w(n))$. Но от $u(n)$ никакая вычислимая функция — в том числе $q(w(n))$ — не может отличаться всюду, в силу $u(n) = f_n(n)$. Противоречие завершает доказательство. ▶

- При любой гёделевской нумерации неподвижных точек бесконечно много. (?)
- Какова бы ни была вычислимая всюду определенная функция $q(n)$, при гёделевской нумерации перечислимых множеств S_n найдется n, при котором $S_n = S_{q(n)}$. (?)

3.5. Теорема Райса

Бесконечный список алгоритмически неразрешимых проблем укладывается в одно предложение.

3.5.1. Теорема Райса. *Любое нетривиальное свойство вычислимых функций алгоритмически неразрешимо.*

Смысл теоремы, как нередко бывает, становится ясен из доказательства.

◀ Пусть $\mathbb{G}$ — непустое подмножество $\mathbb{F}$, не совпадающее с $\mathbb{F}$, и A — множество гёделевских номеров функций из $\mathbb{G}$. Если предположить разрешимость A, то всюду определенная функция

$$q(n) = \begin{cases} \bar{a}, & \text{если } n \in A, \\ a, & \text{если } n \in \overline{A} \end{cases} \qquad (\overline{A} \text{ дополнение } A),$$

где $a \in A$, $\bar{a} \in \overline{A}$, — не будет иметь *неподвижной точки* в смысле теоремы 3.4.1. ▶

Требование «нетривиальности свойства», фигурирующее в теореме, как видно из доказательства, равносильно $\mathbb{G} \neq \varnothing, \mathbb{F}$. Другими словами, свойство нетривиально, если имеются функции, обладающие этим свойством и — не обладающие.

Таким образом, по программе $f_n(x)$ невозможно в общем случае определить, обладает или не обладает вычисляемая функция тем или иным свойством. Алгоритмически неразрешимыми оказываются, в частности, проблемы выяснения:

- *зацикливания алгоритма на любом входе* (*неразрешимость множества номеров нигде не определенной функции*) [10];
- *конечности множества решений* $f(x) = 0$;
- *конечности или бесконечности множества значений* $f(x)$;
- *периодичности*, *ограниченности*, *порядка роста*;
- *содержит ли в десятичной записи конструктивно определяемое число* (*типа* π) *сколько угодно идущих подряд нулей.*

Невозможность алгоритмически определить в общем случае, конечно или бесконечно множество значений $f(x)$, обычно интерпретируется как неразрешимость *проблемы эффективной конечности* или *эффективной бесконечности* перечислимого множества.

Особо стоит выделить неразрешимость проблемы существования эквивалентного полиномиального алгоритма [11]. Не вдаваясь в подробности, заметим, что необходимые уточнения в формулировку здесь достаточно легко вносятся. Интересно, что при изучении NP-полных задач этот факт как-то упускается из виду. Ответ ищется либо в варианте $NP \neq P$, либо $NP = P$. Но есть и третья возможность: полиномиальный алгоритм для NP-полных задач существует, но факт недоказуем.

В последнем случае задача оказывается безнадежной, сталкиваясь с новым типом недоказуемости. С полиномом такого бы не могло случиться. «Уравнение $P(x) = 0$ имеет решение, но факт недоказуем», — явная нелепость [12]. Полиномиальность же вычислений по теореме 3.5.1 алгоритмически неразрешима, причем

[10] Множество номеров хоть где-то определенных функций тоже неразрешимо, как дополнение, — но перечислимо.

[11] Полиномиального — по времени счета.

[12] Разумеется, если перебор не запрещен, что обсуждать малоинтересно.

полиномиально вычислимые функции еще и неперечислимы, что теоремой Райса уже не улавливается. (?) В таких условиях существование «принципиально неуловимого» полиномиального алгоритма для NP-полных задач гипотетически вполне возможно.

Не следует думать, что упомянутый «новый тип недоказуемости» является чем-то принципиально новым. Он нов по сравнению с тем, что уже рассматривалось. Недоказуемость, как следствие неразрешимости, ранее возникала при разбиении $\mathbb{N}$ на два подмножества X и $\overline{X}$, одно из которых неперечислимо.

Вот другая ситуация на языке полиномиальных уравнений. Пусть $\mathscr{P}_1$ обозначает множество неразрешимых уравнений

$$P(x) = 0; \tag{3.3}$$

$\mathscr{P}_2$ — множество уравнений (3.3), имеющих конечное число решений; $\mathscr{P}_3$ — бесконечное. *Все три множества $\mathscr{P}_1, \mathscr{P}_2, \mathscr{P}_3$ — не только неразрешимы, но и неперечислимы* (?) [13] (но $\mathscr{P}_2 \cup \mathscr{P}_3$ — перечислимо).

3.6. Нумерации и гёделизация

Теория алгоритмов развивается на фоне перечисления программ и элементов множеств. Никаких особых знаний в области конструктивного счета при этом не требуется. Тем не менее манипулирование постепенно смещает акценты, и становится ясно, что вся теория может быть отражена в зеркале жонглирования номерами. Вспомогательные фокусы превращаются в язык. Проблемам нумерации посвящаются целые книги [9].

Пары натуральных чисел могут быть выстроены линейно (друг за другом) многими способами. Один из наглядных вариантов (1.8) уже упоминался. Несколько иной порядок в *канторовском* расположении:

$$(1,1);\ (1,2)\ (2,1);\ (1,3)\ (2,2)\ (3,1);\ (1,4)\ \ldots$$

Элементы (x, y) идут в порядке возрастания суммы членов, а при одинаковой сумме раньше идет пара с меньшим x. Номер $c(x, y)$ двуместного элемента (x, y) в такой последовательности называется *канторовским* [14]. Понятно, что пара по номеру $n = c(x, y)$

[13] Это трудная задача.

[14] Перечисление Кантора называют также *нумерацией Пеано*.

однозначно восстанавливается, $x = \boldsymbol{l}(n)$, $y = \boldsymbol{r}(n)$. Формулы для $\boldsymbol{c}(x, y)$, $x = \boldsymbol{l}(n)$ и $y = \boldsymbol{r}(n)$ см. в разделе 5.10, но их конкретный вид никакой роли в данном случае не играет. Важен сам факт взаимно однозначного соответствия, которое имеет место и при любой другой алгоритмически осмысленной нумерации пар.

Отталкиваясь от нумерации пар, легко получить нумерацию троек,

$$\boldsymbol{c}^3(x, y, z) = \boldsymbol{c}[\boldsymbol{c}(x, y), z],$$

и вообще n-ок чисел, продолжая процесс индуктивно,

$$\boldsymbol{c}^{k+1}(x_1, \ldots, x_{k+1}) = \boldsymbol{c}^k[\boldsymbol{c}(x_1, x_2), x_3, \ldots, x_{k+1}]. \qquad (3.4)$$

При этом $\boldsymbol{c}^m(s_1, \ldots, s_m)$ называют *нумерующей функцией.*

Нумерации Клини и Поста широко используются в теории рекурсивных функций, и о них здесь стоит упомянуть хотя бы с просветительской точки зрения. *Нумерация Клини* вместо *канторовской нумерующей функции* $\boldsymbol{c}(x, y)$ берет за основу функцию

$$[x, y] = \boldsymbol{c}(\boldsymbol{l}(x), \boldsymbol{c}(\boldsymbol{r}(x), y)),$$

которая, как и $\boldsymbol{c}(x, y)$, обеспечивает взаимно-однозначную нумерацию пар.

Резон перехода к новому перечислению заключается в построении — на базе $[x, y]$ — *универсальной функции Клини* $\boldsymbol{K}(n, x)$. Преимущества $\boldsymbol{K}(n, x)$ заключаются в простых формулах, дающих номера композиции функций, суммы и других комбинаций рекурсивного характера. Но эти выгоды не столь принципиальны (хотя где как). Главное с точки зрения данного контекста заключается в том, что клиниевская нумерация является *гёделевской.*

Нумерация Поста относится к перечислению множеств. Если S — перечислимое множество, то постовский номер S является клиниевским номером функции

$$f_n(x) = \boldsymbol{K}(n, x),$$

множество значений которой совпадает с S.

Гёделизация. Особую роль играет *нумерация по Гёделю*, базирующаяся на принципиально иной идее. Как известно, любое N

разлагается на простые множители [15] p_k:

$$N = 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \dots p_n^{a_n},$$

что устанавливает соответствие n-кам $\{a_1, \dots, a_n\}$ номеров из $\mathbb{N}$.

В отличие от нумераций Кантора и Клини множество номеров Гёделя n-ок чисел имеет «дырки», которые частично заполняются при увеличении n. Этот «недостаток» оборачивается преимуществами, когда возникает необходимость нумерации не только наборов чисел, но и любых текстов в любом алфавите. Делается это, например, так.

В алфавите

$$0, 1, a, b, c, \dots, +, =, (,), /, \dots, \exists, \forall, \dots \tag{3.5}$$

фиксируется порядок символов, после чего множество (3.5) *инъективно* [16] отображается в $\mathbb{N}$ с помощью некоторой функции $\varphi(\cdot)$. Тогда тексту (выражению) $T = \{s_1, \dots, s_n\}$, где s_j символы алфавита, присваивается номер

$$\alpha(T) = 2^{\varphi(s_1)} \cdot 3^{\varphi(s_2)} \dots p_n^{\varphi(s_n)}.$$

При необходимости говорить о последовательностях текстов $D = \{T_1, \dots, T_k\}$ — например, о доказательствах, — трюк повторяется. Последовательности D сопоставляется номер

$$\beta(D) = 2^{\alpha(T_1)} \cdot 3^{\alpha(T_2)} \dots p_k^{\alpha(T_k)}.$$

[15] Вопрос о том, входит ли двойка (и даже единица) в список простых чисел, в разных контекстах может решаться различно. У нас $p_1 = 2$.

[16] Функция $\varphi(\cdot)$ называется *инъективной*, если образы $\varphi(a)$, $\varphi(b)$ при $a \neq b$ не совпадают.

Глава 4

Доказуемость

Чтобы снять недоверие, не надо настаивать.

При достаточном богатстве «изобразительных средств» возникает диспропорция между теоремами и доказательствами. Теорем оказывается «больше». Доказательств «не хватает», условно говоря. Главный вариант такой ситуации описан в разделе 2.1. Возникающая там картина достаточно прозрачна и представляется исчерпывающей. Но это на самом деле лишь один край диапазона. На другом краю задача сужена, и все доказывается. Посредине точка бифуркации, и там калейдоскоп частных случаев обнажает явление с иных сторон. При этом важны детали. Слишком общая точка зрения обязательно что-то упускает. Конкретика сильнее философии.

4.1. Конфликт с определением истины

Итак, недоказуемая часть арифметики в разделе 2.1 оценивается с большим запасом. Выделяется то, что не будет доказано никогда. В действительности же неаксиоматизируемая арифметика стоит на якоре общепринятой системы аксиом, и круг недоказуемых фактов получается намного шире.

Природа конфликта доказуемости с истинностью заключается *в конструктивном определении теорем и неконструктивном определении истины*. Точка зрения на истинность «плавает», в определенной степени неконтролируемо, в диапазоне от *смыслового* (логического) задания до *синтаксического* [1] «истинно то и только то, что синтаксически доказуемо».

Истинное логически — допускает обороты «для всех x» «не существует x», а поскольку возможных значений x бесконечно много — не ясно, как это проверить. Доказательства же рассматриваются как цепочки, соединяющие «предположения» с «выводами», —

[1] См. главу 5.

звенья которых регулируются аксиоматикой. Концы цепочек — это доказуемые *теоремы*. Все однозначно определено. Но если возможностей языка хватает для формулировки результатов, у которых «посылки» не соединяются с «заключениями», — возникает ниша недоказуемых фактов.

Как ни странно, традиционное присутствие понятия истины здесь в значительной мере запутывает суть дела. В «очищенном» виде проблема выглядит проще. Доказательства, как «цепочки», — перечислимы, а значит, перечислимо множество T теорем. Если же аксиоматика устроена так, что перечислимое множество T неразрешимо, — возникает недоказуемость. Для любой теоремы $t \in T$ перечисляющий алгоритм рано или поздно дает доказательство, а для $s \notin T$ — алгоритма нет.

Нарисованная картина при внимательном взгляде несколько расползается, — ибо зачем нужна неразрешимость множества T? Достаточно, чтобы T не совпадало с множеством $\mathbb{T}$ всех утверждений. Тогда существуют недоказуемые $s \notin T$, и разрешимость T не спасает.

Возражение резонное. Проблематика доказуемости имеет несколько ракурсов, и в тех случаях, когда нет *дихотомического* противопоставления всех утверждений — «t» и «не t», — недоказуемость равносильна неравенству $T \neq \mathbb{T}$ (см. *проблема эквивалентности слов*). В таких случаях неразрешимость и прочая «тьюрингова эквилибристика» отношения к делу не имеет. Множество T может быть как разрешимо в $\mathbb{T}$, так и неразрешимо, но это уже проблема следующего уровня.

В разделе 4.2 рассматриваются примеры двух теорий. В одной — за основу берутся обычные свойства сложения и умножения, комбинация которых порождает множество T *тождеств* (теорем). Все тождества в совокупности $\mathbb{T}$ равенств, записываемых с помощью сложения, умножения и расстановки скобок, — оказываются доказуемы.

В другой теории (*HSI-проблема Тарского*) к предыдущей системе аксиом добавляются обычные свойства возведения в степень, которые присовокупляются также к разрешенным средствам записи тождеств. Множества T и $\mathbb{T}$ расширяются, но теория *неожиданно* оказывается неразрешимой в результате несовпадения $T \neq \mathbb{T}$.

(!) Иного сорта проблема доказуемости возникает в известной *задаче об эквивалентности слов* (раздел 4.5). Слова в некотором алфавите $\mathbb{A} = \{a, b, c \ldots\}$ считаются *эквивалентными*, $\alpha \sim \beta$, если одно получается из другого с помощью заданной *системы подстановок*, позволяющих заменять некоторые куски текста другими. Скажем, «$\ldots ac \ldots$» на «$\ldots bbca \ldots$».

Если теперь несколько слов объявить аксиомами, то разрешенными подстановками [2] их можно превратить в множество T *правильных слов*. В большинстве случаев T не совпадает с множеством $\mathbb{T}$ всех слов, но это не решает задачу, присутствующую за кадром. По большому счету хотелось бы уметь определять по любому слову, принадлежит оно T или нет. «Уметь определять» — значит, уметь доказывать одно из двух. Но $\alpha \notin T$ принципиально недоказуемо с помощью исходной аксиоматики.

Однако почему бы не предположить, что $\alpha \notin T$ может быть выведено той же системой подстановок из специально подобранных «неправильных слов», либо с помощью другой системы подстановок, либо еще как-нибудь конструктивно. Оказывается, никак (!), что устанавливается уже только с привлечением алгоритмического подхода.

Таким образом, проблематика доказуемости может пониматься иначе, — как в данном случае. Теоремами естественно считать утверждения о выводимости или невыводимости того или иного слова α, причем для каждого α имеет место одно из двух: «верно, не верно», «выводится, не выводится», — что порождает истину и ложь. Далее о доказательстве теорем можно говорить «расширительно», допуская новую «аксиоматику доказательств», либо вообще выходя на орбиту «любых формализуемых методов». В последнем случае недоказуемость будет означать невозможность обоснования ($\alpha \in T$ или $\alpha \notin T$) какими угодно способами, использующими любые непротиворечивые аксиомы и правила вывода. Именно в таком ключе решена *проблема эквивалентности слов* [3]. При определенном соглашении о терминологии это можно интер-

[2] Которые принято называть *правилами вывода*, но ничто не мешает их тоже считать аксиомами, скажем, второго сорта.

[3] Существует такая система подстановок в некотором алфавите, что проблема эквивалентности слов неразрешима никакими средствами.

претировать как неаксиоматизируемость соответствующей теории подобно арифметике.

Сказанное мотивирует появление в фокусе внимания математической логики, потому что преобразование слов с помощью подстановок начинает выглядеть слишком узко. Становится понятно, что для формулировки теорем надо подобрать адекватный язык, куда бы входили плюсы-минусы, кванторы и прочий инструментарий. Для доказательств — другой язык, который бы не допускал неэффективных конструкций. Тогда бы можно было рассчитывать на изучение не игрушечных теорий, а скажем, всей арифметики.

Такую программу матлогика действительно реализует, но в итоге (после крайне запутанных построений) — перевод смысловой стороны дела на чисто синтаксическую основу[4)] сводит задачу к проблеме эквивалентности слов. Тем самым выясняется, что можно было обойтись без всех этих хлопот, которые так безобразят логические рассуждения.

4.2. HSI-проблема Тарского

Иногда говорят, что без аксиомы индукции невозможно доказывать утверждения, справедливые для любых целых чисел. Это не совсем так. Например, совокупность аксиом A_0:

- *коммутативность (перестановочность) сложения и умножения*,
- *правило умножения на единицу*,
- *произвол в расстановке скобок для суммы и произведения*,
- *дистрибутивный закон*

$$a(b+c) = ab + ac$$

позволяет доказывать любые тождества, записываемые с помощью сложения, умножения и расстановки скобок. Получается замкнутая теория, в которой все истины доказуемы.

Тарский задался вопросом о «незначительном» расширении языка, добавив к A_0 возведение в степень и постулируя обычные

[4)] В которой знаки $+, \times, =, \forall, \exists$ превращаются в ничего не значащие буквы.

свойства:

$$1^a = 1, \quad a^1 = a,$$
$$c^{a+b} = c^a c^b, \tag{4.1}$$
$$(ab)^c = a^c b^c, \quad (a^b)^c = a^{bc}.$$

Будут ли в этом случае (на базе аксиоматики «A_0 *плюс* (4.1)») доказуемы все правильные тождества?

Эта так называемая *HSI-проблема Тарского*[5] наградила бессонными ночами немалое количество людей, включая самого Тарского. Поначалу казалось, что решение должно быть положительным. Через 20 лет нашлось верное в $\mathbb{N}$ *тождество Уилки*[6]

$$[(1+n)^n + (1+n+n^2)^n]^m[(1+n^3)^m + (1+n^2+n^4)^m]^n =$$
$$= [(1+n)^m + (1+n+n^2)^m]^n[(1+n^3)^n + (1+n^2+n^4)^n]^m, \tag{4.2}$$

недоказуемое с помощью аксиом «A_0+(4.1)».

◀ Справедливость (4.2) в $\mathbb{N}$ устанавливается просто. Очевидно,

$$\frac{1+n^2+n^4}{1+n+n^2} = \frac{1+n^3}{1+n} = 1-n+n^2, \qquad n \in \mathbb{N},$$

что проверяется «в лоб» делением многочленов. Причем $1-n+n^2 \in \mathbb{N}$.

В обозначениях

$$\alpha = 1-n+n^2, \quad \beta = 1+n, \quad \gamma = 1+n+n^2$$

равенство (4.2) приобретает вид

$$(\beta^n + \gamma^n)^m \cdot [(\beta\alpha)^m + (\gamma\alpha)^m]^n = (\beta^m + \gamma^m)^n \cdot [(\beta\alpha)^n + (\gamma\alpha)^n]^m,$$

что уже легко доказывается только с помощью «A_0+(4.1)». ▶

Обойтись только лишь системой «$A_0 + (4.1)$» не удается из-за невозможности установить *в рамках* «$A_0 + (4.1)$», что

$$1-n+n^2 \in \mathbb{N}.$$

Но это, конечно, не аргумент недоказуемости. Обоснование последней вообще выглядит проблематично. Ведь можно констатировать,

---

[5] HSI — аббревиатура от *High School Identities*.

[6] См. также: *Gurevich R.* Equational theory of positive numbers with exponentiation // Proc. Amer. Math. Soc. 1985. **94**. 135–141.

что еще не получилось. Но как гарантировать, что и не получится? Оказывается, можно. Для этого создается *интерпретация*, отличная от множества обычных чисел, в которой аксиомы «A_0+(4.1)» выполняются, а тождество (4.2) ошибочно. Вот соответствующая модель [7], состоящая из 14 «букв» 1, 2, 3, 4, a, b, c, d, e, f, g, h, i, j.

Таблица сложения

$x+y$	1	2	3	4	a	b	c	d	e	f	g	h	i	j
1	2	3	4	4	2	3	d	3	4	4	4	4	4	4
2	3	4	4	4	3	4	3	4	4	4	4	4	4	4
3	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
a	2	3	4	4	b	3	b	3	4	4	4	4	4	4
b	3	4	4	4	3	4	3	4	4	4	4	4	4	4
c	d	3	4	4	b	3	b	3	4	4	4	4	4	4
d	3	4	4	4	3	4	3	4	4	4	4	4	4	4
e	4	4	4	4	4	4	4	4	4	g	4	4	4	4
f	4	4	4	4	4	4	4	4	g	4	4	i	4	4
g	4	4	4	4	4	4	4	4	4	4	4	4	4	4
h	4	4	4	4	4	4	4	4	4	i	4	4	4	4
i	4	4	4	4	4	4	4	4	4	4	4	4	4	4
j	4	4	4	4	4	4	4	4	4	4	4	4	4	4

Таблица умножения

$x \times y$	1	2	3	4	a	b	c	d	e	f	g	h	i	j
1	1	2	3	4	a	b	c	d	e	f	g	h	i	j
2	2	4	4	4	b	4	b	4	4	4	4	4	4	4
3	3	4	4	4	3	4	3	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
a	a	b	3	4	c	b	c	b	4	f	4	4	4	4
b	b	4	4	4	b	4	b	4	4	4	4	4	4	4
c	c	b	3	4	c	b	c	b	4	f	4	4	4	4
d	d	4	4	4	b	4	b	4	4	4	4	4	4	4
e	e	4	4	4	4	4	4	4	4	4	4	j	4	4
f	f	4	4	4	f	4	f	4	4	4	4	4	4	4
g	g	4	4	4	4	4	4	4	4	4	4	4	4	4
h	h	4	4	4	4	4	4	4	j	4	4	4	4	4
i	i	4	4	4	4	4	4	4	4	4	4	4	4	4
j	j	4	4	4	4	4	4	4	4	4	4	4	4	4

[7] Это модель *Джексона*, заимствованная из статьи *М. В. Волкова* «Проблема конечности базиса тождеств» (МИФ. 1997. № 2).

Таблица возведения в степень

x^y	1	2	3	4	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	4	4	*e*	4	4	4	4	4	4	4	4	4
3	3	4	4	4	*f*	4	4	4	*f*	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
a	*a*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*
b	*b*	4	4	4	4	4	4	4	4	4	4	4	4	4
c	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*	*c*
d	*d*	4	4	4	4	4	4	4	*h*	4	4	4	4	4
e	*e*	4	4	4	4	4	4	4	4	4	4	4	4	4
f	*f*	4	4	4	4	4	4	4	4	4	4	4	4	4
g	*g*	4	4	4	4	4	4	4	*h*	4	4	4	4	4
h	*h*	4	4	4	4	4	4	4	4	4	4	4	4	4
i	*i*	4	4	4	*e*	4	4	4	4	4	4	4	4	4
j	*j*	4	4	4	4	4	4	4	4	4	4	4	4	4

В описанных обстоятельствах, естественно, возникает соблазн присоединить (4.2) к «A_0+(4.1)», чтобы получить полный набор аксиом. Но барьер разнообразия средств уже преодолен, и *тождества начинают размножаться быстрее, чем доказательства*. Точнее говоря, добавление к «A_0+(4.1)» любой конечной совокупности тождеств, выражаемых на языке «=, +, ×, ↑»[8], — не дает исчерпывающей аксиоматики, которая бы гарантированно позволяла доказывать тождества, записанные на том же языке[9].

Ситуация в целом выглядит следующим образом. Из *арифметики Пеано* извлекаются тождества, записанные на языке «=, +, ×, ↑», и ставится задача выделить конечный набор (базис) тождеств, из которых бы все остальные следовали. Такого базиса в данном случае нет, что можно интерпретировать как *неаксиоматизируемость арифметики в срезе «=, +, ×, ↑»*.

Проблемы для размышления

- Доказуемость некоторых формул на одном языке и недоказуемость — на другом — естественная основа для неоднозначного толкования истины. А все ли

[8] Знак ↑ обозначает операцию возведения в степень.

[9] *Gurevich R.* Equational theory of positive numbers with exponentiation is not finitely axiomatizable // Ann. Pure and Applied Logic. 1990. **49**. 1–30.

тождества на языке «$=$, $+$, $\times$, $\uparrow$» могут быть доказаны в *арифметике Пеано* (с использованием индукции)?

- Верные тождества
$$\forall\, x \in \mathbb{N}^m : A(x) = B(x)$$
непроверяемы (но могут быть доказуемы), ошибочные — проверяемы перебором, и потому *перечислимы*. Множество ошибочных тождеств в языке «$=$, $+$, $\times$» также *разрешимо*. А в «$=$, $+$, $\times$, $\uparrow$»?

4.3. Нормальные алгоритмы Маркова

Вернемся на некоторое время к проблемам алгоритмизации. Естественный подход к формализации понятия вычислимости был предложен *Марковым*.

Любой алгоритм при записи опирается на некие правила, сводимые на синтаксическом уровне (по крайней мере, так кажется) к некоторой *системе подстановок*. Точнее говоря, исходное слово в избранном алфавите — скажем, $\mathbb{A} = \{a, b, c\}$, — шаг за шагом преобразуется с помощью регламентированных замен кусков текста — другими, например,

$$\begin{cases} ac \Rightarrow aa, \\ cc \Rightarrow bac, \\ cb \Rightarrow bbc, \end{cases} \tag{4.3}$$

что порождает цепочки преобразований вида

$$cbc \to bbcc \to bbbac \to bbbaa.$$

В *нормальном алгоритме* процедура уточняется следующим образом. На каждом шаге подстановки перебираются в заданном порядке, и применяется первая возможная (слова просматриваются слева направо). При отсутствии разрешенной подстановки алгоритм останавливается.

В алфавите $\mathbb{A} = \{1, *, a, b\}$ нормальный алгоритм

$$\begin{aligned} *11 &\Rightarrow a * 1, \\ *1 &\Rightarrow a, \\ 1a &\Rightarrow a1b, \end{aligned}$$

$$
\begin{aligned}
ba &\Rightarrow ab,\\
b1 &\Rightarrow 1b,\\
a1 &\Rightarrow a,\\
ab &\Rightarrow b,\\
b &\Rightarrow 1,
\end{aligned}
$$

осуществляет умножение, перерабатывая $\underbrace{111\ldots1}_{n} * \underbrace{111\ldots1}_{m}$ в слово $\underbrace{111\ldots1}_{n\cdot m}$. Символы a, b играют вспомогательную роль. Нечто вроде зарубок.

Нетрудно сообразить, что машина Тьюринга реализует, по сути, нормальный алгоритм, поэтапно преобразуя слово, записанное на ленте, с помощью списка команд (1.9), который тривиальными ухищрениями приводится к стандартной форме подстановок вида (4.3) [10]. Поэтому сразу ясно, что тьюринговские «неразрешимости» переносятся на нормальные алгоритмы (самоприменимость, проблема останова).

Таким образом, машина Тьюринга явно представляет собой частный случай нормального алгоритма. В то же время *нормальные алгоритмы реализуются на подходящих машинах Тьюринга* (*что устанавливается несколько сложнее*), *и отнюдь не расширяют диапазон вычислимости, давая тот же результат.*

Определенный интерес может представлять рассмотрение прежних вопросов в терминах нормальных алгоритмов. Вот простейшая иллюстрация. Расширяя исходный алфавит $\mathbb{A} = \{a_1, \ldots, a_n\}$ двумя знаками a_{n+1} и a_{n+2}, отвечающими «запятой» и стрелке «$\Rightarrow$», получаем возможность записывать *систему подстановок* любого алгоритма словом в алфавите

$$\mathbb{A} = \{a_1, \ldots, a_{n+2}\}.$$

В результате появляется возможность применить алгоритм к собственной записи и поставить вопрос о самоприменимости алгоритмов.

Допустим, нормальный алгоритм U перерабатывает запись любого самоприменимого алгоритма в слово «Yes», а любого несамоприменимого — в слово «No». Дополняя алгоритм U зацикливающей подстановкой

$$\mathbf{Y}es \Rightarrow \mathbf{Y}es,$$

получаем алгоритм $\widehat{U}$, который не останавливается на самоприменимых алгоритмах и останавливается на — несамоприменимых. Понятно, что на собственной

[10] Надо лишь договориться, как добавлять текущее состояние машины q_j к слову на ленте. Например, вписывать в обозреваемую ячейку слева от символа.

записи алгоритм $\widehat{U}$ «ломает зубы». Противоречие свидетельствует о неразрешимости проблемы самоприменимости нормальных алгоритмов.

4.4. Системы Поста

Системы Поста идеологически близки к нормальным алгоритмам Маркова, но это все же иной по духу инструмент.

В центре внимания по-прежнему подстановки типа (4.3), но теперь помимо символов собственного алфавита $\mathbb{A} = \{a, b, \ldots\}$ в записи подстановок могут фигурировать переменные (обозначаемые большими буквами), вместо которых можно подставлять слова, записанные в $\mathbb{A}$. Такие подстановки называются *продукциями Поста*. Например, «$S \Rightarrow Saa$» обозначает возможность приписать aa справа к любому слову.

Примеры

• *Палиндромы*[11] в алфавите $\mathbb{A} = \{a, b, c\}$ охватываются *продукциями*:

$$S \Rightarrow a\,S\,a, \quad S \Rightarrow b\,S\,b, \quad S \Rightarrow c\,S\,c,$$

но для «заземления» надо еще постулировать *аксиомы*:

$$a,\ b,\ c,\ aa,\ bb,\ cc,$$

чтобы задача «стала на фундамент».

Вот цифровой пример:

$$111111111 \times 111111111 = 12345678987654321.$$

• *Правильные скобочные выражения* в алфавите $\mathbb{A} = \{\ (,)\ \}$ с аксиомой () описываются продукцией:

$$XY \Rightarrow X()Y. \tag{4.4}$$

Здесь возникает обычная для аксиоматических систем проблема. Ограничиваясь минимумом правил, легче доказывать общие теоремы. А расширяя инструментарий, легче решать конкретные задачи.

Возможность ограничиться единственной продукцией (4.4) позитивна в первом смысле, но сразу не ясно, исчерпывает ли (4.4) все правильные скобочные выражения, которые могут строиться также по очевидным рецептам

$$S \Rightarrow (S), \quad X \Rightarrow XY.$$

Ответ: «исчерпывает», — но это задача, хотя и не трудная.

[11] Слова, читаемые одинаково в обоих направлениях. Например, *aba*, *bbcacbb*.

• Продукции позволяют записывать также правила вывода типа

$$(X+Y)Z \Rightarrow XZ+YZ, \tag{4.5}$$

которые в рамках иного подхода могут именоваться аксиомами [12].

При необходимости отразить $(X+Y)Z = XZ+YZ$ продукцию (4.5) можно дополнить противоположной

$$XZ+YZ \Rightarrow (X+Y)Z.$$

4.4.1. Определение. *Каноническая система Поста есть система из трех составляющих*:

- *собственный алфавит* $\mathbb{A}$ *плюс алфавит переменных* $\mathbb{X}$,
- *набор аксиом* (*слов в алфавите* $\mathbb{A}$),
- *совокупность продукций.*

4.4.2. Определение. *Последовательность слов в канонической системе есть* ***доказательство****, если каждое слово этой последовательности есть либо аксиома, либо выводимо из предыдущих слов применением одной из продукций. Последнее слово любого доказательства называется* ***теоремой****.*

Из дальнейшего будет видно, что такое определение доказательства отвечает пониманию доказательства в математической логике при символической записи содержательных теорий.

Машина Тьюринга — это система Поста. Такое соответствие спасает от многих лишних рассуждений. Речь идет о следующем. Если набор продукций сделать, отталкиваясь от списка команд (1.9) машины Тьюринга, а в качестве аксиомы взять начальное слово, записанное на ленте, — работа машины Тьюринга будет совпадать с последовательным применением системы продукций Поста. И потому — тьюринговы «неприятности» будут присущи системам Поста при подходящей интерпретации.

Сказанное, вообще говоря, требует расшифровки, потому что продукции из команд (1.9) сделать не так просто. Сначала надо договориться об алфавите $\mathbb{A}$ системы Поста. В $\mathbb{A}$ включаются тьюринговы символы $\{a_i\}$, которые пишутся на ленте, плюс символы q_j, обозначающие внутренние состояния. Затем примем соглашение, что состояние машины q_j вклинивается в слово на ленте слева

[12] Аксиомы в рамках систем Поста опираются только на собственный алфавит $\mathbb{A}$.

от обозреваемого символа[13]. Тогда списочная команда $q_i a_j \to q_k a_l R$ (при движении головки вправо) переделывается в продукцию

$$X q_i a_j Y \Rightarrow X a_l q_k Y.$$

При движении головки влево, $q_i a_j \to q_k a_l L$, возникает неудобная ситуация, которую можно было бы разрешить так

$$X S q_i a_j Y \Rightarrow X q_k S a_l Y, \tag{4.6}$$

если бы переменная S предполагала возможную подстановку на ее место только одной буквы из $\{a_1, \ldots, a_m\}$, но такой переменной, по определению, нет. Поэтому (4.6) приходится заменять несколькими продукциями, подставляя вместо S последовательно все буквы из $\mathbb{A}$. Кроме того, надо еще добавить продукции, предусматривающие выход головки машины за пределы слова. Но в итоге все же достигается требуемый результат.

В общем случае система Поста не предполагает алгоритмическую реализацию, поскольку при последовательном применении не предусмотрено правило выбора продукции на каждом шаге. Если вернуться к *нормальным алгоритмам Маркова*, добавив к исходному — алфавит свободных переменных и оговорив список начальных слов (аксиом), — получится система Поста с наложением дополнительного правила выбора продукции. В рассмотренном примере с машиной Тьюринга проблемы не возникает, потому что выбор, собственно, не нужен — на каждом шаге оказывается применима лишь одна продукция.

Возможность имитации работы любой машины Тьюринга с помощью канонической системы указывает на справедливость следующего результата.

4.4.3. Теорема. *Каково бы ни было перечислимое множество T слов в алфавите $\mathbb{A}$, существует каноническая система, множество теорем которой совпадает с T.*

Пример. Каноническая система, генерирующая простые числа в единичном коде [20]: алфавит $\mathbb{A} = \{1, a, b, c, d\}$, две аксиомы $\{11, a111\}$ и 6 продукций:

$$\begin{aligned} aX &\Rightarrow aX1, \\ aX1 &\Rightarrow cXdbX1, \\ X1dY1 &\Rightarrow 1Xd1Y, \end{aligned}$$

[13] Если кому-то кажется, что это является вмешательством в работу машины, нарушающим ход процесса, — переписывать слово на ленте, вписывая q_j, можно на отдельной бумаге.

$$Xcd Y1 \Rightarrow cXdY1,$$
$$XcY1dZb \Rightarrow cXYdbZ,$$
$$11cdXb1 \Rightarrow X1.$$

Довольно экономная программа, моделирующая сложное поведение.

Канонические расширения. Продукции канонических систем могут иметь довольно сложную структуру, что затрудняет использование инструмента. Пост установил довольно неожиданный факт: за счет *канонического расширения* любая система может быть сведена к системе с *единственной аксиомой* и *нормальными продукциями* вида

$$\alpha X \Rightarrow X\beta, \tag{4.7}$$

где α, β — слова в расширенном алфавите [14].

Разумеется, речь идет об *эквивалентном* сведéнии. Исходный алфавит $\mathbb{A}$ расширяется до $\mathbb{A}'$, но совокупность теорем расширенной системы, использующих только символы из $\mathbb{A}$, в точности совпадает с совокупностью теорем исходной системы.

4.5. Проблема эквивалентности слов

При заданном наборе продукций $\{\Pi_k\}$ естественно возникает вопрос о возможности преобразовать то или иное слово α в слово β. Для некоторых наборов $\{\Pi_k\}$ такая задача *алгоритмически разрешима* для любой пары слов (α, β). Но не в общем случае.

Обоснование неразрешимости легко получается благодаря связи канонических систем Поста с машинами Тьюринга. Вот конструкция, приводящая к ответу.

Пусть q_n обозначает заключительное состояние и работа машины Тьюринга организована так, что она останавливается (если останавливается) после стирания записанного на ленте слова [15]. Сопоставим такой машине систему продукций, как описано в предыдущем разделе. Возможность преобразования слова $q_1\alpha$ в слово q_n равносильна ответу на вопрос, остановится ли машина, начиная работу со слова α. Неразрешимость *проблемы останова* решает исходную задачу отрицательно.

[15] Это делается последовательным присоединением к машине другой машины Тьюринга, которая стирает запись на ленте и останавливается.

Близкая по характеру проблема возникает для так называемых *ассоциативных исчислений*, или *систем Туэ*, — определяемых *системами подстановок* типа (4.3), но с возможностью замен в обоих направлениях, например,

$$acbbc \Leftrightarrow aacb,$$

что не так уж принципиально, поскольку $\alpha \Leftrightarrow \beta$ равносильно совокупности двух подстановок $\alpha \Rightarrow \beta$ и $\beta \Rightarrow \alpha$. Однако для преобразований одних слов в другие возникает, вообще говоря, новая ситуация.

Слова α и β называют *эквивалентными* или *равными*, если одно преобразуется в другое с помощью подстановок ассоциативного исчисления.

4.5.1. Теорема. *Существуют ассоциативные исчисления, в которых проблема эквивалентности слов — неразрешима.*

◀ Фиксация в каждой подстановке $\alpha_i \Leftrightarrow \beta_i$ ассоциативного исчисления $\mathscr{A}$ одного из двух направлений — порождает каноническую систему Поста $\mathscr{P}$. Будь проблема *эквивалентности* — разрешима в $\mathscr{A}$, она была бы разрешима (в «однонаправленном» виде) и в $\mathscr{P}$. ▶

Полугрупповая интерпретация. *Полугруппой* называют множество G с определенным на парах его элементов ассоциативным «умножением» [16]. Полугруппа обычно задается с помощью «таблицы умножения». Совокупности (многообразия) полугрупп выделяются с помощью некоторых систем тождеств, называемых *определяющими соотношениями*. Например, тождество $ab = ba$ выделяет *коммутативные полугруппы*. Система определяющих соотношений может задавать также конкретную полугруппу.

Стандартными примерами могут служить полугруппы непрерывных, дробно-линейных и других преобразований — с композицией функций в качестве полугрупповой операции [17].

Подмножество $G_0 \subset G$ называется *порождающим*, если любой элемент из G представим в виде произведения элементов из G_0.

[16] Ассоциативность позволяет в произведениях произвольно расставлять скобки, в том числе — вообще обходиться без скобок.

[17] Более того, *любая полугруппа с единицей изоморфна некоторой полугруппе преобразований.*

Последние называются *образующими* полугруппы G. При конечном числе образующих $G_0 = \{g_1, \ldots, g_n\}$ элементы G можно рассматривать как слова в алфавите $\{g_1, \ldots, g_n\}$, в которых опущен знак умножения. Слова могут быть эквивалентны, если переводятся друг в друга с помощью системы *определяющих соотношений*, которые на языке ассоциативного исчисления есть не что иное, как системы подстановок.

В итоге получается, что *проблема эквивалентности слов в полугруппах — неразрешима*, поскольку сие установлено для ассоциативных исчислений. Разумеется, речь идет о ситуациях задания полугрупп некими «определяющими» соотношениями. При наличии таблицы умножения проблемы нет — сравниваемые слова просто вычисляются.

Для полугрупп специального вида ситуация может оказаться иной, чего можно было ожидать, например, в случае группы [18].

Группой называется полугруппа с единицей e ($ae = ea = a$ для любого $a \in G$) и существованием обратного элемента $b = a^{-1} \in G$ для любого $a \in G$ ($ab = ba = e$).

Обойтись в определении одной лишь групповой операцией, заменяя системой тождеств требования существования единицы и обратных элементов, — нельзя [19].

Задача об эквивалентности слов в группе оказалась весьма сложной, и была отрицательно решена в 50-х годах прошлого века [20].

Что касается проблемы эквивалентности — в полугруппах, то неразрешимость выше устанавливалась, по виду, неконструктивно. Но по сути, если вспомнить, что универсальная машина Тьюринга конкретно описываема (см. дополнительно [20]), становится понятна возможность эффективно построить ассоциативное исчисление с неразрешимой проблемой эквивалентности слов. Экономный

[18] Машина Тьюринга с неразрешимой проблемой останова дает пример полугруппы, которая, вообще говоря, не обязана быть группой.

[19] Доказывается от противного.

[20] **Теорема Новикова.** *Существует конечно порожденная группа, для которой проблема эквивалентности слов неразрешима.* Уточнения и доказательство есть в [26].

пример указал *Цейтин*: алфавит $\{a, b, c, d, e\}$ с семью подстановками (определяющими соотношениями):

$$ac \Leftrightarrow ca, \quad ad \Leftrightarrow da, \quad bc \Leftrightarrow cb, \quad bd \Leftrightarrow db,$$

$$eca \Leftrightarrow ce, \quad edb \Leftrightarrow de, \quad cca \Leftrightarrow ccae.$$

Матиясевич построил «неразрешимое» ассоциативное исчисление всего с тремя подстановками.

4.6. Таг-проблемы

Существует довольно много итерационных процедур, дразнящих своей простотой, но не поддающихся анализу.

Вот задача, которой безуспешно занимался Пост. *На каждой итерации со словом S из нулей и единиц (двоичным числом) производится одна и та же манипуляция. Если S начинается с нуля, к нему добавляются справа два нуля, а если — с единицы, — справа приписывается* 1101. *В том и другом случае вычеркиваются первые три цифры.*

Вопрос, остающийся пока без ответа, заключается в том, будет ли длина слова расти до бесконечности или установится периодический режим.

Рассмотренная задача — пример из области *таг-проблем*, каковыми называют задачи, связанные с *каноническими системами Поста*, основанными только на *нормальных продукциях*

$$\alpha_j X \Rightarrow X\beta_j,$$

которые удовлетворяют двум требованиям: все α_j имеют одинаковую длину, а β_j зависят только от первой буквы α_j.

Не будь наложены дополнительные требования на продукции, неразрешимость таг-проблем вытекала бы из универсальности систем Поста. Но с некоторыми усилиями устанавливается [20], что эти требования «не мешают», благодаря чему таг-проблемы в общем виде неразрешимы. Другое дело — конкретные задачи. Там занятие на всю жизнь может обеспечить какой-нибудь пустячок.

Широко известна, например, *задача* «$3n + 1$», идеологически ложащаяся в то же русло. Задача с виду совсем простая. Рассмат-

ривается определяемая итерационно числовая последовательность

$$a_{k+1} = \begin{cases} 3a_k + 1, & \text{если } a_k \text{ нечетно}, \\ \dfrac{a_k}{2}, & \text{если } a_k \text{ нечетно}. \end{cases}$$

Вычислительные эксперименты показывают, что процедура, начинаясь с a_0 из очень широкого диапазона[21)], попадает в цикл $\{4, 2, 1\}$, иногда после длительных и весьма экзотических блужданий. Но так ли будет для всех $a_0 \in \mathbb{N}$ — неизвестно.

4.7. Формальные грамматики

Канонические системы Поста по существу широко изучаются под маркой *формальных грамматик*. Различия определяются незначительными нюансами: разделение алфавита на *терминальный* и *нетерминальный*, плюс некоторые дополнительные акценты, на которых в данном контексте не имеет смысла останавливаться.

Принципиальное отличие заключается в фокусе внимания. Если системы Поста в большей степени ориентированы на изучение «неразрешимостей», то формальные грамматики — это идеологический инструмент для практического изучения различных языков, от естественных — до языков программирования (см. [6, 12]). Внимание концентрируется на классификации *систем подстановок*, — которые определяют ядро грамматики, — и выделении тех классов грамматик, которые обладают широким охватом приложений и минимумом аномальных свойств.

Наибольшее распространение получили так называемые *контекстно-свободные грамматики*. Все правила (подстановки) КС-*грамматик* имеют вид $x \Rightarrow \gamma$, где x — нетерминальный символ (переменная), γ — цепочка из терминальных символов.

В контекстной грамматике каждое правило $\alpha x \beta \Rightarrow \alpha \gamma \beta$ имеет *контекст*: цепочки α и β. Можно сказать иначе. В КС-грамматике подстановки $\alpha x \beta \Rightarrow \alpha \gamma \beta$ возможны при любых α и β, в контекстной грамматике — только при некоторых (в определенном контексте).

В естественных языках контекст играет существенную роль. Языки программирования стараются делать контекстно-свободными.

[21)] Вычисления проводились для всех a_0 вплоть до значений порядка 10^{12}.

С точки зрения «неразрешимостей» наиболее удобны *неукорачивающие грамматики*, у которых правые части всех подстановок не короче левых. В таких грамматиках проблема эквивалентности слов всегда разрешима, потому что длины цепочек преобразований только возрастают, в силу чего возможных цепочек, для заданных слов, — конечное число, и поэтому их можно эффективно перебрать [22)].

Вообще надо отметить, что неразрешимость проблемы эквивалентности слов на микроскопическом уровне как раз возникает из-за возможности сколь угодно длинных цепочек вывода. Если слова α и β эквивалентны, то имеется преобразование α в β конечной длины. Но оценки сверху этой длины принципиально нет — в противном случае задача легко решалась бы. Для ответа на вопрос об эквивалентности α и β было бы достаточно перебрать конечное число цепочек.

Поиск в бесконечном лабиринте. Преобразования одних слов в другие естественно интерпретируются как доказательства, т. е. логические пути, ведущие от аксиом к теоремам. Такой поиск удобно мыслить как поиск в бесконечном лабиринте, или бесконечном графе, в котором вершины соответствуют разным словам, а связывающие ребра имеются в тех случаях, когда одно слово получается из другого с помощью одной подстановки. *Системам Туэ* будут отвечать неориентированные графы, *системам Поста* — ориентированные.

Неразрешимым ситуациям (теориям) будут отвечать графы, имеющие сколь угодно длинные минимальные пути, связывающие слова априори ограниченной длины. В таком взгляде на проблему нет ничего нового по сути, но геометрический эквивалент помогает иногда образно мыслить.

4.8. Теория и практика

В неразрешимых теориях типа арифметики у коротких теорем существуют сколь угодно длинные доказательства, которые в компьютерный век дают о себе знать, — и это становится проблемой. *Длинные доказательства теряют убедительность.* Из-за необозримости,

[22)] При нестрогом возрастании цепочки формально могут периодически повторяться. Аргументация насчет «конечности» приобретает силу после удаления «периодических кусков».

несоответствия человеческому стилю мышления, наконец, из-за ошибок программирования и сбоев вычислительных процессов.

Хрестоматийным примером может служить «решение» знаменитой *проблемы четырех красок*[23], предложенное в 1977 году *Аппелем и Хакеном*. История в свое время приобрела скандальную известность в связи с невероятным объемом доказательства, включавшего трудно читаемый текст, несметные диаграммы и 1200 часов компьютерного счета[24]. Проверить было немыслимо, да и кто бы взялся? С другой стороны, трудно было игнорировать декларацию о решении задачи, которая фигурировала в одних списках с теоремой Ферма. Поэтому, из вежливости, сначала объявили, что задача решена. Потом в текстовой части обнаружились «проколы», кое-как их выправили (вроде бы), но история так и осталась во взвешенном состоянии.

Есть и другие истории подобного рода. Может быть, менее эффектные, но длина доказательств, так или иначе, становится параметром, который способен перечеркнуть успех. Соответственно, довольно бурно развиваются исследования сложности алгоритмов, что, по сути, есть оборотная сторона рассматриваемой проблемы.

Вопросы сложности вычислений планируется рассмотреть в другом томе, но здесь уместно обратить внимание на некоторые моменты общего характера.

Достаточно популярна тематика, связанная с *теоремами ускорения*. В части, касающейся длины доказательств, представляют интерес результаты о сокращении «длины» при добавлении к теории независимых аксиом[25]. В принципе, это представляется естественным, если не говорить о том, что от добавления постулатов ждут обычно новых теорем, а не совершенствования старых доказательств. Последнее иногда кажется неожиданным.

Несколько иной ракурс образуют *теоремы ускорения алгоритмов*, история которых началась со статей *Блюма*[26], хотя и до него были публикации в этом направлении.

---

[23] Предположение о возможности раскрасить вершины любого плоского графа (не имеющего пересекающихся ребер) четырьмя красками так, что любые две смежные (соединенные ребром) вершины окрашены в разный цвет.

[24] См.: *Appel K., Haken W.* Every Planar Map Is Four Colorable // Contemporary Mathematics. Providence (R. I.): Amer. Math. Soc., 1989. **98**, а также: *Thomas R.* An Update on the Four-Color Theorem // N. Amer. Math. Soc. 1998. **45**. № 7. P. 848–859.

[25] См. [15], а также статью *Эренфойхта* и *Мыцельского* в [24].

[26] Статьи *Блюма* имеются в сборнике переводов [22].

Сам факт возможности ускорения счета достаточно тривиален. Какова бы ни была машина Тьюринга, существует другая машина с бóльшим алфавитом, которая кодирует группы символов одним символом, за счет чего быстрее считает. На этом пути, однако, есть ограничения. Существуют функции $f(x)$, длина вычисления $N(x)$ которых не может быть сделана меньше $\sqrt{N(x)}$. В то же время есть функции другого типа: если программа «$N(x)$» вычисляет $f(x)$ за $N(x)$ шагов, то существует другая программа, вычисляющая ту же функцию за $M(x)$ шагов, причем $M(x)^{M(x)} \leqslant N(x)$, т. е. ускорение больше экспоненциального. Подробности с дополнительными ссылками можно найти у *Блюма* в сборнике переводов [24].

Беда заключается в том, что подобного сорта результаты обычно излагаются «нейтрально» — с предоставлением читателю возможности делать выводы самостоятельно. В итоге возникают некоторые перехлесты. Для приведения ситуации в норму полезно отметить следующее. *Теорема Блюма* к практике разработки алгоритмов не имеет никакого отношения. Речь идет, скорее, о патологических конструкциях, которые выявляют принципиальные возможности и ограничения. Далее. Без ответа остается обычно «убийственный» вопрос: что будет, если программу «$M(x)$» снова ускорить, и так до бесконечности? Во-первых, *переход к программе (поиск) «$M(x)$» — алгоритмически неразрешимая задача*[27]. Во-вторых, если «$N(x)$» вычисляет функцию $f(x) \equiv 0$, в чем, вообще говоря, алгоритмически убедиться невозможно, то существование ряда

$$\ldots \leqslant M_2(x)^{M_2(x)} \leqslant M_1(x)^{M_1(x)} \leqslant N(x)$$

вполне естественно. Функцию можно вычислить за один шаг, но это остается за семью печатями.

На другом полюсе группируются факты иного сорта.

4.8.1. Теорема (Блюм). *По любой общерекурсивной функции g можно построить общерекурсивную функцию f, принимающую значения 0 и 1, вычисление которой невозможно менее чем за $g(x)$ шагов для бесконечного числа значений x.*

[27] Программа «$M(x)$» существует, но как ее найти — в общем случае не ясно.

Это совсем простой результат, который до некоторой степени раскрывает внутреннюю кухню и показывает, что оценки времени счета могут не зависеть от используемой машины.

◀ *Доказательство.* Пусть

$$f_1, \ldots, f_n \ldots, M_1, \ldots, M_n \ldots,$$

— перечисления, соответственно, частично рекурсивных функций и машин Тьюринга, а $Z_1, \ldots, Z_n \ldots$ — перечисление пар $\{f_p, M_q\}$ (машина M_q вычисляет функцию f_p).

Искомая функция $f(x)$ строится диагональным методом. Если Z_x на входе x останавливается менее чем за $g(x)$ шагов, полагаем $f(x) = 1$. В противном случае $f(x) = 0$. ▶

Все эти результаты показывают, что попытки связать понятие сложности функций с длиной вычислительных программ и определить затем случайность как процесс бесконечной сложности (*Колмогоров*, *Мартин-Лёф*), — сопряжены с принципиальными трудностями.

В данной тематике заслуживает упоминания также нашумевшая PCP-теорема, в рекламных вариантах формулируемая примерно так. *Существует способ записи математических доказательств, при котором проверка их правильности сводится к анализу нескольких случайно выбранных мест, число которых не зависит от длины исходного доказательства.* (!)

Ссылки не даются специально по причине, которую имело бы смысл сделать общезначимой. Наличие Интернета принципиально изменило информационное поле. Набрав в поисковой машине «PCP-теорема», любой пользователь через несколько секунд получает массу адресов, по которым имеется информация, в том числе существенно более свежая, чем можно указать в книге. По-видимому, настало время пересмотреть традиционные требования к ссылочной части. Разумеется, здесь есть поле для обсуждения.

Глава 5

Математическая логика

Трагедия математической логики — в неудобоваримости формы. Нередко думается: «уж лучше бы писали на ассемблере».

При усложнении объектов изучения — от физики к экономике — теория расплывается. Логика изучает язык и каналы движения мысли, но «расплываться» нельзя, ибо главная идея как раз в строгости. На прицеле теория безошибочных рассуждений, которую необходимо создать из лингвистического хаоса. При несовершенной бдительности. Инерциально двигаясь теми же ментальными каналами. Тем же штатом сотрудников, который наделал массу ошибок в других областях.

5.1. В чем состоит миссия

Если говорить о решении конкретных математических задач, то логика больше мешает, чем помогает [1], — ибо задумывалась как *метаматематическая* дисциплина, призванная наблюдать математику извне. В этом ее главная задача. Не способствовать доказательству теорем, а «орлиным взглядом» оценить сам процесс обоснования. Разобраться в принципиальных возможностях и ограничениях.

Поэтому когда теория релейно-контактных схем начинает выдаваться за приложение матлогики, это меняет акценты. Или, скажем, развивается автоматическое доказательство теорем в различных областях [25], что очень интересно само по себе, но с «миссией» все же не коррелирует, хотя диалектически — дает опору. Технические задачи в результате путаются с философскими при отсутствии подходящей интонации. Стиль и ракурс направляют аудиторию «в никуда».

Речь, конечно, не о переходе в другую крайность. Помимо высокой миссии, матлогика — это еще и язык, представляющий

[1] Так же как обычная грамматика — изучению разговорного языка.

самостоятельную ценность и плодоносящий совершенно в неожиданных секторах, вплоть до ментально-психологических. Плодоносящий глубинно и неуловимо, что к «релейно-контактным» аргументам никакого отношения не имеет. Но очень важно не загубить этот язык, омертвляя его излишней строгостью и вычурностью. Поэтому любой шаг в направлении доступности и упрощения здесь представляется благом.

Что касается нижеследующего текста, в главе преследуется скромная цель — дать самое общее представление о тех аспектах математической логики, которые соприкасаются с вопросами доказуемости в избранном ракурсе изложения.

5.2. Переменные, связки и функции

Исходным материалом *двузначной логики* являются переменные $x, y, z \ldots$, принимающие одно из двух значений: $\{1, 0\}$ либо {*истина* (И), *ложь* (Л)}. Цифровой вариант $\{1, 0\}$ выглядит симпатичнее, хотя «кому как».

На том же уровне «первичности» — *логические связки*:

$\bar{}$ (*отрицание «не»*), $\vee$ (*или*), $\wedge$ (*и*), $\rightarrow$ (*следует*),

которые являются функциями, принимающими, как и аргументы, одно из двух значений, 1 или 0.

• Для *отрицания* наряду с «чертой сверху» используется также знак $\neg$: $\bar{x} = \neg x$ означает «не x», т. е. $\bar{x} = 0$, если $x = 1$, и наоборот.

• Связку $\vee$ называют *дизъюнкцией*; $x \vee y$ («x *или* y») — это функция двух переменных, равная 1, если хотя бы одна переменная равна 1, и равная 0 в противном случае.

Точнее говоря, *дизъюнкция* — есть «x, *или* y, или то и другое вместе». Это к вопросу о расплывчатости обычного языка. За «или» нет четко определенного значения. *Во вторник или в среду? Через месяц или через неделю? Или тебе до лампочки? Поищи в шкафу, на столе или у себя в карманах.*

• Функция $x \wedge y$ («x *и* y»), равная 1, если $x = y = 1$, и равная 0 в противном случае, называется *конъюнкцией*; эквивалентные обозначения: $x\&y$ либо $x \cdot y$, и даже xy.

• *Импликация* $x \to y$ («*из* x *следует* y», «*если* x, *то* y»)[2] как функция двух переменных всюду принимает значение 1 за исключением случая $x = 1$, $y = 0$, где $x \to y$ равна 0. Другими словами, из «истины» не может следовать «ложь», все остальное — возможно.

Конъюнкция и дизъюнкция часто путаются в голове. Англоязычному миру легче, там знак & привычен, поскольку используется вместо «and» даже в обычном письме. На территории России приходится искать другие выходы из положения. Кому-то помогает аналогия очертаний $\vee$ со знаком объединения множеств $\cup$, аналогично с $\wedge$ и $\cap$, — см. следующий раздел.

Более кардинально проблему решает переход на знаки «$\cdot$» (либо «$\times$») и «+». На игровом поле $\{1, 0\}$ конъюнкция — это в чистом виде умножение $x \cdot y$. С дизъюнкцией несколько сложнее. Очевидно,

$$x \vee y = x + y - x \cdot y = \max\{x, y\}, \tag{5.1}$$

но это громоздко. Если же вместо (5.1) писать $x + y$, наполняя знак «+» новым содержанием, ситуация упрощается. При этом важно, что легко проверяемый дистрибутивный закон

$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$$

обретает привычную форму

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Как в арифметике с помощью умножения и сложения выписываются сложные формулы, так и в логике комбинации связок позволяют задавать n-местные *логические функции* $\varphi(x_1, \ldots, x_n)$. Например,

$$\varphi(x, y, z) = (x + y) \cdot \overline{(y \to z)}.$$

Без импликации можно обойтись, поскольку

$$u \to v = u \cdot v + \overline{u} \cdot v + \overline{u} \cdot \overline{v}.$$

[2] Надо признать, что импликация, мягко говоря, не соответствует обыденному пониманию «если x, то y».

Обойтись можно и без многих других связок. Любая n-местная логическая функция $\varphi(x_1, \ldots, x_n)$ записывается с помощью (*конъюнкций, дизъюнкций и отрицаний*) в *дизъюнктивной нормальной форме*, т. е. в виде суммы произведений (дизъюнкции конъюнкций) переменных или их отрицаний. Например,

$$x \cdot y \cdot z + x \cdot \bar{y} \cdot z + \bar{x} \cdot y \cdot \bar{z} = x \cdot z + \bar{x} \cdot y \cdot \bar{z}. \qquad (5.2)$$

Существование дизъюнктивной формы представления устанавливается просто. Любая логическая функция $\varphi(x_1, \ldots, x_n)$ может считаться заданной на 2^n вершинах n-мерного куба

$$[0, 1] \times \ldots \times [0, 1]$$

и принимающей в каждой вершине значение 0 или 1. В результате оказывается возможным представление

$$\varphi(x_1, \ldots, x_n) = \sum_{k=1}^{2^n} \varphi_k(x_1, \ldots, x_n), \qquad (5.3)$$

где каждая функция $\varphi_k(x_1, \ldots, x_n)$ принимает значение 1 в k-й вершине куба, и значение 0 — в остальных вершинах, а в сумме (5.3) присутствуют φ_k только с теми номерами вершин, в которых $\varphi = 1$. Понятно, что $\varphi_k(x_1, \ldots, x_n)$ представимы в виде произведения переменных x_i или их отрицаний $\bar{x}_j$.

Скажем, $xyz = 1$ в единственном варианте $x = y = z = 1$, а $x\bar{y}z = 1$ только при условии $x = z = 1$, $y = 0$. Так можно перебрать все вершины.

Указанная запись, как правило, может быть приведена затем к более экономной форме по типу (5.2), на базе различных формул сокращения. Например, $x + \bar{x} = 1$ (*закон исключения третьего*).

Другой стандарт — *конъюнктивная нормальная форма*, в которой любая функция представляется в виде произведения сумм переменных или их отрицаний. Например,

$$(\bar{x} + y + z) \cdot (\bar{x} + \bar{y} + z) \cdot (x + \bar{y} + \bar{z}) \cdot (x + y + z).$$

Существование конъюнктивной формы легко устанавливается аналогично предыдущему. Логическую функцию $\varphi(x_1, \ldots, x_n)$, заданную в вершинах куба

$[0, 1] \times \ldots \times [0, 1]$, можно представить в виде произведения

$$\varphi(x_1, \ldots, x_n) = \prod_{k=1}^{2^n} \psi_k(x_1, \ldots, x_n), \tag{5.4}$$

где каждая функция $\psi_k(x_1, \ldots, x_n)$ принимает значение 0 в k-й вершине куба, и значение 1 — в остальных вершинах. Понятно, что $\psi_k(x_1, \ldots, x_n)$ представимы в виде суммы (дизъюнкции) переменных x_i или их отрицаний $\bar{x}_j$. Запись (5.4), конечно, не экономна, и число сомножителей может быть значительно уменьшено, если нулевые вершины объединяются в грани. Например, дизъюнкция $x_1 + \ldots + \bar{x}_n$, не содержащая k переменных x_j, обнуляется в вершинах k-грани и заменяет в (5.4) сразу 2^k сомножителей.

5.3. Булева алгебра

В рамках матлогики булеву алгебру нередко представляют как вторичную науку, у которой кроме обслуживания логики нет другого предназначения. Не пытаясь выяснить, кто больше тянет одеяло на себя, заметим, что у булевой алгебры не меньше оснований аналогично смотреть на логику.

Приземляя тему, удобнее всего говорить о множествах, как о наиболее привычных объектах. Есть множество E и некоторая система его подмножеств $\mathscr{E}$ с обычными операциями объединения $(x \cup y)$, пересечения $(x \cap y)$, дополнения $(\bar{x} = E \backslash x)$ и включения $(x \supset y)$. Множества обозначаются малыми буквами для поддержания ассоциации с предыдущим.

Если $\mathscr{E}$ состоит всего из двух подмножеств, $\mathscr{E} = \{\varnothing, E\}$, и переменные $x, y, \ldots$ принимают значения из $\{\varnothing, E\}$, — возникает ситуация, полностью аналогичная (*изоморфная*) структуре из предыдущего раздела. Соответствия достаточно очевидны:

$$x = 1 \Leftrightarrow x = E, \quad x = 0 \Leftrightarrow x = \varnothing,$$

$$\cup \Leftrightarrow \vee, \quad \cap \Leftrightarrow \wedge, \quad \supset \Leftrightarrow \rightarrow,$$

наконец, «*дополнение* $\Leftrightarrow$ *отрицание*».

Для психологии восприятия предпочтительна замена терминологии и обозначений, «$\cup \Rightarrow +$», «$\cap \Rightarrow \times$», что в «логическом варианте» уже было сделано. Конечно, «сумма» и «произведение»

для множеств могут показаться неудачными понятиями, — но все зависит от контекста. Там, где приходится объединять множества и складывать числа *рядом*, — удобнее разные знаки и названия. Обозначения $\cap$, $\cup$ «не мешают» и в том случае, когда в поле зрения попадают всего два-три множества. Но когда формулы пестрят знаками $\cup$, $\cap$, — получается каша.

Так или иначе, в *булевой алгебре* рассматривается структура $\mathscr{E}$ с операциями $\{+, \times, \bar{}, \supset\}$, которые не выводят из $\mathscr{E}$ и обладают следующими свойствами (очевидными при теоретико-множественной интерпретации):

- *Коммутативность и ассоциативность сложения и умножения*[3]:

$$x + y = y + x, \quad xy = yx;$$

$$(x + y) + z = x + (y + z), \quad (xy)z = x(yz).$$

- *Идемпотентные законы*:

$$x + x = x, \quad xx = x \qquad (A \cup A = A, \quad A \cap A = A).$$

- *Дистрибутивные законы*[4]:

$$\begin{aligned} &(x + y)z = xz + yz && \{(A \cup B) \cap C = (A \cap C) \cup (B \cap C)\}, \\ &(xy) + z = (x + z)(y + z) && \{(A \cap B) \cup C = (A \cup C) \cap (B \cup C)\}. \end{aligned} \tag{5.5}$$

Второй дистрибутивный закон получается из первого рокировкой знаков «+» и «·», т. е. в булевой алгебре операции сложения и умножения до некоторой степени симметричны. В арифметике это не так, и потому аксиома (5.5) вызывает дискомфорт. Ситуацию усугубляет привычка точку «·» не писать (или не замечать). Поэтому запись

$$(x \times y) + z = (x + z) \times (y + z)$$

вместо левой в (5.5) воспринимается легче.

- *Законы поглощения*:

$$x + xy = x, \quad x(x + y) = x.$$

- *Булева алгебра предполагает существование в $\mathscr{E}$ нуля* $(0 \Leftrightarrow \varnothing)$ *и единицы* $(1 \Leftrightarrow E)$:

$$x + 0 = x, \quad x \cdot 0 = 0, \qquad x + 1 = 1, \quad x \cdot 1 = x.$$

---

[3] Знак умножения (точка), как правило, опускается.

[4] Обратим внимание, насколько «$\cup$, $\cap$»-язык неудобен для восприятия. По этой причине теоретико-множественные иллюстрации далее опускаются, в основном.

• *Свойства операции отрицания/дополнения*:

$$\bar{\bar{x}} = x, \quad \bar{0} = 1, \quad \bar{1} = 0,$$

$$x + \bar{x} = 1, \quad x \cdot \bar{x} = 0,$$

$$\overline{x + y} = \bar{x}\bar{y}, \quad \overline{xy} = \bar{x} + \bar{y} \quad (\textit{правила де Моргана}).$$

Далее можно выписать еще полстраницы аксиом для отношения $\supset$, воспроизводя свойства обычного знака «включения».

Все это вместе взятое и есть *булева алгебра*. Поскольку перечисленные свойства (аксиомы) не независимы, громоздкое основание может быть сильно ужато, причем — разными способами. Поэтому в литературе встречаются различные определения, сводящиеся друг к другу.

Из *правил де Моргана*, например, следует, что можно обойтись одним умножением либо, наоборот, одним сложением, — но при сохранении отрицания (дополнения). Другими словами, для описания любых логических функций достаточны две базовые связки, «дизъюнкция, отрицание» либо «конъюнкция, отрицание». Еще более экономны в этом отношении *штрих Шеффера* (сумма дополнений):

$$x \mid y = \bar{x} + \bar{y},$$

и *стрелка Пирса* (пересечение дополнений):

$$x \downarrow y = \bar{x} \cdot \bar{y}.$$

Каждая из этих связок в отдельности достаточна для записи любой логической функции (любой комбинации любого количества множеств).

Штрих Шеффера $x \mid y$ в логической интерпретации означает несовместимость x и y, т. е. x и y не могут быть истинны одновременно. Отрицание, конъюнкция и дизъюнкция через штрих Шеффера выражаются так:

$$\bar{x} = x \mid x, \quad x \cdot y = (x \mid y) \mid (x \mid y), \quad x + y = (x \mid x) \mid (y \mid y).$$

Принцип двойственности позволяет автоматически получать новые соотношения из имеющихся — переходом к двойственным функциям. Функция $\varphi(x_1, \ldots, x_n)$ называется *двойственной* по отношению к $\psi(x_1, \ldots, x_n)$, если

$$\varphi(x_1, \ldots, x_n) = \overline{\psi}(\bar{x}_1, \ldots, \bar{x}_n).$$

Очевидно, двойственная двойственной — есть исходная функция. Константа 1 двойственна 0, конъюнкция — дизъюнкции, что проверяется «в лоб». Отрицание самодвойственно. При желании для всех элементарных функций легко строятся двойственные.

Общий принцип перехода к двойственной функции в стандартном логическом варианте обычно формулируется так: все конъюнкции меняются на дизъюнкции, дизъюнкции — на конъюнкции, 1 на 0, 0 на 1.

При изучении матлогики возникают естественные вопросы, что и насколько нужно. Книги неохотно дают ответы на такие вопросы, и читатели после долгих мытарств самостоятельно приходят к выводу, что технические подробности им необходимы, как бухгалтеру интегралы.

С точки зрения общего образования их действительно можно пробежать вскользь. Тем более что для понимания «главных» вопросов требуются общие представления, а не частности. Речь не идет о логиках, у которых иная судьба.

5.4. Формулы, высказывания, предикаты

Стерильные модели из раздела 5.2 разрабатывались не только «из любви к искусству», но и с прицелом на изучение рассуждений. Привязка к объекту осуществляется следующим образом.

Рассуждения предполагаются состоящими из элементарных фрагментов u_j, называемых *высказываниями*, которые представляют в совокупности некое множество $U = \{u_j\}$ и могут быть либо истинными, либо ложными. Высказывания объединяются с помощью логических связок в *формулы*: $f(u_1, \ldots, u_n)$. Символы f называют *функциональными*. Формулам, каковыми в том числе считаются *константы языка*, приписываются имена (*термы*, см. далее уточнения).

Таким образом, объекты изучения в логике напоминают стандартную ситуацию. Есть аргументы и функции. Элемент «странности» заключается в том, что переменные могут принимать значения «высказываний», и потому такие переменные называют *пропозициональными*, что является шагом к терминологическому хаосу. Хотя шаг — формально оправдан наличием специфики.

Логический анализ обычно направлен на изучение той или иной предметной области — теории множеств, арифметики, теории групп. Высказывания, соответственно, констатируют свойства и взаимоотношения изучаемых объектов, например,

$$a > b, \quad \textit{число } x \textit{ простое}, \quad z < y, \quad A \subset B.$$

Все это так называемые *предикаты*.

Говоря более общим языком, *предикат* $P(x_1, \ldots, x_n)$ — это многоместное (в том числе, одноместное) отношение, которое превращается в истинное или ложное высказывание при подстановке конкретных значений переменных $\{x_1, \ldots, x_n\}$. Предикатами часто называют сами знаки отношений: $+$, $-$, $\geqslant$, $\times$.

При общетеоретическом рассмотрении предикаты записываются в виде $P_j(x_1, \ldots, x_n)$ с помощью *предикатных символов* P_j, но фактически за этим подразумеваются отношения типа $x > y$, которые удобнее воспринимать в их привычном виде, а не в форме $>(x, y)$. В то же время, скажем, отношение трех чисел $a^b = c$ иногда напрашивается быть вытянутым в строчку, и тогда за ним закрепляется какое-нибудь обозначение типа $P_{25}(a, b, c)$. Подобного рода дилеммы все время загоняют логику в тупики нелегкого выбора, в результате чего стремление к строгости оборачивается неразберихой. Но это специфика предмета.

Висящая без опоры запись $P(u_1, \ldots, u_n)$ подразумевает обычно истинность $P(u_1, \ldots, u_n)$, т. е. $P(u_1, \ldots, u_n) = 1$. Понятно, что в этом случае предикат $P(x_1, \ldots, x_n)$ представляет собой характеристическую функцию множества истинных высказываний о совокупностях $\{x_1, \ldots, x_n\}$. Вместе с тем запись *арифметических предикатов* в виде

$$P(x_1, x_2) = \{x_1 > x_2 + 3\}; \quad P(x_1, x_2, x_3) = \{x_1^5 + x_2^5 = x_3^5\}$$

напоминает о первичности интерпретации — как отношения. Стремиться здесь к четкому разграничению терминологии едва ли имеет смысл. В логике вообще проблема неисчерпаемости напрашивающихся уточнений стоит особенно остро. Поэтому, как ни в какой другой дисциплине, здесь важна гибкость и терпимость к неопределенности.

Исчисление предикатов. При переходе от исчисления высказываний к исчислению предикатов возникает дрейф терминологии, что для «вре́менных посетителей» создает большие неудобства. Предикаты $P(t_1, \ldots, t_n)$, где t_j — *термы*, называются теперь *атомарными формулами*, а просто *формулы* в новой редакции определяются как *атомарные формулы* и их комбинации с помощью *логических связок*, которые могут находиться под действием *кванторов*.

При этом *термы* понимаются несколько шире, чем было сказано выше. Переменная — терм, и если $t_1, \ldots, t_n$ термы, а f n-местная функция, то $f(t_1, \ldots, t_n)$ — также терм.

«Небольшой» порочный круг здесь шит белыми нитками, но он легко распутывается дополнительным расходом чернил. Тем не менее даже у книг, стремящихся дать четкое изложение предмета, обычно не хватает терпения на все необходимые уточнения, и каждый автор запутывает изложение, т. е. распутывает, по-своему.

Настаивать здесь на кардинальной реформе, разумеется, бессмысленно. Но параллельно традиции полезно иметь в голове какую-либо простую модель, не отягощенную универсализмом. Есть переменные и функции, которые образуются: *логическими связками*, *отношениями* (если речь идет о предметной области) *и композицией*. Функции могут принимать два значения 0, 1 и быть подверженными действию кванторов. При движении в различных теоретических направлениях подобный взгляд может уточняться, исходя из потребностей.

Кванторы. Характерной особенностью исчисления предикатов является использование кванторов: *квантора общности* $\forall x$ — «для всех x», и *квантора существования* $\exists x$ — «существует x». Область изменения x подразумевается оговоренной либо указывается,

$$\forall x \in X, \quad \exists x \in X.$$

Под $\forall x P(x)$ имеется в виду $\forall x P(x) = 1$, аналогично $\exists x P(x)$ трактуется как $\exists x P(x) = 1$. Для придания рельефности в записи могут использоваться дополнительные знаки. Например,

$$\forall x : P(x), \quad \exists (x > 1) : P(x).$$

Переход от $P(x)$ к $\forall x P(x)$ либо $\exists x P(x)$ связывает переменную x, принципиально меняя ее роль. Переменные, находящиеся под действием какого-либо квантора, называют *связанными* (*немыми*), остальные — *свободными*. *Формулы*, не содержащие свободных переменных, называются *замкнутыми*.

Замкнутые формулы представляют собой высказывания, правильные или неправильные,

$$\forall a, b : a^2 - b^2 = (a - b)(a + b), \quad \exists x : x^2 < 0.$$

Навешивание квантора, $\forall x_1 P(x_1, \ldots, x_n)$, превращает n-местный предикат $P(x_1, \ldots, x_n)$ в $(n-1)$-местный [5].

Кванторы в логике доставляют массу неприятностей, встречаясь в формулах многократно и влияя друг на друга. Скажем,

$$\boxed{\forall x P(x) \to P(y)} \tag{5.6}$$

[5] Аналогично $\sum_x f(x, y)$ превращает двуместную функцию $f(x, y)$ — в одноместную.

представляется очевидным фактом: «если отношение $P(x)$ справедливо при любом аргументе, то в $P(\cdot)$ можно подставить любой y». Но представим, что $P(x) = \exists y Q(y, x)$. Например, $P(x) = \exists y(y \neq x)$, что при подстановке в (5.6),

$$\forall x \exists y(y \neq x) \to \exists y(y \neq y),$$

приводит к глупости.

Поэтому в логике уделяется значительное внимание регламентации работы с кванторами, на чем глава не останавливается, поскольку пишется не для того, чтобы по ней предмет можно было освоить. Вообще перед серьезным изучением матлогики надо семь раз подумать, потому что любое «овладение» в определенной степени опасно, ибо пускает жизнь в другую колею.

Языки. Логика уделяет повышенное внимание средствам описания изучаемых явлений. Правда, без особого успеха. Трудности начинаются с алфавита. Казалось бы, фиксируй конечный набор *символов* (*букв*) — вот и *алфавит*. Но

$$\{a, b, c, \ldots\}, \qquad \{\forall, \neg, \vee, \wedge, \subset, \in, \vdash\}, \qquad \{(, [:]\{\})\}$$

не резон смешивать. За каждой группой знаков своя специфика, причем напрашивается дальнейшее дробление — отделение логических связок от арифметических операций. Потом буквы — одни для обозначения переменных, другие для функций, третьи для предикатов[6]. Специфику языка определяют: *константы языка*, а также функциональные и предикатные символы, — объединяемые в так называемую *сигнатуру*. Причем *константами языка* называют не обязательно конкретные числа (что не исключается), а вообще *собственные символы* — элементы множества, на котором «разворачивается сюжет» (переменные имеют право принимать значения констант языка).

Словом в алфавите $\mathbb{A}$ называют конечную последовательность символов из $\mathbb{A}$. Чтобы аморфная масса текстов стала языком, надо утрясти массу вещей: пробелы, правильные скобочные выражения, синтаксис, аксиомы и т. п. Короче, как и при создании языка программирования, надо создать *грамматику* и детально все оговорить. Но если с *алголом* есть резон довести дело до конца, иначе пар уйдет в гудок, то с логикой — такого резона нет. Все равно писанина остается на бумаге, и никто не читает дальше середины. Поэтому,

[6] Затем становится ясно, что букв все равно не хватит, и проще взять бесконечный алфавит $\{x_1, x_2, \ldots\}$.

когда «наблюдение» теряет бдительность, порыв к регламентации сходит на нет.

Удивительно, что получению и восприятию конечных результатов это не мешает, давая повод задуматься. Традиционный способ изложения предмета «от и до» — в данном случае не работает. И от него целесообразно отказаться в пользу давно существующих эталонов иного сорта. Работу компьютера, например, хорошо понимают многие специалисты, имеющие о кодах машины и других «микроскопических» подробностях весьма смутное представление (точнее, никакого). Логика же пытается рассказать о себе, начиная с «клеточного» уровня.

Примеры

- *Язык теории множеств.* Сигнатура состоит из единственного предикатного символа $\in$. Вместо $\in(x, y)$ пишут, конечно, $x \in y$. Отношение (формула) $x \subset y$ может быть записано в виде $\forall u : (u \in x \to u \in y)$.
- *Язык арифметики.* Сигнатура состоит из константы 1 и трех функциональных символов: $+$, $\times$ и функционального символа σ, обозначающего *следование*, $\sigma(n) = n + 1$.

5.5. Синтаксис и семантика

Логические исследования развиваются двумя параллельными курсами, *семантическим* и *синтаксическим*, которые то и дело криптографически пересекаются.

В семантическом русле за символами стоят реальные операции («или», «не», «для всех», «+») и объекты (числа, множества). Синтаксическое рассмотрение предмета оставляет только символы. Знаки $\forall$, $\exists$, $\vee$, $\subset$, $\times$ — превращаются в буквы, за которыми нет никакого смыслового содержания. Поэтому преобразования и выводы, базировавшиеся ранее на понимании свойств операций, теперь должны регулироваться новыми механизмами, каковыми являются различные *правила вывода* и *аксиомы*.

Операция вывода[7] обозначается знаком $\vdash$. Выражения

$$p_1, \ldots, p_n \vdash q \qquad (\textit{из } p_1, \ldots, p_n \textit{ следует } q)$$

[7] Сосуществование импликации и операции вывода часто служит источником путаницы.

называются *секвенциями*[8], а *правила вывода* записываются в форме

$$\frac{S_1, \ldots, S_m}{S},$$

что означает: «*из секвенций* $S_1, \ldots, S_m$ *следует* S».

Например,

$$\frac{p \vdash a, q \vdash b}{p, q \vdash a \wedge b} \quad (\textit{введение конъюнкции}).$$

Секвенция, находящаяся под чертой, называется *заключением*, а секвенции над чертой называются *посылками*.

«Вводить конъюнкцию» необходимо заново, потому что речь идет о синтаксисе, — содержательная часть осталась за бортом. С другой стороны, человеку трудно делать вид, что конъюнкция ему неведома. Да и жалко отказываться от наглядных соображений. Поэтому любой профессионал жонглирует синтаксическими описаниями, опираясь на семантику. Как говорится, думает одно, делает другое. Выглядит это, если не знать подоплеки, как сумасшедший дом.

Инструменты типа широко известного правила *модус поненс*,

$$\frac{x, x \to y}{y},$$

либо правила подстановки «*если функция тождественно равна* 1, *то она равна* 1 *и при конкретных значениях аргументов*» — производят на здравомыслящего, но неискушенного человека — жуткое впечатление. Слишком поздно приходит понимание, что при переходе со смыслового описания на формальное — выуживание таких банальностей необходимо. И это самая трудная часть моделирования, поскольку очевидное имеет тенденцию ускользать из-под контроля.

Переход на формальное описание — есть не что иное как перевод ситуации на язык, понятный вычислительной машине.

Что касается традиционной многоэтажности правил вывода, то от такой записи было бы желательно избавиться. Дело в том, что

[8] Запись $\vdash p$ означает «p доказуемо», а $p_1, \ldots, p_n \vdash$ — «система $p_1, \ldots, p_n$ противоречива».

матлогика в фарватере решения принципиальных проблем аксиоматизации и доказуемости нужна для придания строгости некоторым интуитивно ясным представлениям. Даже не столько «для придания», сколько — для понимания, что такую строгость можно придать.

Скажем, чтобы согласиться с существованием «цепочек доказательств», ведущих от аксиом к выводам, многим достаточно интуитивной ясности, а другим — и матлогики не хватает. Так или иначе, но формализация правил вывода — способствует прояснению сути. Возникновение же «многоэтажности» действует, скорее, в обратном направлении, создавая впечатление, что линейности рассуждения недостаточно.

Упразднить «многоэтажность», конечно, совсем легко, например, заменяя «введение конъюнкции» на

$$(p \vdash a, q \vdash b) \Rightarrow (p, q \vdash a \wedge b),$$

а также множеством других способов.

Аксиоматика и семантическое следование. В предметных областях обычно фиксируется некоторая совокупность *замкнутых формул*, называемых *аксиомами*. Выводить следствия из аксиом можно по правилам синтаксического следования — такие правила специально оговариваются (см. следующий раздел), — и тогда используется знак $\vdash$. Например, $A_1, A_2 \vdash X$ означает, что X «синтаксически» следует из A_1, A_2, где A_1, A_2 могут быть аксиомами или ранее доказанными формулами.

Семантическое следование $A_1, A_2 \models X$ означает, что X «логически» вытекает из A_1, A_2.

Соответствия

$$A_1, A_2 \vdash X \Leftrightarrow A_1, A_2 \models X$$

являются обычно предметом специального исследования, и свидетельствуют о том, насколько хорошо определена грамматика.

На основе семантического и синтаксического следования определяются два типа *теорий*. Множество замкнутых формул, которые семантически следуют из принятой системы аксиом, называют *семантической теорией*, а если следуют синтаксически — *дедуктивной*

теорией. При согласовании смыслового и грамматического следования обе теории совпадают друг с другом, что обычно оформляется «теоремами о полноте исчислений», — см. далее.

5.6. Исчисление высказываний

Логическая функция $\varphi(x_1, \ldots, x_n)$ считается *тавтологией*, или *общезначимой формулой*, если она истинна при подстановке любых конкретных высказываний $x_i = u_i$. Примеры тавтологий:

$$x + \bar{x} = 1, \quad (x \to y) \cdot (x \to \bar{y}) \to \bar{x}.$$

Это из области семантики.

Продемонстрируем теперь фундамент синтаксического подхода, чтобы «взглянуть и забыть». Аппарат исчисления высказываний составляют *правила вывода* (ниже приводится почти половина от стандартного набора, остальная часть выглядит аналогично):

$$\frac{p \vdash a;\ q \vdash b}{p, q \vdash a \wedge b} \quad (\textit{введение конъюнкции});$$

$$\frac{p \vdash a}{p \vdash a \vee b};\quad \frac{p \vdash b}{p \vdash a \vee b} \quad (\textit{введение дизъюнкции});$$

$$\frac{p, q \vdash a \wedge b}{p \vdash a};\quad \frac{p, q \vdash a \wedge b}{p \vdash b} \quad (\textit{удаление } \wedge);$$

$$\frac{p, q \vdash}{p \vdash \neg q} \quad (\textit{введение отрицания});$$

$$\frac{p \vdash a;\ q \vdash \neg a}{p, q \vdash} \quad (\textit{сведение к противоречию});$$

$$\frac{p, a, b, q \vdash c}{p, b, a, q \vdash c} \quad (\textit{перестановка}).$$

Реальные списки исполняются готическим шрифтом, выглядят более солидно и сопровождаются расстановкой многочисленных акцентов.

Естественно, возникает вопрос, насколько хороши дозволенные средства. Все ли истинное доказывается, и все ли доказуемое истинно? Ответ — «да» на оба вопроса, что, безусловно, является теоремой (*о полноте теории*), но едва ли способно вызвать интерес.

Доказательство сводится к рутинной проверке, которая на смысловом уровне тривиальна, и в некотором роде заставляет читателя

ломиться в открытую дверь, — а время от времени вычеркивать из головы информацию о логических связках (чтобы получить удовольствие) не так просто.

Вообще говоря, исчисление высказываний, охватывающее общезначимые формулы, *само по себе* ценности не представляет, поскольку лишь запутывает легко решаемую задачу проверки истинности логических функций. Но это ступенька к исчислению предикатов, в том числе — предметных, таких как арифметика.

Итак, как бы там ни было, при формализации математических теорий на базе логики высказываний семантика игнорируется. *Теоремы* трактуются как формулы, которые могут быть выведены по определенным правилам, составляющим *аксиоматику теории*. Примером может служить правило *модус поненс* (*modus ponens*): «если x и $x \to y$, то y», — входящее обычно в любую аксиоматику.

5.7. Языки первого уровня

Исчисление предикатов, в отличие от исчисления высказываний, допускает использование в *языке первого уровня* кванторов $\forall$ и $\exists$. В то же время, ввиду взаимозаменяемости типа

$$\forall x : P(x) = 0 \Leftrightarrow \neg\exists x : P(x) \neq 0,$$

в литературе встречаются разные варианты определений.

Языки первого уровня (*порядка*) подразумевают использование кванторов по отношению к переменным. В *исчислениях второго порядка*[9] допускается применение кванторов по предикатам типа $\forall P : P(x) = 0$. Когда речь идет просто об исчислении предикатов, имеется в виду «первый уровень».

Для грамматических манипуляций с предикатами конструируется синтаксис (формальные правила вывода, с которыми можно ознакомиться по любому курсу математической логики [21, 26]). Как и в исчислении высказываний, здесь возникает тот же вопрос, насколько хороши дозволенные средства. Все ли истинное доказывается, и все ли доказуемое истинно? Ответ — снова «да», но это уже более сложная теорема *о полноте исчисления предикатов*[10].

[9] Остающихся, как правило, вне поля зрения.

[10] Принадлежащая Гёделю, а в полном объеме (для произвольной сигнатуры) — А. И. Мальцеву.

(!) В *теоремах о полноте* есть два аспекта. Первый из них наиболее важен и совсем прост. *Пока истинность определяется конструктивно* на основе семантического следования — исчисление предикатов заведомо будет полным, и вообще, дидактическая теория будет совпадать с семантической. Вопрос лишь в том, как надлежащим образом определить грамматику (синтаксис). Принципиальное существование подходящих правил вывода следует из *тезиса Чёрча* (или *Тьюринга*), ибо конструктивная основа как раз предполагает возможность формальной символьной алгоритмизации. Другими словами, «полный» синтаксис — это язык программирования.

Другой аспект — это трудоемкая рутина, заключающаяся в построении такого языка, т. е. в указании конкретных правил вывода и в обосновании их «полноты». Для понимания общих вопросов это не так существенно. Для автоматического доказательства теорем с помощью компьютера, разумеется, важно.

Представления о полноте исчисления предикатов на практике сталкиваются с разнородными ситуациями. Если переменные в языке могут принимать ограниченное количество значений, то проверка истинности любой формулы сводится к перебору, всегда приводящему к однозначному ответу. При «хорошо заданной грамматике» то же самое устанавливается синтаксически, — и это вполне ожидаемо.

Интуитивная неясность возникает, если переменные могут принимать бесконечно много значений — в арифметике, например. Однако фактически, с точки зрения полноты, ничего не меняется. Какие-то формулы могут быть доказаны «логически» (с опорой на индукцию и перебор) — и то же самое может быть проделано синтаксически, при «хорошей грамматике». В этом, собственно, и заключается полнота синтаксиса — в способности воспроизводить семантику на формальном языке. Та же часть формул, истинность которых не может быть доказана «логически», не распознается и формально.

Вот еще один из вариантов *Гёделя теоремы о полноте*.

5.7.1. Теорема. *Если формула* $\neg f$ *недоказуема в исчислении предикатов, то* f *выполнима в* $\mathbb{N}$.

В проекции на диофантову тематику это означает очевидное:

$$\text{если } \exists\, x : P(x) = 0 \text{ недоказуемо, то } \forall\, x : P(x) \neq 0.$$

Полнота исчисления предикатов никак не облегчает жизнь в отношении разрешимости.

5.7.2. Теорема Чёрча. *Исчисление предикатов неразрешимо.*

Другими словами, существуют замкнутые формулы, истинность которых не определяется ни логически, ни синтаксически.

Если речь идет об *арифметике Пеано*, то теорема 5.7.2 — элементарное следствие *теоремы Гёделя*. Но теорема Чёрча справедлива также в чисто логическом исполнении — без подключения предметных областей. На фоне неразрешимости *проблемы эквивалентности слов* — факт в принципе понятный, но для утряски деталей необходимо обращаться к аксиоматике исчисления предикатов, чего не хочется делать под предлогом бережного отношения к читателям.

5.8. Интерпретации и модели

Напомним, что *сигнатурой* языка называют часть алфавита, которая включает *константы языка*, а также функциональные и предикатные символы.

Интерпретация языка — есть преобразование φ множества C *констант языка* в некоторое множество M, сопоставляющее функциональным символам [11] f над C — функции f_φ над M, принимающие значения 0 или 1. При этом под $f \Rightarrow f_\varphi$ подразумевается

$$\varphi[f(t_1, \ldots, t_n)] = f_\varphi(t_{1\varphi}, \ldots, t_{n\varphi})$$

с сохранением соответствия между композициями функций и соблюдением обычных «правил истинности» для логических связок.

Все это находится в рамках стандартной идеологии, когда изучаемый предмет переводится в другую область, где анализ оказывается проще и эффективнее, или хотя бы дает выигрыш в некоторых отношениях.

Комплексным числам сопоставляются векторы на плоскости, сложению и умножению — соответствующие векторные операции, — и «дышать» отчасти становится легче. Такого сорта примерами разного масштаба математика пестрит. Схематично это выглядит обычно как взаимно однозначное соответствие между

[11] Имеется в виду понятие функции в рамках исчисления предикатов.

двумя множествами, $\boxed{A \rightleftarrows B}$, с таким же соответствием между операциями в A и B. В данном случае ситуация похожа, но иная.

Специфика интерпретаций в логике состоит в наполнении «смыслового вакуума» разными способами, которые могут отличаться друг от друга. Любой язык, как правило, создается сначала под содержательную теорию. Но потом можно оставить от языка только символы и попробовать наполнить их другим смыслом. Это и рождает *интерпретацию.*

Повороты $\{a, b, \ldots\}$ самосовмещения, скажем, тетраэдра характеризуются наличием тождественного поворота e, обратного поворота — для каждого $x \in \{a, b, \ldots\}$, принадлежностью $\{a, b, \ldots\}$ последовательности двух поворотов $x \otimes y$, и ассоциативностью введенной операции $\otimes$.

Если теперь отвлечься от тетраэдра, остается общее определение *группы*, куда помещаются различные *интерпретации*: группы матриц, преобразования Лоренца и т. п.

При заданной *интерпретации* подстановка в $f_\varphi(\ldots)$ конкретных значений переменных дает «истину» или «ложь» — 1 или 0. Любые *замкнутые формулы* [12] являются, по сути, высказываниями и также принимают значения 1 или 0.

Функцию f называют *общезначимой*, если $f_\varphi(\ldots) \equiv 1$ при любой интерпретации φ, и — *выполнимой*, если существует интерпретация, в которой $f_\varphi(\ldots) = 1$ при некоторых значениях переменных.

5.8.1. Определение. *Моделью множества A замкнутых формул называется интерпретация, в которой истинны все формулы из A.*

Множество A замкнутых формул может быть, в частности, совокупностью аксиом, из которых выводятся другие замкнутые формулы, $A \vdash f$, и такой процесс расширяет A до *теории* T. Причем в силу полноты исчисления предикатов семантическое ($\models$) и синтаксическое ($\vdash$) расширение дает в итоге одинаковый результат. Если говорить точнее, то *теория* T — это наименьшее множество формул, содержащее систему аксиом и замкнутое относительно правил вывода. *Теория* T называется *полной*, если любая замкнутая формула f либо сама, либо ее отрицание $\neg f$ — принадлежит T.

[12] Не содержащие свободных переменных.

Множество A замкнутых формул считается *непротиворечивым*, если из него нельзя вывести два противоположных утверждения f и $\neg f$.

5.8.2. Теорема. *Множество A замкнутых формул, имеющее модель, непротиворечиво.*

◄ В предположении противного существует такое f, что

$$A \vdash f \quad \text{и} \quad A \vdash \neg f.$$

Но тогда, в силу полноты исчисления предикатов,

$$A \models f \quad \text{и} \quad A \models \neg f,$$

что невозможно по определению модели. ►

Баланс силы и слабости теоремы 5.8.2 демонстрирует пример ошибочной на вид формулы

$$\exists x : P(x) \to \forall x : P(x),$$

которая непротиворечива, потому что существует модель, в которой x может принимать единственное значение, и там формула верна.

5.8.3. Теорема. *Если аксиоматизируемая теория полна и непротиворечива, то она разрешима.*

◄ Из предположений вытекает перечислимость всех формул языка теории. Фильтруя это перечисление $f_1, f_2, \ldots$ и оставляя только формулы, являющиеся доказательствами, получаем перечень доказательств $p_1, p_2, \ldots$, а значит, и теорем. Для любой формулы f в этом перечне найдется, в силу полноты теории, либо сама f, либо ее отрицание $\neg f$. Конечный поиск в списке $p_1, p_2, \ldots$ дает, таким образом, решающую процедуру. ►

Как правило, особо выделяют *теории с равенством*, характеризуемые включением аксиом равенства. При этом интерпретация теории называется *нормальной*, если равенство интерпретируется как совпадение элементов.

Требование интерпретировать равенства «как равенства» — не так глупо, как может показаться. Многочисленные *двойственные* интерпретации свидетельствуют о продуктивности смены точек зрения. Например, любое тождество в $\mathbb{N}$ на основе операций $+$, min, max — остается истинным при замене перечисленных операций,

соответственно, на $\times$, НОД и НОК[13]. (?) Аналогичная манипуляция в обратном направлении также оставляет тождества в силе.

Теорема *Гёделя о полноте* исчисления предикатов обобщается на исчисление с равенством, и из нее извлекаются также различные следствия: *устранимость сечения* и различные *теоремы отделения*. Например, если формула, не содержащая равенства, выводима в теории с равенством, то она выводима и в теории без равенства. Либо, скажем, если формула выводима в арифметике со свободными предикатными переменными, то она выводима и в исчислении предикатов.

Теоремы компактности. В логике довольно широко используются переходы к моделям большей и меньшей мощности. От континуальных, например, — к счетным моделям, и даже конечным.

Обоснование таких переходов опирается на конечность вывода любой формулы. Модель может быть сколь угодно мощна, но только ее конечная часть может иметь отношение к доказательству отдельной теоремы. Если формула выводится в рамках некоторой системы, то она выводится и в рамках конечной подсистемы. В переводе на менее понятный язык это звучит так:

5.8.4. Теорема. *Если* $X \models f$, *то существует конечное подмножество* $S \subset X$ *замкнутых формул такое, что* $S \models f$.

Топологическая окраска термина «компактность» в определенной степени оправданна. Если «покрытие» X накрывает f, то существует конечное подпокрытие S — также накрывающее f.

В большинстве случаев, конечно, представляют интерес не подмножества для отдельных формул, а подструктуры (подмодели), годящиеся для вывода групп формул, а также всех формул теории. Конструкция таких подструктур производится по следующей схеме. В модели рассматриваемой сигнатуры берется конечное или счетное подмножество $S \subset M$, и к нему добавляются результаты применения к элементам S всех сигнатурных функций (функций и предикатов). Затем операция повторяется снова и снова. В результате получается счетное замыкание S по сигнатуре, что дает счетную модель $\mathcal{M} \subset M$.

[13] Наибольший Общий Делитель и Наименьшее Общее Кратное.

На этом пути случаются препятствия, но в основном процесс приходит к финишу без особых помех, порождая группу результатов, каждый из которых называют *теоремой Лёвенгейма—Сколема*. Ограничимся формулировкой двух вариантов.

5.8.5. Теорема. *Если счетная теория*[14] *имеет модель, то она имеет также счетную модель.*

5.8.6. Теорема. *Любое выполнимое множество формул выполнимо в некоторой счетной структуре.*

5.9. Язык арифметики

Энциклопедии омертвляют знание. Чересчур правильные определения теряют гибкость и перестают работать. Поэтому *формальные языки* целесообразно регламентировать, лишь задавая направление и уточняя детали по мере надобности.

Любой язык строится на базе того или иного *алфавита* $\mathbb{A}$, в который входят символы для обозначения переменных и вспомогательные символы типа знаков препинания. Эта «общая часть» обычно умалчивается, если речь не идет о компьютерах.

Язык L_0. Суть языка определяется специальными средствами (логические связки, кванторы, арифметические операции), допустимыми для использования. Например, *арифметический язык*

$$L_0 = \{+, \times, =, \exists\}$$

подразумевает возможность использования перечисленных (и только перечисленных) средств (*сложение*, *умножение*, *равенство и декларация существования*).

Язык L_0 позволяет записать любой полином $p(a, x)$ и делать высказывания $\exists\, x : p(a, x) = 0$, где

$$a = \{a_1, \ldots, a_k\}, \quad x = \{x_1, \ldots, x_n\},$$

откуда ясно, что *диофантовы множества* — это те и только те множества, которые могут быть выражены в языке L_0.

[14] Опирающаяся на счетную сигнатуру.

Необходимое здесь уточнение связано с использованием в определении диофантовых множеств только положительных чисел (раздел 1.11). Чтобы не выходить из области $\mathbb{N}$, но сохранить возможность появления отрицательных коэффициентов у полинома $p(a, x) = 0$, — вместо $\exists x : p(a, x) = 0$ достаточно писать $\exists x : p_1(a, x) = p_2(a, x)$, где коэффициенты полиномов p_1 и p_2 положительны.

Итак, с учетом оговорок, справедлив следующий факт.

5.9.1. Теорема. *Множество является диофантовым в том и только том случае, когда оно описывается на языке* L_0.

Таким образом, язык L_0 равносилен языку диофантовых множеств. Все, записанное с помощью L_0, — диофантово. Факт, безусловно, очевидный, но примеры здесь привносят дополнительные краски.

Примеры

- Множество A пар $\{a_1, a_2\}$, у которых a_2 делится на a_1 («a_1 делит a_2», пишут «$a_1 \mid a_2$»),

$$A \quad \Leftrightarrow \quad \exists x : a_1 x = a_2 \quad \Leftrightarrow \quad p(a, x) = a_1 x - a_2 = 0.$$

- Множество A упорядоченных пар $\{a_1 < a_2\}$,

$$A \quad \Leftrightarrow \quad \exists x : a_1 + x = a_2 \quad \Leftrightarrow \quad p(a, x) = x + a_1 - a_2 = 0.$$

  В случае $A = \{(a_1, a_2) : a_1 \leqslant a_2\}$ условие $\exists x : a_1 + x = a_2$ меняется на $\exists x : a_1 + x = a_2 + 1$.

- «Множество нечетных чисел» $\Leftrightarrow \exists x : a = 2x - 1$.

- «Множество $a \neq 2^n$» $\Leftrightarrow \exists x_1, x_2 : a = x_1(2x_2 + 1)$.

Внимательное рассмотрение примеров создает впечатление о достаточной эффективности подобной техники. Но ее возможности, конечно, ограничены. Если, например, *составные числа* легко описать параметрическим уравнением $a = (x_1 + 1)(x_2 + 1)$, то *простые числа* $a \in \Pi$ уже не ясно, как описать. Разумеется, это легко сделать на каком-нибудь более мощном языке. Например, $a \in \Pi$, если и только если

$$(a > 1) \wedge \forall\, (x_1, x_2 \leqslant a) : \{a \neq (x_1 + 1)(x_2 + 1)\}, \tag{5.7}$$

но здесь набор инструментов несколько шире, чем в L_0.

Правда, из рассмотренных выше примеров ясно, что в ассортимент L_0 можно включить знаки «больше» и «меньше», что повышает удобства L_0, но в принципе — сводится к использованию стандартного набора $\{+, \times, =, \exists\}$.

Это общая идея. Все, что выражается с помощью $\{+, \times, =, \exists\}$, можно включать в L_0. Из тех же примеров ясно, что $\{+, \times, =, \exists\}$ безболезненно дополняется операцией (свойством) «делимости» («$a \mid b$»).

Легко видеть, что в L_0 можно включить также *конъюнкцию* и *дизъюнкцию* (без расширения принципиальных возможностей языка). Действительно, если полиномиальные уравнения $P_1 = 0$ и $P_2 = 0$ выражают некие свойства в L_0, то

$$(P_1 = 0) \wedge (P_2 = 0) \Leftrightarrow P_1^2 + P_2^2 = 0,$$

$$(P_1 = 0) \vee (P_2 = 0) \Leftrightarrow P_1 P_2 = 0.$$

Знаки $\vee$, $\wedge$, в свою очередь, позволяют с удобствами выражать дополнительные возможности. Например,

$$a \neq b \Leftrightarrow (a > b) \vee (a < b).$$

Перечисленного достаточно, чтобы утверждать эквивалентность L_0 языку

$$L' = \{+, \times, =, \neq, >, \geqslant, \mid, \vee, \wedge, \exists\}.$$

Но этого все же недостаточно для (5.7), где используется *ограниченный квантор общности* $\forall_{\leqslant}$. Другое дело, что $\forall_{\leqslant}$ может оказаться — и оказывается (!) — выразимым в языке L'.

Еще один вариант записи множества простых чисел:

$$a \in \Pi \Leftrightarrow (a > 1) \wedge (\text{НОД}\{a, (a-1)!\} = 1),$$

но здесь другая «неприятность»: *наибольший общий делитель* (НОД) и факториал. Можно ли выразить эти функции с помощью L_0, — сразу неочевидно.

5.10. Арифметичность вычислимых функций

Расширение L' — с сохранением эквивалентности языку L_0 — легко осуществляется во многих направлениях. Существенно, что к языку могут добавляться любые функции, выразимые в этом языке.

Легко устанавливается, что «остаток от деления $\operatorname{rem} a/b$», «целая часть a/b» и многие другие функции — диофантовы. Для *канторовской нумерующей функции*,

$$\boldsymbol{c}(x, y) = \frac{(x + y - 2)(x + y - 1)}{2} + x$$

запись в L_0,

$$z = \boldsymbol{c}(x, y) \Leftrightarrow 2z = (x + y - 2)(x + y - 1) + 2x,$$

обеспечивает диофантовость $\boldsymbol{c}(x, y)$. Функции $x = \boldsymbol{l}(z)$, $y = \boldsymbol{r}(z)$ также оказываются диофантовыми в силу

$$x = \boldsymbol{l}(z) \Leftrightarrow \exists y : 2z = (x + y - 2)(x + y - 1) + 2x,$$
$$y = \boldsymbol{r}(z) \Leftrightarrow \exists x : 2z = (x + y - 2)(x + y - 1) + 2x.$$

Функции, диофантовость которых установлена, можно различным образом комбинировать.

5.10.1. *Суперпозиция диофантовых функций — диофантова.*

◀ Действительно, если функции $\psi, \varphi_1, \ldots, \varphi_m$ диофантовы, то и *суперпозиция*

$$\omega(x_1, \ldots, x_n) = \psi[\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_m(x_1, \ldots, x_n)]$$

диофантова:

$y = \omega(x_1, \ldots, x_n) \Leftrightarrow \exists u_1, \ldots, u_m :$

$$\{u_1 = \varphi_1(x_1, \ldots, x_n) \wedge \ldots \wedge u_m = \varphi_m(x_1, \ldots, x_n) \wedge y = \psi(u_1, \ldots, u_m)\}. \quad ▶$$

Полезным инструментом в рассматриваемой области является *функция Гёделя*

$$\Gamma(i, n) \equiv \boldsymbol{l}(n) \bmod [1 + i\boldsymbol{r}(n)], \quad \Gamma(i, n) \leqslant 1 + i\boldsymbol{r}(n), \tag{5.8}$$

восстанавливающая последовательности в следующем смысле.

5.10.2. Лемма. *Функция $\Gamma(i, n)$ обладает тем свойством, что для любой последовательности $\{a_1, \ldots, a_N\}$ существует номер n, для которого $\Gamma(i, n) = a_i$ для всех $i = 1, 2, \ldots, N$.*

Доказательство легко следует из известной в теории чисел *китайской теоремы*.

5.10.3. Китайская теорема об остатках. *Каковы бы ни были взаимно простые* $p_1, \ldots, p_n \in \mathbb{N}$ *и целые* $a_1, \ldots, a_n \in \mathbb{N}$, — *существует такое* x, *что*

$$x \equiv a_1 \bmod p_1,$$

$$x \equiv a_2 \bmod p_2,$$

$$\ldots\ldots\ldots\ldots$$

$$x \equiv a_n \bmod p_n,$$

т. е. существует x, *дающее при делении на* $p_1, \ldots, p_n$ *остатки* $a_1, \ldots, a_n$.

◀ Векторы остатков $a = \{a_1, \ldots, a_n\}$ от деления целого $x \leqslant p_1 \cdot p_2 \ldots p_n$ на $p_1, \ldots, p_n$ — все различны. В противном случае, $a' = a''$,

$$x' = \{a'_1, \ldots, a'_n\} \bmod \{p_1, \ldots, p_n\}, \quad x'' = \{a''_1, \ldots, a''_n\} \bmod \{p_1, \ldots, p_n\},$$

целое $x' - x'' < p_1 \cdot p_2 \ldots p_n$ делилось бы на $p_1 \cdot p_2 \ldots p_n$, что невозможно в силу взаимной простоты $p_1, \ldots, p_n$.

Различные наборы остатков

$$a_1 \leqslant p_1, \quad \ldots, \quad a_n \leqslant p_n$$

исчерпывают таким образом все $p_1 \cdot p_2 \ldots p_n$ возможностей, гарантируя существование подходящего $x \leqslant p_1 \cdot p_2 \ldots p_n$ для любого наперед заданного набора $a = \{a_1, \ldots, a_n\}$. ▶

Поскольку выбором достаточно большого q можно обеспечить взаимную простоту чисел

$$p_i = 1 + iq, \quad i = 1, \ldots, N,$$

получается, что любую сколь угодно длинную последовательность $\{a_1, \ldots, a_N\}$ можно закодировать всего тремя числами: x, q, N, — с простым правилом декодирования «$x \equiv a_i \bmod (1 + iq)$».

Функция (5.8) обыгрывает идею, дополняя конкретикой, связанной с канторовской нумерацией. При этом обеспечивается не только кодирование, но и диофантовость функции.

5.10.4. Теорема[15]. *В языке* $L_G = \{+, \times, =, \wedge, \exists, \forall_{\leqslant}\}$ *выразимы любые частично рекурсивные функции.*

[15] Результат по существу принадлежит Гёделю (*Gödel K.* // Monatsh. Math. und Phys. 1931. **38**. 173–198).

◄ Для доказательства достаточно проверить, что язык L_G позволяет выразить операции (1.11)–(1.15) и оператор минимизации из определения частично рекурсивной функции (раздел 1.10). Операции (1.11)–(1.13) рассматриваются совсем просто. Возможность суперпозиции установлена выше. Остается два пункта.

• *Примитивная рекурсия*:

$$\begin{cases} f(x, 0) = g(x), \\ f(x, \tau + 1) = h[x, \tau, f(x, \tau)], \end{cases}$$

где $x = \{x_1, \ldots, x_n\}$, а функции g и h диофантовы. Используя *функцию Гёделя* $\Gamma(i, n)$ для нумерации последовательности $f(x, 1), \ldots, f(x, t)$, получаем

$$y = f(x,t) \Leftrightarrow \exists u : \Big\{\exists v : \{v = \Gamma(1, u) \wedge v = g(x)\} \wedge$$

$$\wedge \forall (\tau \leqslant t) : \big\{(\tau = t) \vee \big[\exists w : w = \Gamma(\tau + 1, u) \wedge w = h[x, \tau, c(\tau, u)]\big]\big\} \wedge y = \Gamma(t, u)\Big\}.$$

• *Оператор минимизации*

$$y = \mu y\{\varphi(x; y) = 0\},$$

дающий наименьшее $y \in \mathbb{N}$, которое удовлетворяет уравнению $\varphi(x; y) = 0$, либо неопределенный, если такое y не существует, — в случае диофантовости $\varphi(x; y)$ порождает диофантову функцию в силу

$$y = \mu y\{\varphi(x; y) = 0\} \Leftrightarrow \exists z : \Big\{[\varphi(x; z) = 0] \wedge \big[\forall (t \leqslant y) : \varphi(x; t) \neq 0\big]\Big\}.$$

Использованное отношение «$\neq$», хотя и не фигурирует непосредственно в L_G, легко может быть включено в L_G (см. предыдущий раздел). ►

Главная теорема. Теорема 5.10.4 дает еще один язык для описания вычислимых функций. Однако успех этот — промежуточный. Справедлив гораздо более сильный результат.

5.10.5. Теорема. *Языки L_G и L_0 эквивалентны.*

Это трудная теорема [16], которая решает по сути *десятую проблему Гильберта*. Здесь уместно сказать о ее роли в данном контексте. Средства описания вычислимых функций и перечислимых множеств, оказывается, могут быть ужаты до чисто арифметического языка диофантовых уравнений, $L_0 = \{+, \times, =, \exists\}$, выделяющегося на общем фоне экономностью и фундаментальностью.

[16] Доказательство — в главе 6.

Экономность языка по части используемого набора инструментов важна при доказательстве общих теорем. Разнообразие инструментов — существенно в другой ситуации, когда нужно построить конкретную функцию, написать конкретную программу. С этой точки зрения представляют интерес вопросы расширения языка при сохранении эквивалентности.

Равноправие L_0 языкам *машин Тьюринга*, *нормальных алгоритмов Маркова*, *рекурсивных функций* [17] — подталкивает к отсеву лишнего. Но этому соблазну не суждено осуществиться по той же причине, по которой вилка и ложка не вытесняют друг друга. Проблема тождества слов, например, удобно решается с помощью идеологии машин Тьюринга. Последняя кажется будто специально приспособленной для решения подобного сорта задач. Гёделевская тематика удачнее схватывается диофантовым языком. Короче, разные языки в области программирования обречены на сосуществование.

5.11. Запрещенные средства

После того как установлено, что потенциала языка L_0 хватает для описания любой вычислимой функции, к L_0 можно добавлять любые алгоритмически осмысленные инструменты [18]. Но есть заведомо негодные средства: неограниченный квантор общности $\forall$, логическое «не» $\neg$, и кое-что еще.

Подозрения о негодности $\forall$ и $\neg$ возникают естественно. Если проверку истинного высказывания $\exists\, x : P(x) = 0$ алгоритмически реализует обыкновенный поиск, то проверить истинное

$$\neg\exists\, x : P(x) = 0, \quad \textit{равносильно} \quad \forall\, x : P(x) \neq 0,$$

в общем случае непонятно как.

Перевести мираж подозрения в обоснованный запрет не так просто. Спасает «тяжелая артиллерия» — существование неразрешимого уравнения (1.18), точнее говоря, неперечислимость множества Y тех y, при которых уравнение $P(x_1, \ldots, x_k) - y = 0$

[17] Все это — языки программирования, пригодные для написания вычислительных программ.

[18] Опираясь на *тезис Тьюринга* или *Чёрча*.

со специальным полиномом P не имеет решения. Но

$$y \in Y \quad \Leftrightarrow \quad \forall x : P(x) \neq y,$$

либо

$$y \in Y \quad \Leftrightarrow \quad \neg\exists x : P(x) = y,$$

и получается, что $\forall$ и $\neg$ могут выводить за пределы перечислимых (диофантовых) множеств.

(?) Совсем другая история возникает при использовании языка не для программирования (как выше), а для описания аксиоматики. Утверждениями типа [19]

$$\forall x : P_1(x) \neq 0, \quad \ldots, \quad \forall x : P_N(x) \neq 0,$$

можно дополнить обычную *аксиоматику Пеано*, и далее интересоваться последствиями [20]. Кванторы общности здесь вполне «на своем месте». С тем же успехом в поле зрения могут быть введены и другие операции.

В результате возникает то или иное русло теории доказательств, где можно придерживаться как семантической точки зрения, так и чисто синтаксической интерпретации, считая $\forall$ и другие «изыски» просто буквами и словами. В последнем варианте тексты аксиом и доказательств кодируются [21], и вся теория отображается в арифметику номеров с возвращением к машинам Тьюринга, либо рекурсивным функциям, либо диофантовым инструментам, не допускающим использования неограниченных кванторов общности.

5.12. Комментарии

• *За обилием терминов в матлогике стоят разные причины. От субъективной тяги противостоять дилетантам до объективных потребностей самой дисциплины. Как рождаются неудобоваримые языки программирования низкого уровня? Под давлением особых условий. Если, общаясь с человеком, можно рассчитывать на «додумывание», то для компьютера все должно быть недвусмысленно. Тот же дамоклов*

[19] См. обсуждение в разделе 2.1

[20] Множество доказуемых теорем расширится, но оно никогда не покроет все арифметические истины, как уже было установлено.

[21] Проводится гёделизация, например.

меч строгости висит над матлогикой, а диалектика ситуации требует еще и «человечности». Противоречия в результате искрят до ряби в глазах. Как правило, это связано с абстрактными определениями, которые пытаются учесть нюансы «на все случаи жизни». В конкретных областях бесформенные абстракции «входят в берега», и воспринимаются легко. Но для этого, как принято говорить, надо «въехать в тему».

• **Нейтральные полосы.** Между любой теорией и областью ее приложения — будь то природа или виртуальная реальность — всегда есть нейтральная полоса. Что касается физики, не говоря о бухгалтерии, то там нестыковка моделей — очевидна. Зубчатые колеса алгебраической и общей топологии тоже не вполне согласуются друг с другом. Да что угодно. Кроме, как думают многие, математической логики, которая, дескать, точно отражает изучаемые явления.

Иллюзию создают громоздкие процессы уточнений, которые никем до конца не читаются, и потому мало кто знает, что они до конца и не доводятся. Имеются в виду процессы, не замыкающиеся в самой логике, а направленные на взаимосвязь с прикладными областями. Самый удачный экспонат — геометрия, базирующаяся на постулатах Евклида, но и там внимательное изучение фундамента обнаруживает «проколы» [22].

Хотим мы того или нет, но существенную часть математики составляет разговорный язык. Замечательный инструмент — гибкий, обволакивающий, но принципиально не поддающийся точному измерению. Как в микромире теряют абсолютный смысл координата и скорость, так и слово со своими обертонами не помещается в капкан стерильных формул. Поэтому между чисто логическими моделями и их реальными прообразами всегда есть расхождение, явное или неуловимое.

[22] Это становится ясным при составлении компьютерных программ для доказательства геометрических теорем.

Глава 6

Диофантов язык и десятая проблема Гильберта

О решении 10-*й проблемы Гильберта* уже шла речь в разделе 1.11. Вопрос был вынесен на авансцену, с одной стороны, чтобы не затерялся, а с другой, — в соответствии с его значимостью для изучаемой проблематики. В данной главе рассматривается закулисная часть.

6.1. Диофантовы множества и функции

Напомним то, что уже было сказано и доказано ранее.

Множество A положительных векторов $a = \{a_1, \ldots, a_k\}$ называется диофантовым, если при любом a, и только при $a \in A$, уравнение [1]

$$p(a_1, \ldots, a_k; x_1, \ldots, x_m) = 0$$

разрешимо в целых положительных $x_1, \ldots, x_m$.

Лемма [2] **1.11.2.** *Множество $A \subset \mathbb{N}$ диофантово в том и только том случае, когда оно является множеством положительных значений некоторого полинома $P(x_1, \ldots, x_k)$.*

Диофантовы функции определяются как функции, график которых (множество пар)

$$G = \{x_1, \ldots, x_n,\ y = f(x_1, \ldots, x_n)\},$$

диофантов.

Положительность переменных $\{a, x\}$ не принципиальна и связана с техническими причинами. При желании переход от ситуации $a, x \in \mathbb{N}$ к $a, x \in \mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ осуществляется с помощью *теоремы Лагранжа* (см. раздел 1.11).

---

[1] Где p полином с целыми коэффициентами.

[2] Номер леммы дается по начальному местоположению. Там же доказательство

Что касается отрицательных коэффициентов в уравнении $p(a, x) = 0$, то все слагаемые $p(a, x)$ с отрицательными коэффициентами можно перенести в правую часть и рассматривать диофантовы уравнения $q(a, x) = s(a, x)$ с полиномами q и s, имеющими только положительные коэффициенты.

На диофантовы функции и множества удобно смотреть через призму «разрешенных» операций *арифметического языка*

$$L_0 = \{+, \times, =, \exists\},$$

допускающего для конструирования *высказываний* четыре операции: *сложение*, *умножение*, *равенство и декларацию существования.*

Теорема 5.9.1. *Множество является диофантовым в том и только том случае, когда оно описывается на языке* L_0.

С помощью L_0 легко выражаются многие функции и отношения, которые могут быть включены в ассортимент языка L_0. В результате L_0 оказывается эквивалентен (раздел 5.9) языку

$$L' = \{+, \times, =, \neq, >, \geqslant, |, \vee, \wedge, \exists\},$$

куда может быть включена масса других функций [8, 18, 19]. Но в этом расширении инструментария есть трудный шаг — включение ограниченного квантора общности $\forall_{\leqslant}$, — который необходимо сделать, чтобы пробить тоннель к перечислимым множествам. Необходимость этого шага ясна из следующего результата, полученного в разделе 5.10.

Теорема 5.10.4. *В языке*

$$L_G = \{+, \times, =, \wedge, \exists, \forall_{\leqslant}\}$$

выразимы любые частично рекурсивные функции.

Таким образом, как только $\forall_{\leqslant}$ вносится в реестр разрешенных средств, между диофантовыми уравнениями и перечислимыми множествами устанавливается прямая связь, потому что выясняется эквивалентность L_G чисто *диофантову языку* L_0. Диофантовость оказывается равносильной вычислимости. Центральный результат звучит так.

6.1.1. Теорема. *Диофантовость множества равносильна его перечислимости.*

При этом все упирается в обоснование следующего факта (доказательство в разделе 6.4).

6.1.2. Теорема. *Ограниченный квантор общности* $\forall_{\leqslant}$ *может быть выражен в языке* L_0.

Долгие годы теорема 6.1.2 была камнем преткновения. На каком-то этапе она была сведена к выразимости в L_0 показательной функции n^k — в таком виде ядро задачи и запомнилось аудитории. Окончательно проблема была решена Матиясевичем в 1969 году, ему и досталась основная слава.

Здесь имеет смысл обратить внимание на психологический аспект. Любые достижения в мире всегда являются плодом коллективных усилий. Иногда это скрыто в глубине, иногда — лежит на поверхности. В решении десятой проблемы Гильберта коллективный характер успеха очевиден. При этом заслуживает восхищения позиция Матиясевича и всей группы, принимавшей участие в покорении вершины. Взаимное уважение, минимум амбиций. Если выпячиваются какие-то результаты, то это результаты партнеров.

Обычно бывает не так. Достаточно вспомнить тяжбу Ньютона с Гуком [2] насчет закона всемирного тяготения [3)].

6.2. Неразрешимые проблемы

Диофантовы уравнения, наряду с другими средствами программирования, являются универсальным языком описания любых алгоритмически *разрешимых* задач. Это могут быть как задачи вычислительного характера, так и проблемы доказуемости тех или иных теорем на базе фиксированной аксиоматики.

Что касается *неразрешимых* задач, то их описание с помощью диофантовых уравнений не всегда возможно. Например, когда проблема сводится к неразрешимости множества, неперечислимого вместе со своим дополнением.

Способы сопоставления конкретным задачам диофантовых уравнений — рассматривались в разделе 5.10. Здесь важно добавить, что все рецепты расширения языка L_0, как рассмотренные,

[3)] Математике учат не только арифметические ошибки, но и человеческие.

так и оставленные за кадром, *имеют конструктивный характер*, т. е. *позволяют в любом конкретном случае указать подходящий полином*. В сложных ситуациях это бывает технически сложно, но всегда реализуемо.

Вот яркий пример. Множество простых чисел порождают положительные значения следующего полинома[4] от 26 переменных от a до z,

$$\begin{aligned}(k+2)\Big\{1 &- [n+l+v-y]^2\\ &- [wz+h+j-q]^2\\ &- [ai+k+1-l-i]^2\\ &- [2n+p+q+z-e]^2\\ &- [(a^2-1)l^2+1-m^2]^2\\ &- [(a^2-1)y^2+1-x^2]^2\\ &- [(gk+2g+k+1)(h+j)+h-z]^2\\ &- [e^3(e+2)(a+1)^2+1-o^2]^2\\ &- [16r^2y^4(a^2-1)+1-u^2]^2\\ &- [z+pl(a-p)+t(2ap-p^2-1)-pm]^2\\ &- [16(k+1)^3(k+2)(n+1)^2+1-f^2]^2\\ &- [q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2\\ &- [((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2\\ &- [p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2\Big\}.\end{aligned}$$

Интерпретировать результат можно так. Если каждую квадратную скобку приравнять нулю, — получится система из 14 полиномиальных уравнений. Извлекая из ее положительных решений $\{a, b, \ldots, z\}$ значения k, получаем исчерпывающий список простых чисел $\nu = k+2$, — однако, в крайне запутанном порядке.

Проблема Гольдбаха. Предположение: *«любое четное $n \geqslant 4$ представимо в виде суммы двух простых чисел»* — до сих пор не доказано (2005).

[4] *Jones J. P., Sato D., Wada H., Wiens D.* Diophantine representation of the set of prime numbers // Amer. Mathem. Monthly. 1976. **83**(6). 449–464.

Имея описанный выше полином $P(x_1, \ldots, x_m)$, перечисляющий простые числа, проблему Гольдбаха можно переформулировать как проблему разрешимости диофантова уравнения

$$(2k+2-q_1-q_2)^2+[q_1-P(x_1,\ldots,x_m)]^2+[q_2-P(y_1,\ldots,y_m)]^2=0$$

относительно $q_1, q_2, x_1, \ldots, x_m, y_1, \ldots, y_m$ при любых значениях $k \in \mathbb{N}$, что как раз соответствует значению $n = 2k+2 \geqslant 4$.

Чтобы освободиться от параметрической зависимости, надо начинать все сначала. Предположение Гольдбаха можно записать в форме:

$$\forall u \leqslant 2k-1 \;\; \exists x, y : \{[u=(x+1)(y+1)] \vee [2k+2-u=(x+1)(y+1)]\}, \quad (6.1)$$

т. е. если $n = 2k+2 = u+v$, то либо u составное число, либо v.

В разделе 6.4 описан конструктивный способ сопоставления формулам с ограниченным квантором общности полиномиальных уравнений вида

$$Q(k, x_1, \ldots, x_m) = 0,$$

разрешимых относительно $x_1, \ldots, x_m$ при тех и только тех k, которые удовлетворяют исходным формулам типа (6.1).

Предположение Гольдбаха тогда эквивалентно неразрешимости уравнения

$$Q(x_0, x_1, \ldots, x_m) = 0$$

относительно $x_0, \ldots, x_m$.

Другой пример — *теорема Ферма*: неразрешимость уравнения

$$x^n + y^n = z^n, \quad n > 2. \quad (6.2)$$

При фиксированном $n > 2$ — это, конечно, вопрос о неразрешимости диофантова уравнения. Но «при любом $n > 2$» — это уже задача о неразрешимости уравнения, куда входит показательная функция. Последняя относится к ассортименту диофантовых инструментов, поэтому уравнение (6.2) может быть переписано (конструктивно) как диофантово

$$p(x, y, z, n; x_1, \ldots, x_k) = 0,$$

но технически — это довольно обременительно.

К цели ведут следующие конструктивные шаги. В разделе 6.4 при доказательстве диофантовости показательной функции $m = n^k$ указан конкретный полином $P(m, n, k; w)$, имеющий корни $w = \{w_1, \ldots, w_q\}$ *в томм*[5] случае, когда $m = n^k$. Разрешимость (6.2) с помощью P может быть записана в полиномиальном виде:

$$\exists\, w : P^2(m_1, x, n; w) + P^2(m_2, y, n; w) + P^2(m_1 + m_2, z, n; w) = 0.$$

В качестве сложной проблемы, сводящейся к диофантову представлению, обычно указывают [14, 19] *гипотезу Римана* о нулях *дзета-функции* $\zeta(z)$, которая представляет собой аналитическое продолжение ряда $\sum_{n=1}^{\infty} n^{-z}$. Гипотеза состоит в предположении, что все нетривиальные нули[6] дзета-функции расположены на прямой $\mathrm{Re}\, z = 1/2$.

Аккуратный перевод задачи на игровое поле диофантовых уравнений требует определенных усилий[7], но практического значения, вообще говоря, не имеет, поскольку никаких дивидендов не сулит. Тут, скорее, вопрос философского характера — попытка уловить принципиальную взаимосвязь явлений. Поэтому широкий охват здесь имеет помимо спортивных — идеологические цели, и даже «диофантово переобувание» задачи о четырех красках, не говоря о полиномах для *простых множеств*[8] [19], вполне уместно.

Что же касается прагматической точки зрения, то перспективнее выглядит противоположный ход — перевод «диофантовой задачи» в какую-нибудь аналитическую область, где больше инструментов и они острее заточены.

Перевод задач из разных областей на диофантов язык, имея «свое лицо», по сути, говорит лишь об алгоритмизуемости этих задач. А когда последняя изначально ясна, то ясна и принципиальная возможность диофантова описания.

---

[5] В английской математической литературе употребляется iff вместо грамматически правильного if (если) для обозначения громоздкого оборота «если и только если». Трюк удобен. В русском — ему могло бы соответствовать «в томм случае» = «в том и только том случае».

[6] Разумеется, речь идет о нулях аналитического продолжения, а не самого ряда $\sum_{n=1}^{\infty} n^{-z}$.

[7] Если иметь в виду конструктивный перевод. Принципиальная возможность обосновывается гораздо проще.

[8] По поводу *простых* и *иммунных множеств* см. раздел 10.3.

В то же время необходимо отдавать себе отчет, что многие математические проблемы не описываются на языке L_G, рáвно как и вообще на любом алгоритмическом языке. Примером могут служить некоторые проблемы, связанные с *эффективной конечностью* или *бесконечностью*. Для уравнения $P(x) = 0$ невозможно в общем случае (по *теореме Райса*) указать алгоритм, который бы отвечал на вопрос, конечно или бесконечно множество решений. Для конкретного полинома — может быть. Но все нерешенные пока проблемы, где утверждается конечность или бесконечность множества элементов, удовлетворяющих некоторым свойствам, — подпадают под подозрение. Такова, например, *проблема бесконечности пар простых чисел-близнецов*. Как ее записать в L_G — не видно. Но если проблема решаема, то соответствующая запись возможна.

6.3. Универсальный многочлен

Из существования эффективного перечисления

$$S_1, S_2, \ldots \tag{6.3}$$

всех перечислимых (равносильно, диофантовых) множеств — вытекает (раздел 3.2) существование всюду определенной вычислимой функции двух переменных $f(n, k)$, которая при фиксированном n перечисляет элементы S_n.

По теореме 5.10.4 функция $f(n, k)$ может быть описана в языке L_G, а тогда, по центральной теореме 6.1.1, — и в языке L_0. Другими словами, перечислению (6.3) может быть поставлен в соответствие *универсальный полином* $U(n, s, x_1, \ldots, x_k)$, перечисляющий все S_n,

$$s \in S_n \quad \Leftrightarrow \quad \exists\,(x_1, \ldots, x_k) : U(n, s, x_1, \ldots, x_k) = 0, \tag{6.4}$$

причем $U(n, s, x)$ при желании строится конструктивно, поскольку все звенья за кадром конкретно определены [9].

В эквивалентном варианте (лемма 1.11.2) существует универсальный полином $\widehat{U}(n, x_1, \ldots, x_{k+1})$, множество положительных значений которого при фиксированном n совпадает с S_n,

$$s \in S_n \quad \Leftrightarrow \quad \exists\,(x_1, \ldots, x_{k+1}) : s = \widehat{U}(n, x_1, \ldots, x_{k+1}) \wedge s > 0.$$

[9] Конкретная запись одного из вариантов универсального полинома есть в [19], см. также *Jones J. P.* // J. Symb. Logic. 1982. № 3. **47**. 549–571.

Конкретно:

$$\widehat{U}(n, x_1, \ldots, x_{k+1}) = x_{k+1}[1 - U^2(n, x_{k+1}, x_1, \ldots, x_k)].$$

Степень m универсального полинома и число переменных

$$x = \{x_1, \ldots, x_k\}$$

зависят от способа построения $U(n, s, x)$. Чисел m и k порядка двух-трех десятков, как правило, достаточно (см. раздел 6.5). Если ситуацию сравнивать с *универсальной машиной Тьюринга*, то набор переменных $\{x_1, \ldots, x_k\}$ идеологически соответствует внутренним состояниям машины [10]. При этом ограниченная размерность $x = \{x_1, \ldots, x_k\}$ не вызывает удивления, поскольку достаточность конечного числа внутренних состояний для решения любых задач — в интерпретации Тьюринга очевидна (раздел 1.8). Однако на языке полиномов получается совершенно неожиданная вещь.

6.3.1. Теорема. *Каков бы ни был полином $P(n, z_1, \ldots, z_N)$ и какова бы ни была размерность N, существует полином*

$$\widehat{U}(n, x_1, \ldots, x_m)$$

фиксированной размерности m, множество положительных значений которого при любом n в точности совпадает с множеством положительных значений полинома $P(n, z_1, \ldots, z_N)$.

◄ Для доказательства достаточно заметить, что множество положительных значений любого полинома $P(n, z_1, \ldots, z_N)$ перечислимо, и потому совпадает с множеством положительных значений универсального полинома $\widehat{U}$. ►

Параметр n в формулировке теоремы можно опустить.

Параметр s в (6.4) можно считать векторным, $s = \{s_1, \ldots, s_m\}$, записывая тем самым универсальное уравнение в виде

$$U(n, s_1, \ldots, s_m, x_1, \ldots, x_k) = 0. \tag{6.5}$$

Иногда это удобно. В то же время от (6.5) с помощью *нумерующей функции* $s = c^m(s_1, \ldots, s_m)$ всегда можно перейти к универсальному

[10] Число состояний машины, как показал Шеннон, может быть уменьшено до двух за счет увеличения алфавита.

уравнению с одним параметром s,

$$U^2(n, s_1, \ldots, s_m, x_1, \ldots, x_k) + [s - c^m(s_1, \ldots, s_m)]^2 = 0,$$

и $k + m$ неизвестными $s_1, \ldots, s_m, x_1, \ldots, x_k$.

6.4. Технические результаты

Данный раздел включен в главу после некоторых колебаний. Аргументов «против» довольно много. Во-первых, это десяток страниц лишнего текста, который «никто» читать не будет [11]. Во-вторых, подробное доказательство есть в доступных источниках [15, 18, 19]. В-третьих, раздел 5.10 дает общее представление о технике, которая при достаточном напряжении сил приводит к успеху. Аргумент «за», собственно, один. Многие из тех, кто «читать не будет», захотят все же пробежаться взглядом, дабы понять, на что это похоже. А искать другой источник при слабой мотивировке — не резон. В то же время намерение «взглянуть» при несерьезности формулировки часто носит глубинный характер, недаром за лицезрение каких нибудь Чудес Света платят большие деньги.

Раздел фактически посвящен доказательству теоремы 6.1.1 и текстуально в значительной мере следует статье *Дэвиса* [8]. С другими, но близкими по духу вариантами — можно ознакомиться по указанным выше источникам.

Еще раз о причинах, по которым детальный разбор доказательств не имеет большого смысла. Обоснования бывают интереснее и важнее фактов. В данном случае ситуация иная. Факты уникальны, доказательства рутинны. Конечно, из-за большого количества формул может показаться, что за этим стоит нечто нетривиальное. Однако, если присмотреться, все рассуждения достаточно просты. Их, правда, много, и они перепутаны. Поэтому шагать легко, выйти из леса трудно. Но когда выход уже найден, изучать маршрут полезно — если есть намерение ходить за грибами в тот же лес.

Уравнения Пелля. Последующий текст опирается на свойства хорошо изученного в теории чисел уравнения Пелля специального вида [12]

$$x^2 - dy^2 = 1, \quad d = a^2 - 1, \tag{6.6}$$

где целые $x, y \geqslant 0$, $a > 1$.

Биномиальное разложение $(a + \sqrt{d})^n$ порождает, в результате

$$(a + \sqrt{d})^n = x_n(a) + y_n(a)\sqrt{d}, \tag{6.7}$$

две целочисленные функции $x_n(a)$, $y_n(a)$,

$$x_n(a) = \sum_{2k \leqslant n} C_n^{2k} a^{n-2k} d^k, \qquad y_n(a) = \sum_{2k+1 \leqslant n} C_n^{2k+1} a^{n-2k-1} d^k, \tag{6.8}$$

[11] И будет, безусловно, прав, если ориентируется в жизни на другие цели.

[12] Специфика — в дополнительном условии $d = a^2 - 1$.

которые, очевидно, удовлетворяют уравнению (6.6), поскольку наряду с (6.7) имеет место [13]

$$x_n(a) - y_n(a)\sqrt{d} = (a - \sqrt{d})^n,$$

приводящее после умножения на (6.7) к

$$x_n^2(a) - dy_n^2(a) = a^2 - d = 1.$$

Небольшие дополнительные усилия приводят к справедливости следующего факта.

6.4.1. Лемма. *Совокупность* $\{x_n(a), y_n(a)\}$ *исчерпывает все решения уравнения* (6.6).

Для удобства дополнительно полагается

$$x_n(1) = 1, \quad y_n(1) = n. \tag{6.9}$$

6.4.2. Лемма. $x_{m\pm n} = x_m x_n \pm dy_n y_m$, $y_{m\pm n} = x_n y_m \pm x_m y_n$.

◀ Доказательство легко получается манипулированием сопряженностью чисел $x_n + y_n\sqrt{d}$ и $x_n - y_n\sqrt{d}$. ▶

При $n = 1$ лемма 6.4.2 приводит к *рекуррентным соотношениям*

$$\boxed{x_{m\pm1} = ax_m \pm dy_m, \quad y_{m\pm1} = ay_m \pm x_m.} \tag{6.10}$$

6.4.3. Лемма. *Если* $a \equiv b \bmod c$, *то*

$$x_n(a) \equiv x_n(b) \bmod c, \quad y_n(a) \equiv y_n(b) \bmod c.$$

В частности, $y_n(a) \equiv n \bmod(a-1)$; *а также*

$$x_n(a) - y_n(a)(a - y) \equiv y^n(b) \bmod(2ay - y^2 - 1). \tag{6.11}$$

◀ Соотношения непосредственно следуют из (6.10) и свойств сравнений. Для обоснования (6.11) дополнительно используется индукция. ▶

6.4.4. Лемма. *Функция* $y_n(a)$ *монотонно возрастает по* a *и* n, *и имеет место оценка*

$$(2n-1)^a \leqslant y_n(a+1) \leqslant (2n)^a.$$

Функция x_n *также монотонно возрастает, причем*

$$x_{n+1}(a) > x_n(a) \geqslant a^n, \quad x_n(a) \leqslant (2a)^n.$$

◀ Обоснование получается из рекуррентных соотношений (6.10). ▶

---

[13] Числа $\alpha + \beta\sqrt{d}$ и $\alpha - \beta\sqrt{d}$ называются *сопряженными*, и параллель со случаем $d = -1$ иногда приносит определенные плоды.

6.4.5. Лемма. *Если* $y_m(a)$ *делит* $y_n(a)$, *то* m *делит* n, *и наоборот, т. е.*

$$y_m(a) \mid y_n(a) \quad \Leftrightarrow \quad m \mid n. \tag{6.12}$$

Аналогично,

$$y_m^2(a) \mid y_n(a) \quad \Leftrightarrow \quad my_m(a) \mid n. \tag{6.13}$$

Кроме того, если $y_i(a) \equiv y_j(a) \bmod y_k(a)$, *то*

$$\text{или} \quad i \equiv j, \quad \text{или} \quad i \equiv -j \bmod 2k.$$

◀ Очевидно, $y_n \mid y_{nk}$ при $k = 1$. Далее по индукции, используя лемму 6.4.2,

$$y_{n(k+1)} = x_n y_{nk} + x_{nk} y_n.$$

Поэтому «$y_n \mid y_{nk}$» $\to$ «$y_n \mid y_{n(k+1)}$». Обратная импликация доказывается также просто. В итоге получается (6.12).

Обоснование (6.13) в два раза длиннее. ▶

Из перечисленных опорных пунктов в две-три строчки выводятся *свойства периодичности*:

$$x_{2n\pm k} \equiv -x_k \bmod x_n, \quad x_{4n\pm k} \equiv x_k \bmod x_n,$$

6.4.6. Лемма. *Если* $i \leqslant n$ *и* $x_j \equiv x_i \bmod x_n$, *то* $j \equiv \pm i \bmod 4n$.

Диофантовость экспоненты. Как уже не один раз демонстрировалось, диофантовость сложных функций устанавливается комбинированием (с помощью $\wedge$) простых функций, полиномиальный характер которых очевиден. На этом пути возникают системы уравнений, гарантирующие в случае разрешимости диофантовость исследуемой функции. В данном случае ключом к экспоненте n^k оказывается система из 12 уравнений, имеющая автономную подсистему:

$$\textbf{(1)} \quad x^2 = 1 + (a^2 - 1)y^2,$$

$$\textbf{(2)} \quad u^2 = 1 + (a^2 - 1)v^2,$$

$$\textbf{(3)} \quad s^2 = 1 + (b^2 - 1)t^2,$$

$$\textbf{(4)} \quad v = ry^2,$$

$$\textbf{(5)} \quad b = 1 + 4py = a + qu,$$

$$\textbf{(6)} \quad s = x + cu,$$

$$\textbf{(7)} \quad t = k + 4(d - 1)y,$$

$$\textbf{(8)} \quad y = k + e - 1.$$

6.4.7. Лемма. *При любых фиксированных* a, k, *система* **(1)–(8)** *имеет решение (по остальным переменным) в том и только том случае, когда* $x = x_k(a)$.

◄ Первые три уравнения системы **(1)**–**(8)** являются *уравнениями Пелля*, поэтому при некоторых i, j, n обязаны выполняться соотношения [14]

$$x = x_i(a),\ y = y_i(a);\quad u = x_n(a),\ v = y_n(a);\quad s = x_j(b),\ t = y_j(b),$$

причем $i \leqslant n$, в силу **(4)**.

Далее: лемма 6.4.6 $\Rightarrow$ $j \equiv \pm i \bmod 4n$;

$$(4) \Rightarrow y_i^2(a) \mid y_n(a) \Rightarrow y_i(a) \mid n,$$

откуда $\boxed{j \equiv \pm i \bmod 4y_i(a)}$. Из **(5)** следует $b \equiv 1 \bmod 4y_i(a)$, что в итоге приводит [15] к $\boxed{y_i(b) \equiv j \bmod 4y_i(a)}$. Наконец, **(7)** влечет за собой $\boxed{y_i(b) \equiv k \bmod 4y_i(a)}$. Комбинируя выделенное рамками, получаем

$$k \equiv \pm i \bmod 4y_i(a). \tag{6.14}$$

Поскольку из **(8)** следует $k \leqslant y_i(a)$, то с подключением леммы 6.4.4 — $i \leqslant y_i(a)$. В итоге из (6.14) вытекает

$$x_i(a) = x_k(a) = x.$$

Обратно. Пусть $x = x_k(a)$. Положим $y = y_k(a)$, а также

$$m = 2ky_k,\quad u = x_m(a),\quad v = y_m(a),$$

что обеспечит выполнение **(1)** и **(2)**. Далее: $y^2 \mid v$ (лемма 6.4.5), поэтому существует r, удовлетворяющее **(4)**. Очевидно, НОД$(u, v) = 1$, откуда НОД$(u, v \cdot 4y) = 1$. Поэтому (по теореме 5.10.3) существует такое b_0, что

$$b_0 \equiv 1 \bmod 4y,\quad b_0 \equiv a \bmod u.$$

Тем же соотношениям удовлетворяет $b_0 + 4juy$. Следовательно, существуют b, p, q, удовлетворяющие уравнению **(5)**. Уравнение **(3)** удовлетворяется подстановкой $s = x_k(b)$, $t = y_k(b)$. В силу леммы 6.4.3 и **(5)**, $s \equiv x \bmod u$, поэтому существует c, удовлетворяющее **(6)**. Далее (леммы 6.4.3 и 6.4.4) $t \equiv k \bmod b - 1$, и в силу **(5)**, $t \equiv k \bmod 4y$. Поэтому существует d, удовлетворяющее **(7)**. Наконец, $y \geqslant k$ (лемма 6.4.4), благодаря чему уравнению **(8)** можно удовлетворить, полагая $e = y - k + 1$. ►

Понятно, что такое доказательство доставить удовольствие не может, но держа в голове систему из 8 уравнений, трудно рассчитывать на что-нибудь другое.

Теперь подсоединяем к **(1)**–**(8)** следующую часть:

$$(9)\quad (x - y(a - n) - m)^2 = (f - 1)^2(2an - n^2 - 1)^2,$$

$$(10)\quad m + g = 2an - n^2 - 1,$$

---

[14] Условие $b > 1$ выполняется в силу **(4)**, $b > a > 1$.

[15] Из (6.10) вытекает $y_n \equiv n \bmod a - 1$.

$$\textbf{(11)}\quad w = n + h = k + l,$$

$$\textbf{(12)}\quad a^2 - (w^2 - 1)(w - 1)^2 z^2 = 1.$$

6.4.8. Теорема. *Соотношение $m = n^k$ выполняется в том и только том случае, когда система уравнений* **(1)–(12)** *имеет решение по остальным переменным.*

◀ *Достаточность.* Покажем, что $m = n^k$ вытекает из разрешимости системы. В силу **(11)**, $w > 1$, откуда $(w - 1)z > 0$, что с опорой на **(12)** гарантирует $a > 1$. Поэтому «внешние условия» для леммы 6.4.7 выполнены, и можно считать $x = x_k(a)$, $y = y_k(a)$.

Используя рекуррентные соотношения для *уравнений Пелля* и учитывая **(9)**, получаем

$$m \equiv n^k \bmod(2an - n^2 - 1),$$

причем $k, n < w$ в силу **(11)**.

Уравнение **(12)** дает

$$a = x_j(w), \quad (w - 1)z = y_j(w)$$

при некотором

$$j \equiv 0 \bmod(w - 1),$$

откуда ясно $j \geqslant w - 1$, и лемма 6.4.4 в итоге приводит к неравенству

$$a \geqslant w^{w-1} > n^k.$$

Теперь из неравенства $m < 2an - n^2 - 1$, следующего из **(10)**, и легко проверяемой импликации

$$a > y^k \;\to\; 2an - n^2 - 1 > y^k$$

вытекает

$$n^k < 2an - n^2 - 1.$$

А так как оба числа m и n^k сравнимы по модулю $2an - n^2 - 1$, то они равны.

Необходимость. По сути, приблизительно тот же путь надо пройти в обратном порядке: $m = n^k \Rightarrow$ «разрешимость **(1)–(12)**».

Итак, пусть $m = n^k$. Возьмем любое $w > n$, $w > k$, положим $a = x_{w-1}(w) > 1$, и тогда, по лемме 6.4.3,

$$y_{w-1}(w) \equiv 0 \bmod(w - 1),$$

что равносильно равенству $y_{w-1}(w) = z(w - 1)$, — и **(12)** тем самым выполнено. Равенство **(11)** можно обеспечить, полагая

$$h = w - n, \quad l = w - k.$$

Аналогично предыдущему $m = n^k < 2an - n^2 - 1$, и **(10)** удовлетворяется выбором

$$g = 2an - n^2 - 1 - m.$$

Наконец, в силу (6.11), значение f можно выбрать из условия

$$x - y(a - n) - m = \pm(f - 1)(2an - n^2 - 1),$$

обеспечивая в результате равенство **(9)**. Выполнимость **(1)–(8)** берет на себя лемма 6.4.7. ►

Некоторые плоды. Диофантовость экспоненты оказывается тем рычагом, который переворачивает всю тематику. Диофантовыми «становятся» многие другие функции.

6.4.9. Теорема. *Функции*

$$n!, \qquad C_n^k = \frac{n!}{k!(n-k)!}, \qquad h(a,b,y) = \prod_{k=1}^{y}(a + bk)$$

диофантовы.

Заключение достигается в несколько шагов.

6.4.10. Лемма. *При условии $u > 2^n$, $k \leqslant n$, — справедливо равенство*

$$\left[\frac{(u+1)^n}{u^k}\right] = \sum_{i=k}^{n} C_n^i u^{i-k},$$

где квадратные скобки обозначают целую часть.

◄ Результат элементарно следует из представления

$$\frac{(u+1)^n}{u^k} = \sum_{i=0}^{n} C_n^i u^{i-k} = \sum_{i=k}^{n} C_n^i u^{i-k} + \sum_{i=0}^{k-1} C_n^i u^{i-k}$$

и оценки

$$\sum_{i=0}^{k-1} C_n^i u^{i-k} < u^{-1} \sum_{i=0}^{k-1} C_n^i < u^{-1} 2^n < 1. \quad ►$$

Таким образом, в условиях леммы 6.4.10 ($u > 2^n$, $k \leqslant n$) имеет место

$$\left[\frac{(u+1)^n}{u^k}\right] \equiv C_n^k \bmod u. \tag{6.15}$$

◄ На этом основании легко устанавливается диофантовость C_n^k. Действительно, из (6.15) следует, что $z = C_n^k$ равносильно условию

$$\exists\, u, v, w : \{v = 2^n \wedge (u > v) \wedge w = [(u+1)^n/u^k] \wedge (z \equiv w \bmod u) \wedge (z < u)\}.$$

Далее остается заметить, что все предикаты между конъюнкциями здесь диофантовы. Главную тяжесть на себя берет, конечно, теорема 6.4.8, обеспечивая диофантовость $v = 2^n$. Остальное: $(z \equiv w \bmod u) \wedge (z < u)$ равносильно

$$\exists\, x, y : \{(w = z + (x-1)u \wedge (u = z + y))\},$$

а соотношение $w = [(u+1)^n / u^k]$ равносильно

$$\exists\, x, y, t : \{(t = u+1) \wedge (x = t^n) \wedge (y = u^k) \wedge (wy \leqslant x < (w+1)y)\}. \quad \blacktriangleright$$

Факториал в случае $r > (2x)^{x+1}$ *представи́м формулой*

$$x! = \left[\frac{r^x}{C_r^x}\right]. \tag{6.16}$$

$\blacktriangleleft$ $$\frac{r^x}{C_r^x} = \frac{x! r^x}{r(r-1)\dots(r-x+1)} < \frac{x!}{\left(1-\frac{x}{r}\right)^x} < \frac{x!}{\left(1+\frac{2x}{r}\right)^x},$$

а поскольку $\left(1+\frac{2x}{r}\right)^x < 1 + \frac{2x}{r}\cdot 2^x$, в итоге получается

$$\frac{r^x}{C_r^x} < x!\left(1+\frac{2x}{r}\right)\cdot 2^x < x! + \frac{2^{x+1}x^{x+1}}{r} < x! + 1,$$

что в сопоставлении с легко проверяемым неравенством $x! \leqslant r^x / C_r^x$ приводит к (6.16). $\blacktriangleright$

Вернемся к факториалу. Легко проверить, что равенство $m = n!$ эквивалентно предикату

$$\exists\, x, y, t, u, v : \{(s = 2x+1) \wedge (t = x+1) \wedge$$
$$\wedge (r = s^t) \wedge (u = r^n) \wedge (v = C_n^r) \wedge (mv \leqslant u < (m+1)v)\},$$

диофантовость которого устанавливается «пофрагментно» на основе (6.16) и теоремы 6.4.8.

Осталось показать диофантовость функции $h(a, b, y)$.

$\blacktriangleleft$ Установим сначала

$$bq \equiv a \bmod M \quad \Rightarrow \quad \prod_{k=1}^{y}(a+bk) \equiv b^y y! C_{q+y}^y \bmod M. \tag{6.17}$$

Действительно,

$$b^y y! C_{q+y}^y = b^y (q+y)(q+y-1)\dots(q+1) = (bq+by)(bq+by-b)\dots(bq+b) \equiv$$
$$\equiv (a+by)(a+by-b)\dots(a+b) \bmod M. \quad \blacktriangleright$$

◀ Полагая в (6.17) $M = b(a+by)^y + 1$, имеем НОД$(M, b) = 1$ и

$$M > \prod_{k=1}^{y}(a+bk).$$

Поэтому сравнение $bq \equiv a \bmod M$ разрешимо относительно q, и тогда при соответствующем q произведение $\prod_{k=1}^{y}(a+bk)$ сравнимо с $b^y y! C_{q+y}^y$ по модулю M, что означает эквивалентность условий $z = \prod_{k=1}^{y}(a+bk)$ и

$$\exists\, p, q, r, s, t, u, v, w, x, M :$$
$$(r = a+by) \wedge (s = r^y) \wedge (M = bs+1) \wedge (bq = a+Mt) \wedge (u = b^y) \wedge$$
$$\wedge\, (v = y!) \wedge (z < M) \wedge (w = q+y) \wedge (x = C_w^y) \wedge (z + Mp = uvx).$$

Доказательство завершается применением к этому предикату установленных выше результатов. ▶

Ограниченный квантор $\forall_{\leqslant}$. Как уже отмечалось в разделе 6.1, для «замыкания круга» необходимо установить диофантовость квантора $\forall_{\leqslant}$. Стержневая теорема 6.1.2 в переформулировке звучит так.

6.4.11. Теорема. *Множество*

$$S = \{(y, x) : \forall\, z \leqslant y \;\; \exists\, g : P(y, z, x, g) = 0\},$$

где P полином, $x = \{x_1, \ldots, x_n\}$, $g = \{g_1, \ldots, g_m\}$, — диофантово[16].

Следуя Дэвису [8], начнем с двух вспомогательных утверждений. Первое из них (о равносильности двух предикатов) практически очевидно:

$$\forall\, z \leqslant y \;\; \exists\, g : P(y, z, x, g) = 0 \quad \Leftrightarrow \quad \exists\, u \;\; \forall\, z \leqslant y \;\; \exists\, g \leqslant u : P(y, z, x, g) = 0, \quad (6.18)$$

где $g \leqslant u$ означает $g_1 \leqslant u, \ldots, g_m \leqslant u$.

Другое — требует доказательства.

6.4.12. Лемма. *Если полином Q удовлетворяет неравенствам*

$$Q(y, u, x) > u, \quad Q(y, u, x) > y$$

и при $k \leqslant y$, $g \leqslant u$ мажорирует полином P:

$$|P(y, k, x, g)| \leqslant Q(y, u, x),$$

то для $\forall\, k \leqslant y \;\; \exists\, g \leqslant u : P(y, k, x, g) = 0$ необходима и достаточна истинность высказывания:

$$\exists\; u, c, t, a_1, \ldots, a_m : \left\{\left[1 + ct = \prod_{k=1}^{y}(1+kt)\right] \wedge\right.$$

[16] Вместо принятого $\forall_{\leqslant y}\, z$ здесь и далее используется $\forall\, z \leqslant y$.

$$\wedge [t = Q(y, u, x)!] \wedge \left[1 + ct \mid \prod_{j=1}^{u}(a_1 - j)\right] \wedge \ldots \wedge \left[1 + ct \mid \prod_{j=1}^{u}(a_m - j)\right] \wedge$$

$$\wedge \left[P(y, c, x, a_1, \ldots, a_m) \equiv 0 \bmod (1 + ct)\right] \Bigg\}$$

свободного от ограниченных кванторов.

◀ *Необходимость.* Пусть

$$P\big(y, k, x, g_1(k), \ldots, g_m(k)\big) = 0, \quad k = 1, 2, \ldots, t,$$

и все $g_j(k) \leqslant u$. Для $t = Q(y, u, x)!$, в силу

$$\prod_{k=1}^{y}(1 + kt) \equiv 1 \bmod t,$$

значение c можно выбрать так, что

$$1 + ct = \prod_{k=1}^{y}(1 + kt). \tag{6.19}$$

Далее, *китайская теорема об остатках* гарантирует существование чисел [17]

$$a_i \equiv g_j(k) \bmod (1 + kt), \quad k = 1, 2, \ldots, y. \tag{6.20}$$

Равенство (6.19) влечет $k \equiv c \bmod (1 + kt)$, откуда

$$P(y, c, x, a_1, \ldots, a_m) \equiv P\big(y, k, x, g_1(k), \ldots, g_m(k)\big) \bmod (1 + kt) = 0,$$

а так как $1 + kt$ (при разных k) взаимно просты, то их произведение также делит многочлен $P(y, c, x, a_1, \ldots, a_m)$, т. е.

$$P(y, c, x, a_1, \ldots, a_m) \equiv 0 \bmod (1 + ct).$$

Наконец, из (6.20) следует делимость всех $a_i - g_i(k)$ на $1 + kt$, что в итоге обеспечивает делимость $\prod_{j=1}^{u}(a_j - j)$ на $1 + kt$, а значит и на $1 + ct$.

Достаточность. Пусть p_k простые сомножители в разложении $1 + kt$, а $g_i(k)$ остаток от деления a_i на p_k.

Заметим, что p_k делит $1 + kt$, $1 + kt$ делит $1 + ct$, а $1 + ct$ делит $\prod_{j=1}^{u}(a_i - j)$, откуда вытекает делимость $\prod_{j=1}^{u}(a_i - j)$ на p_k. Следовательно, простое p_k делит

[17] Требуемая китайской теоремой 5.10.3 взаимная простота чисел $1 + kt$ (при разных k) вытекает из следующего рассуждения. Если s делит $1 + kt$ и $1 + lt$, где $1 \leqslant k \leqslant l \leqslant y$, то s делит и $l - k$, откуда $s < y$. Но тогда, в силу $Q(y, u, x) > y$, s делило бы и t, что невозможно.

$a_i - j$ при некотором $j \in \{1, \ldots, u\}$, т. е.

$$j \equiv a_i \equiv g_i(k) \bmod p_k.$$

В силу $t = Q(y, u, x)!$ и предположения $Q(y, u, x) > y$, любой делитель $1 + kt$ больше $Q(y, u, x)$, что влечет за собой $p_k > Q(y, u, x) > u$. Таким образом, $j \leqslant u < p_k$, а поскольку $g_i(k) < p_k$ по определению, то $g_i(k) = j$. В итоге:

$$\boxed{1 \leqslant g_i(k) \leqslant u \quad \text{для всех} \quad i, k.}$$

Далее,

$$1 + ct \equiv 1 + kt \equiv 0 \bmod p_k,$$

что влечет за собой $k \equiv c \bmod p_k$.

В результате $g_i(k) \equiv a_i \bmod p_k$. Поэтому

$$P\big(y, k, x, g_1(k), \ldots, g_m(k)\big) \equiv P(y, c, x, a_1, \ldots, a_m) \equiv 0 \bmod p_k,$$

а в силу мажорирования P полиномом $Q(y, u, x) < p_k$,

$$P\big(y, k, x, g_1(k), \ldots, g_m(k)\big) = 0. \quad \blacktriangleright$$

Теперь доказательство теоремы 6.4.11 завершается относительно просто.

◀ Исходный полином $P(y, k, x, g)$ есть сумма слагаемых

$$t_r = |c| y^a k^b x_1^{q_1} \ldots x_n^{q_n} g_1^{s_1} \ldots g_m^{s_m}.$$

Полагая $u_r = cy^a k^b x_1^{q_1} \ldots x_n^{q_n} g_1^{s_1} \ldots g_m^{s_m}$ и

$$Q(y, u, x) = u + y + \sum_{r=1}^{N} u_r,$$

имеем полином $Q(y, u, x)$, удовлетворяющий предположениям леммы 6.4.12, что элементарно проверяется.

В результате

$$\forall k \leqslant y \;\; \exists g \leqslant u : P(y, k, x, g) = 0$$

эквивалентно сводится к многострочному предикату из леммы 6.4.12, диофантовость которого легко устанавливается с помощью инструментов, разработанных выше. Наконец, (6.18) позволяет избавиться от u. $\blacktriangleright$

За формальными доказательствами, конечно, стоят направляющие соображения, описанием которых уместно заниматься в других книгах. Заинтересованный читатель может обратиться к работам Матиясевича, в которых больший акцент делается на идеологической стороне дела.

6.5. Дополнения

• *Степень полинома* в описании диофантова множества

$$A = \{a : \exists\, x_1, \ldots, x_m [P(a, x_1, \ldots, x_m) = 0]\} \tag{6.21}$$

можно понизить, вводя переменные

$$y_{ij} = x_i x_j, \quad y_{0j} = a x_j, \quad y_{00} = a^2. \tag{6.22}$$

Производя в полиноме P замены (6.22), перейдем от (6.21) к задаче (условно полагаем $x_0 = a$)

$$A = \left\{ a : \exists\, x_1, \ldots, x_m : \left[P^2(\ldots) + \sum_{i,j=0}^{m} (y_{ij} - x_i x_j)^2 = 0 \right] \right\}.$$

Действуя далее в том же духе, степень определяющего полинома можно понизить до 4 (если она изначально не меньше 4).

• Помимо степени n важна и другая характеристика: число переменных $\{x_1, \ldots, x_m\}$, по которым декларируется существование решения. В разделе 1.11 уже отмечалось, что для любого диофантова множества можно указать полином (1.17) с $n \leqslant 4$ (но, возможно, большим m) либо $m \leqslant 9$ (но, может быть, большим n). Интерес, понятно, представляют универсальные пары $\langle n, m \rangle$, оценивающие сверху оба показателя одновременно. *Джонс*[18], например, указывает такие пары $\langle n, m \rangle$:

$$\langle 4, 58\rangle, \quad \langle 8, 38\rangle, \quad \langle 12, 32\rangle, \quad \langle 20, 28\rangle, \quad \langle 24, 26\rangle, \quad \langle 36, 24\rangle,$$

$$\langle 2 \cdot 10^5, 14\rangle, \quad \langle 6{,}6 \cdot 10^{43}, 13\rangle, \quad \langle 4{,}6 \cdot 10^{44}, 11\rangle, \quad \langle 8{,}6 \cdot 10^{44}, 10\rangle, \quad \langle 1{,}6 \cdot 10^{45}, 9\rangle.$$

[18] См.: *Jones J. P.* Universal diophantine equation // J. Symb. Logic. 1982. № 3. **47**. 549–571.

Глава 7

Конструктивная математика

Едва ли не тяжелей остального необходимость допустить, что гипотеза континуума, — возможно, первый приходящий в голову важный вопрос о бесконечных множествах — не имеет внутреннего смысла.

П. Дж. Коэн

Представление о конструктивизме в математике нередко ассоциируется с кучкой формалистов, не способных адекватно реагировать на жизнь в ее многообразии. Подобное мнение обычно возникает «на бегу», из-за нежелания вникнуть. Дескать, есть числа *вычислимые* и *невычислимые*, но это не идет дальше проблем алгоритмической неразрешимости. Оказывается, идет. Чтобы ощутить это, надо вдуматься хотя бы, какой миной для анализа является *шпеккеровская последовательность*.

7.1. Конструктивные числа

При десятичной записи чисел из $[0, 1]$,

$$a = 0{,}\alpha_1\alpha_2 \ldots \alpha_n \ldots, \tag{7.1}$$

естественно задаться вопросом, как и чем α_n определяются.

В ситуациях типа

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!} + \ldots$$

есть алгоритм вычисления α_n, т. е. — конечное правило. То же самое можно сказать о любом рациональном числе, $\sqrt{2}$, π, а также о многих других вещественных числах. Но не обо всех, поскольку $[0, 1]$ — континуум, а конечных правил счетное число.

Если рассуждать образно, то бесконечное количество знаков в (7.1) — это продукт деятельности некоего конечного «механизма». С каждым поворотом ручки появляется следующий знак. Такова

алгоритмическая (конструктивная) позиция, в соответствии с которой бесконечные множества «существуют» лишь как обозначение возможности безостановочной работы алгоритма. Бесконечное количество элементов перечислимого множества — в некотором роде фикция. Их может быть сколь угодно много, но для этого необходимо долго разворачивать процесс вычислений.

Позиция же классического анализа состоит в несколько «безответственной» декларации, что бесконечность состоялась — безостановочная работа проведена до конца, и вот вам иррациональное число.

В соответствии со сказанным числа естественно назвать *конструктивно определяемыми*, если все их знаки α_n алгоритмически вычисляются. Возможны несколько вариантов уточнения. Остановимся пока на двух.

7.1.1. Вариант 1. $\alpha_n = f(n)$, *где* $f(n)$ *эффективный алгоритм, определенный при любом* n.

7.1.2. Вариант 2. *Множество пар* $\{n, \alpha_n\}$ *перечислимо.*

Принципиальное отличие состоит в следующем. В первом варианте знаки определяются *последовательно*:

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n,\ \ldots\ .$$

Во втором — *в неизвестном порядке.*

Первый вариант представляется логически более осмысленным[1], так как по истечении конечного времени имеется $0{,}\alpha_1\alpha_2\ldots\alpha_n???$. Отбрасывая неопределенный хвост (из вопросов), это можно трактовать как приближение $0{,}\alpha_1\alpha_2\ldots\alpha_n$, сходящееся к a при $n \to \infty$.

В «варианте 2» ситуация кажется неприемлемой. По истечении конечного времени счета какие-то знаки определены, какие-то — нет,

$$0{,}???\alpha_4?\alpha_5?\ldots\alpha_n???,$$

и говорить о приближении, тем более сходящемся, вроде бы бессмысленно. Тем не менее, если множество $\{n, \alpha_n\}$ не только перечислимо, но и разрешимо, — второй вариант сводится к первому (?).

Если «вариант 1» принять за определение конструктивного числа, возникают следующие «неприятности». В силу $\alpha_n = f(n)$,

[1] Из-за привычки к догматике теории пределов.

где функция $f(n)$ *общерекурсивна*, т. е. вычислима и определена при любом n, получается, что множество $\mathbb{C}$ конструктивных чисел неперечислимо (теорема 1.7.1) [2], т. е. *конструктивно несчетно*. Но при расширении $\mathbb{C}$ до $\mathbb{F}$ (с точностью до изоморфизма) — снова получается перечислимое множество $\mathbb{F}$.

Ни равенство $a = b$, ни отношение $a < b$, — для конструктивных чисел в общем случае оказываются непроверяемы (теорема 3.5.1).

7.2. Последовательность Шпеккера

Спасти «вариант 2» можно следующим образом. Числа записываем в двоичной системе, все $\alpha_n \in \{0, 1\}$, и пусть всюду определенная вычислимая функция $f(k)$ перечисляет *без повторений* те номера n, которым отвечает $\alpha_n = 1$, т. е. те позиции в записи числа, где стоят единицы (а не нули).

Изначально во всех позициях пусть стоят нули. Через N шагов в каких-то N позициях будут расставлены единицы. Получится рациональное число

$$S_n = 0{,}00101101\ldots011.$$

Очевидно, последовательность $\{S_n\}$ строго монотонно возрастает, $S_{n+1} > S_n$, и ограничена, $S_n \leqslant 1$.

Но *если $f(k)$ перечисляет неразрешимое множество, — воспользоваться классической теоремой анализа о сходимости ограниченной монотонной последовательности не удается.* В этом случае $\{S_n\}$ называют *последовательностью Шпеккера*.

Она не может сходиться, поскольку не является фундаментальной. Например, $f(k) = 2$ все не появляется и не появляется, но гарантировать, что и не появится, — невозможно. Если вдруг появится, значение S_n сразу подпрыгнет на $1/4 = 2^{-2}$, и это может

[2] Тот факт, что здесь $f(n) \leqslant 9$ ничего принципиально не меняет. При доказательстве аналога теоремы 1.7.1 вместо $g(n) = f_n(n) + 1$ достаточно взять любую функцию $g(n) \neq f_n(n)$. Например, ту же $f_n(n) + 1$, если цифры расположить по кругу и под «+1» понимать сдвиг на одну позицию по часовой стрелке.

произойти когда угодно. В результате дискомфорт ожидания остается вплоть до бесконечности. В этом, собственно, и заключается коварство неразрешимых множеств.

В то же время $f(k)$ — совершенно нормальная функция с точки зрения анализа, а S_n — совершенно нормальная последовательность рациональных чисел, которая монотонна и ограничена, но не сходится! Теперь о конструктивных числах можно забыть. Необходимо разобраться с противоречием.

Заметим, кстати, что S_n можно записать в виде

$$S_n = \sum_{k=1}^{n} 2^{-f(k)}, \tag{7.2}$$

где $f(k) \in \mathbb{N}$, причем все $f(k)$ различны [3]. На языке числовых рядов отмеченная выше катастрофа звучит не менее безнадежно. Ряд

$$\sum_{k=1}^{\infty} 2^{-f(k)}$$

ограничен ($\leqslant 1$), но не сходится, хотя все члены положительны.

Посмотрим, как в анализе доказывается обратное. Пусть Ω_N обозначает множество значений $f(k)$ при $k \geqslant N$, и пусть $m(N)$ есть минимальное в Ω_N число [4]. Легко видеть, что

$$m(N) \to \infty \quad \text{при} \quad N \to \infty, \tag{7.3}$$

поскольку $f(k)$ перечисляет Ω_0 без повторений, т. е. все элементы Ω_0 различны. Из (7.3) следует

$$\sum_{k=N}^{\infty} 2^{-f(k)} \leqslant 2 \cdot 2^{-m(N)} \to 0 \quad \text{при} \quad N \to \infty,$$

т. е. хвост ряда стремится к нулю — ряд сходится. Соответственно, последовательность S_n фундаментальна.

[3] Перечисление без повторений.

[4] Существующее в силу ограниченности Ω_N снизу.

Разногласие подходов локализовано в том месте, где предполагается существование минимального в Ω_N числа $m(N)$. На территории классического анализа предположение выглядит настолько естественно, что его фундаментальный характер, способный направить математику по разным путям, — как правило, остается незамеченным.

Существование минимального в Ω_N числа в некотором роде предполагает, что вычисление $f(k)$ проведено до конца (*проблема актуальной бесконечности*) и минимум надо выбрать на «*состоявшемся*» бесконечном множестве Ω_N. *Машине Тьюринга* остается завидовать такой свободе мышления.

7.3. Конфликт с аксиомой выбора

Напомним принятые в анализе «правила игры».

7.3.1. Аксиома выбора. *В любом семействе*

$$\Phi = \{X_\alpha : \alpha \in A\}$$

непустых множеств X_α в каждом $X_\alpha \in \Phi$ можно выбрать по одному элементу, т. е. существует функция выбора $f : A \to \Phi$.

Следующие два утверждения эквивалентны аксиоме выбора.

7.3.2. Теорема Цермело. *На всяком множестве X можно ввести такое отношение порядка (вполне упорядочить[5]) X), при котором у любого подмножества $A \subset X$ будет наименьший элемент $x^0 \in A$.*

7.3.3. Лемма Цорна. *Если в частично упорядоченном множестве X любое упорядоченное подмножество ограничено снизу, то в X существует минимальный элемент x^*.*

Интересно заметить, что некоторые вещи, будучи озвученными, меняют ситуацию. От взаимоотношения двух людей до благополучия государства. Такой же *магический эффект провозглашения* случился с *аксиомой выбора*, которая до явной формулировки использовалась как самоочевидный факт. Декларация привлекла внимание «разрушителей», которые изобрели столь невероятные следствия [2], что впору было отказываться от аксиомы. Но тогда пришлось бы отказаться от массы привычных инструментов анализа, к чему «созидатели» (иногда в тех же лицах) оказались не готовы.

[5] Отрезок $[0, 1]$ при обычном отношении $\geqslant$ не вполне упорядочен, поскольку у интервалов $(a, b) \subset [0, 1]$ нет наименьших элементов, и $[0, 1]$ еще никому не удалось упорядочить конструктивно.

Вернемся к дилемме из предыдущего раздела. Расхождение в оценке сходимости S_n возникает из-за неоднозначного решения вопроса о существовании минимального в Ω_N числа $m(N)$. И дело не только в «состоявшейся бесконечности». Существование $m(N)$ гарантирует лемма Цорна, эквивалентная аксиоме выбора, на что, как становится ясно, и опирается классический анализ [6].

Здесь может возникнуть иллюзия, что анализу требуется лишь факт существования $m(N)$, а не алгоритмическая вычислимость. Однако в данном случае это одно и то же. Существование $m(N)$ означает, что по любому N можно указать такое m, что $f(k) \geqslant m$ при $k \geqslant N$. Но из неразрешимости множества значений $f(k)$ вытекает существование таких m, что ни $f(k) = m$, ни $f(k) \geqslant m$ принципиально не проверяемо.

(?) При поверхностном знакомстве с основаниями математики — на конструктивном углублении в анализ лучше не задерживаться. Конфликт респектабельных теорий наносит ущерб репутации обеих сторон. Восхищение машиной Тьюринга идет на убыль, когда выясняется, что вычислимость замешана в скандалах с устоявшимися областями математики. В то же время подрывается доверие к анализу, когда уходящий в гудок пар сообщает, что здесь не все чисто.

В каком-то смысле лучше было бы вообще не совмещать несовместимое. Все циники единодушны в одном. От конструктивного анализа нет никакого толку. Но что скажут они о поиске смысла жизни, в котором важен не смысл, а поиск. Конструктивный анализ — тот же поиск под выдуманным предлогом. Поиск, опосредованно ведущий к очень важным результатам идеологического характера, которые рецептурно ни на что не влияют, но поддерживают тонус и бдительность. Последнее весьма существенно для ощущения среды, в которой развивается математика.

7.4. Актуальная бесконечность

При открытой форточке для обсуждения бесконечности все приходят и высказываются. Каждый «о своем». Особенно философы,

[6] В данном случае опора происходит на счетный вариант аксиомы выбора.

не говоря о поэтах. Между тем в проблеме есть чисто математический аспект, если присмотреться.

Обратимся сначала к основным моментам теории вещественного числа и сопоставим их с конструктивной точкой зрения. Вот каркас теории Дедекинда, — см. подробнее [3, т. 1].

7.4.1. Определение. *Непустое множество A рациональных чисел называется* ***сечением*** *Дедекинда $d(A)$ при выполнении двух условий*:

1. *Если $\alpha \in A$, $\beta < \alpha$ и β — рациональное число, то $\beta \in A$.*
2. *В A нет наибольшего числа.*

Называть сечением множество неестественно, но проблема заключается в том, что игра начинается в отсутствие иррациональных чисел. Указать сечением $\sqrt{2}$ для «$x^2 < 2$» нет возможности. Поэтому в роли сечения оказывается само множество, что режет слух, но напоминает о стартовых условиях.

Подготовка сечений к трансформации в числа состоит в определении для них арифметических операций, что делается легко, но скучно. Например, неравенству $d(A) < d(B)$ сопоставляется строгое включение $A \subset B$. Сумме $d(A) + d(B)$ — сечение множества $A + B$, состоящего из рациональных чисел $\alpha + \beta$, где $\alpha \in A$, $\beta \in B$. Чтобы такие определения имели смысл, проверяются стандартные условия, которым они обязаны удовлетворять (коммутативность и прочее). Рутинная работа заканчивается введением на сечениях обычных числовых операций, после чего *термин «сечение» приравнивается термину «вещественное число»*. Рациональные сечения оказываются рациональными числами, остальные — *иррациональными*.

С помощью сечений вводятся также понятия *инфинума* и *супремума*. Сначала для ограниченного снизу множества M вводится множество Γ нижних граней M как совокупности рациональных $\gamma < m$, где m — любое рациональное число из M. Очевидно, Γ удовлетворяет определению 7.4.1 и поэтому является сечением. Число $d(\Gamma)$ называется точной нижней гранью множества M (возможно $d(\Gamma) = -\infty$). Аналогично определяется *точная верхняя грань*.

Рациональные монотонные последовательности a_n теперь сходятся к своим точным граням, что в конечном счете приводит к определению сходимости и немонотонных последовательностей. Итоговый вопрос «не появятся ли „новые числа“, если сечения производить уже с помощью вещественных множеств?» — решается *основной теоремой Дедекинда*:

7.4.2. *Любое сечение в области вещественных чисел является вещественным числом. Другими словами, операция пополнения вещественных чисел не дает новых элементов (как в случае с рациональными числами).*

С конструктивной позицией в перечисленном не вяжется «ни одна строчка». Сечения эффективно не определяются принципиально. Конструктивный облик примера $x^2 < 2$ — оазис в континуальной пустыне.

Для установления континуальности, правда, нужен еще *диагональный метод Кантора*, который на первый взгляд не менее прост и очевиден, чем аксиома выбора. В предположении счетности вещественных чисел их можно пронумеровать

$$a_1, a_2, \ldots, a_n, \ldots, \tag{7.4}$$

и тогда любое число b с десятичной записью

$$b = 0, \beta_1, \beta_2 \ldots,$$

отличающееся от a_1 в первом десятичном знаке, от a_2 — во втором, и так далее, — не входит в список (7.4), что дает противоречие.

Чтобы остановиться и задуматься, здесь достаточно вспомнить, что те же самые диагональные рассуждения в алгоритмической теории приводят совсем к другим выводам (о неразрешимости). Скользкий момент рассуждений «от противного» состоит в опоре на *закон исключения третьего*. Когда силы истрачены на поиск противоречия, разрушающего одну из альтернатив, вторая — принимается автоматически. Но откуда взялась вторая? Можно ли быть уверенным, что нет третьей возможности?

Такого рода вопросы обычно навевают скуку и всерьез не воспринимаются, потому что в большинстве случаев за ними стоит пустота. Но бывают ситуации, в которых наличие проблемы все же ощущается, и там имеет смысл задержаться, чтобы почувствовать дуновение загадки.

Схематично суть дела выглядит примерно так. Сколько бы ни говорилось о канонизации теорий с помощью математической логики, любая реальная теория в той или иной степени размыта. Речь не о том, что все «вилами по воде писано». Всегда есть более-менее четко очерченное ядро, но есть и пограничная зона, в которой утверждения, как потенциальные теоремы, не обязаны быть либо верными, либо неверными [7]. Доказательства от противного в такой ситуации ведут к порочным выводам.

[7] Нечто подобное довольно часто встречается в обыденной жизни, когда на вопрос невозможно ответить ни «да», ни «нет».

Гипотеза континуума[8], например, долгие годы выглядела фактом (или «не фактом») теории множеств. Выяснилось, однако, что гипотеза — «не теорема». Ее, либо ее отрицание, можно принимать в качестве дополнительной аксиомы [11].

7.5. Инструмент или реальность

Принципиальные неприятности любой теории возникают из-за бесконечности, благодаря которой математика, собственно, и процветает (если не говорить о финансовой поддержке).

Значительная часть трудностей проистекает из смешения понятий. В первую очередь стоит обратить внимание, что *актуальная*, т. е. *состоявшаяся* бесконечность — часто не требуется. У машины Тьюринга лента бесконечна в смысле наращиваемости. Если требуется, можно удлинить. Такая постановка вопроса не вызывает дискомфорта, рáвно как и противоречий.

«Идея наращиваемости» вполне работоспособна и в некоторых секторах анализа. Когда речь идет о последовательности a_n, т. е. о функции $a_n = f(n)$, $n \in \mathbb{N}$, — в большинстве случаев за кадром можно иметь в виду ограниченный диапазон, $n = 1, \ldots, M$ при возможности увеличивать M по мере необходимости. Но это — неудобно. Желателен короткий стенографический эквивалент, причем образный. Спрос, как известно, удовлетворяется понятием действительного числа, что подключает геометрическую интуицию. Далее возникает вера в выдуманное понятие, притупляющая критическое чутье.

Но дело не только в стенографии, которую можно было бы заменить неуклюжими реверансами. Бесконечность работает, как инструмент, в роли, которую не способно сыграть ничто другое.

- Решения *уравнения Пелля* $x^2 - 2y^2 = 1$ определяются формулами

$$x_n = \frac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2}, \qquad y_n = \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}.$$

[8] *Гипотеза континуума Кантора* состоит в предположении об отсутствии множества, промежуточного по мощности — между счетным и континуумом.

Неожиданно решения в целых числах порождаются механизмом, работающим на иррациональном топливе. Корень из двух возникает в результате «завершения» бесконечного процесса последовательных приближений. Тем не менее «незаконный» инструмент дает правильный результат. Причем уход в иррациональную область (бесконечным путем) позволяет вскрыть причинные связи, которые было бы трудно обнаружить без подходящего инструмента.

> *В то же время не случайно, что $\sqrt{2}$ здесь — конструктивное число (конечно определяемое). И это общее правило. Если рассуждения не начинаются с «безответственных» заявлений типа «пусть λ произвольная точка из $[0, 1]$», то они заканчиваются уравнениями и формулами, содержащими только вычислимые константы, e, π и т. п.*

• Другой пример. Рассмотрим уравнение

$$\sqrt{x+6\sqrt{x+\ldots+6\sqrt{x+6x}}}=x, \tag{7.5}$$

в левой части которого 10 радикалов.

По условию x равно выражению, стоящему слева в (7.5). Заменяя последнее x под радикалом на всю левую часть (7.5), получим уравнение того же вида, но содержащее уже 20 радикалов. Продолжая в том же духе, получим в итоге уравнение

$$\sqrt{x+6\underline{\sqrt{x+6\sqrt{x+\ldots}}}}=x, \tag{7.6}$$

с бесконечным числом радикалов. Заменяя теперь, по аналогичной причине, подчеркнутое в (7.6) выражение на x, приходим к эквивалентному уравнению

$$\sqrt{x+6x}=x,$$

откуда $x=7$.

На проделанную манипуляцию полезно взглянуть из прежних исторических времен, когда подобное было в диковинку. Трюк, безусловно, опирается на «состоявшуюся бесконечность», но дает правильный ответ во многих других ситуациях. Что делать? Здравый смысл подсказывает — узаконить фокус. Бесконечность провозглашается инструментом. Детали утрясаются аксиоматизацией. Вот и все. Существует ли бесконечность, — спрашивать теперь бессмысленно. Существует как инструмент. Вопрос «почему работает?» — выносится за скобки, а его острота смазывается философствованием. Вариации формулировок пускают мысль по кругу, создавая видимость понимания.

Окончательному пониманию принципиальных проблем всегда что-то мешает. Результат достигается единственным способом: непонятное убирается из поля зрения. Достаточно вспомнить, например, теорию относительности, где все непонятное было трансформировано в «необсуждаемую» ограниченность скорости света. Рассмотрение под тем же углом зрения квантовой механики или Библии — приводит к аналогичным выводам.

Неразбериху при обсуждении бесконечности создают различные попытки добиться парадоксальности за счет некорректности. Обсуждается, например, вопрос о «равенстве» бесконечностей

$$1,\ 2,\ 3,\ 4,\ \ldots,\ n,\ \ldots,$$

$$1,\ 4,\ 9,\ 16,\ \ldots,\ n^2,\ \ldots,$$

тогда как обеим сторонам ясно, что речь идет о возможности установить взаимно-однозначное соответствие $n \Leftrightarrow n^2$. Но термин «равенство» создает почву для незаметного дрейфа в сторону какого-нибудь парадокса.

Глава 8

Аксиоматические теории

Настоящий поиск ведет в никуда.

Хотя бы пару раз в жизни полезно «пробежаться» вдоль аксиоматического построения какой-нибудь теории, чтобы ощутить «тайну корней» и невероятную сложность «начального слова». Дом легко строить, когда работы уже в разгаре, — в плену набранной инерции. Совсем другое дело, когда еще ничего нет, и надо выбрать проект, привязать его к местности, обеспечить условия для старта и, держа в голове виртуальный замысел, сказать «А».

8.1. Арифметика Пеано

Отсев лишнего рождает произведение искусства. Замечательный образец в этом отношении дает *аксиоматика Пеано*, сводящая арифметическую систему $\{\mathbb{N}, +, \times\}$ к алгебре с одной *операцией счета* σ, называемой также *функцией следования*, $\sigma : \mathbb{N} \to \mathbb{N}$, и удовлетворяющей трем *аксиомам Пеано* [1]:

A1 $\sigma(m) = \sigma(n) \Rightarrow m = n$.

A2 $\forall n \in \mathbb{N} : \sigma(n) \neq 1$.

A3 Если $1 \in Q \subset \mathbb{N}$, где Q — произвольное подмножество $\mathbb{N}$, и «$n \in Q \Rightarrow \sigma(n) \in Q$», то $Q = \mathbb{N}$.

Последняя аксиома A3 [2] выражает *принцип математической индукции* и часто формулируется в менее общем виде: если 1 обладает свойством $\mathcal{P}$, т. е. $\mathcal{P}(1) = 1$, и

$$\mathcal{P}(n) = 1 \quad \to \quad \mathcal{P}(\sigma(n)) = 1,$$

то свойством $\mathcal{P}$ обладает любое n. Такую индукцию называют *ограниченной*.

---

[1] Многим почему-то кажется, что Дж. Пеано (1858–1932) ровесник натурального ряда.

[2] Аксиомы типа A3 принято называть *схемами аксиом* в связи с тем, что в них можно подставлять любые функции или предикаты, в данном случае — множества Q.

Разница, безусловно, принципиальна. В последнем случае дело приходится иметь со счетным множеством подмножеств $\mathbb{N}$, в варианте А3 — с континуальным. При этом А3 постулирует больше, чем арифметика может «проглотить», потому что утверждений и доказательств (а значит, и подмножеств $Q \subset \mathbb{N}$, которые имеют шанс попасть в поле зрения) — счетное число. Последнее обстоятельство связано с тем, что подмножества Q конструктивно выделяются только с помощью перечислимых предикатов.

Если говорить точнее, *аксиоматическая система Пеано* есть А1–А3 плюс стандартные «логические аксиомы». В совокупности это порождает весьма нетривиальный механизм, называемый *арифметикой*, или *теорией чисел*. Единственный инструмент доказательства общих утверждений[3] в *арифметике Пеано* — это индукция. Вернее, инструментов много, но без индукции они не работают.

Опираются ли все известные в теории чисел результаты только на аксиоматику Пеано — сказать трудно, потому что в доказательствах без каких-либо «угрызений совести» используются соображения из разных областей (анализ, топология, ТФКП). Проектируются ли эти соображения в идеологию Пеано — не всегда ясно, да и малоинтересно, поскольку репутация соответствующих дисциплин достаточно высока.

В то же время нумерация, скажем, топологических теорем переводит их в утверждения о натуральных числах, и, вообще говоря, не ясно, богаче ли топология, чем арифметика Пеано. То же самое касается других дисциплин. Экстраполяция мыслей в этом направлении приводит к вопросу: не является ли арифметика Пеано — наукой всех наук.

Не является. Аналитические методы позволяют доказывать кое-что недоказуемое в арифметике Пеано[4]. При этом не надо даже забираться в чересчур абстрактные области. Достаточно комбинаторики.

Известно, например, что среди любых шести человек обязательно найдутся трое, которые друг с другом либо все знакомы, либо все — не знакомы. Это маленькая иллюстрация *теоремы Рамсея*, которая на языке графов может быть сформулирована так:

---

[3] Справедливость чего-либо для всех $n \in \mathbb{N}$.

[4] Но, безусловно, доказуемое в некоторой расширенной арифметике, потому что все доказуемое аксиоматизируемо и алгоритмизуемо.

По любым целым m и r можно указать такое n, что полный граф с $N > n$ вершинами, каждое ребро которого раскрашено в один из r цветов, обязательно содержит полный подграф с m вершинами, все ребра которого имеют один цвет.

Имеется также *усиленная теорема Рамсея*, формулировка которой здесь не суть важна. Вся эта теория примечательна и достаточно глубока, но в данном контексте интересно другое. Если *обычная теорема Рамсея* — факт арифметики Пеано, то *усиленная* — в этой арифметике недоказуема [5]. Таким образом, тот факт, что арифметика Пеано не исчерпывает всех арифметических истин, в данном случае подтверждается конкретным примером.

Технические подробности. С помощью σ операции сложения и умножения в $\mathbb{N}$ определяются рекурсивными описаниями, а свойства (ассоциативность и прочее) устанавливаются индукцией А3.

• Вот как вводится *сложение*. Возьмем любое m. Функция $\sigma^m(n) = m + n$ задается рекурсией:

$$\sigma^m(1) = m + 1 \;=\; \sigma(m),$$
$$\sigma^m(n+1) = m + (n+1) \;=\; \sigma^m(\sigma(n)) = \sigma(\sigma^m(n)),$$

но этого пока мало для завершения начатого дела.

Пусть N_m обозначает множество тех $n \in \mathbb{N}$, для которых функция

$$\sigma^m(n) = m + n$$

определена. В силу принятого описания, $1 \in N_m$ и, если $\sigma^m(n)$ определена, то и $\sigma^m(n+1)$ определена. Теперь А3 гарантирует определенность $\sigma^m(n) = m + n$ при любом $n \in \mathbb{N}$.

• Функция умножения $\nu_m(n) = m \times n$ вводится рекурсией:

$$\nu^m(1) = m, \qquad \nu^m(\sigma(n)) = m + \nu_m(n) = \sigma^m(\nu_m(n)).$$

Обоснование завершается применением индукции.

Далее с помощью индукции устанавливаются обычные свойства сложения и умножения. Если эти свойства включить в аксиоматику, а индукцию с частью логического арсенала исключить, — получится разрешимая *арифметика Тарского* (раздел 4.2), в которой мало что поддается формулировке, зато все доказывается.

Все *выводимое* в арифметике Пеано можно включать в аксиоматику в качестве «лишних» постулатов, к каковым часто относят следующее утверждение.

[5] См.: *Paris J., Harrington L.* A mathematical incompleteness in Peano arithmetic // Handbook of Math. Logic. Holland, Amsterdam, 1978. Формулировка усиленной теоремы Рамсея есть в [15].

8.1.1. Принцип Дирихле. *Отображение $f : \Omega \to \Omega$ конечного множества Ω взаимно однозначно тогда и только тогда, когда оно сюръективно (является отображением «на»).*

Школьные представления, что все «правильное» может быть доказано с помощью индукции, разумеется не верно. Кое-что из «правильного» не может быть доказано никак (*теорема Гёделя*).

8.2. Парадокс категоричности

Вариант аксиоматики Пеано в предыдущем разделе был выбран бесхитростный — речь сразу шла о натуральном ряде $\mathbb{N}$.

Чаще вместо $\mathbb{N}$ принято говорить о некотором абстрактном множестве $\mathcal{N}$, добавляя еще две аксиомы,

$$1 \in \mathcal{N} \quad \text{и} \quad n \in \mathcal{N} \Rightarrow \sigma(n) \in \mathcal{N},$$

и доказывая затем *категоричность* (*полноту*) *модели*, т. е. равенство $\mathcal{N} = \mathbb{N}$ с точностью до изоморфизма.

(!) Другие книги параллельно доказывают существование *нестандартных моделей арифметики*. Делается это примерно так. К алфавиту стандартной интерпретации $\{1, 2, \ldots\}$ добавляется новая константа Θ и рассматривается множество замкнутых формул в расширенной сигнатуре

$$T' = T \cup \{\Theta = \bar{1},\ \Theta = \bar{2},\ \ldots\},$$

где $\bar{n}$ обозначает «не n», а $\Theta = \bar{n}$ означает не что иное как $\Theta \neq n$, но знак «$\neq$» изначально отсутствует[6)].

Любое конечное подмножество формул T' содержит конечное число формул

$$\Theta = \bar{n}_1, \quad \ldots, \quad \Theta = \bar{n}_k.$$

Полагая $\Theta = q$, где q — незанятое в $n_1, \ldots, n_k$ число, получаем стандартную *конечную* интерпретацию. Далее решает ссылка на теорему 9.1.1, по которой из существования модели для любого конечного подмножества формул вытекает существование модели для всего множества формул. Затем без труда доказывается неизоморф-

[6)] Такая педантичность, собственно, и является причиной многих «логических неудобств».

ность обычной и нестандартной модели арифметики с алфавитом констант языка $\{\Theta, 1, 2, \ldots\}$.

Контраст существования нестандартных моделей на фоне категоричности приводит к недоразумению. Разнобой объясняется, как правило, скороговоркой насчет различия формальных и неформальных интерпретаций. В принципе, так оно и есть, но здесь имеет смысл особо подчеркнуть проблему, потому что болезнь так хорошо вплетена, что неотличима от здоровой ткани.

Речь идет о двух крайностях. Об аксиоматике как *чисто синтаксической конструкции*, смысл которой может быть придан только извне, и об аксиоматике, изначально обладающей смысловой интерпретацией. Будь возможности разнесены как черное и белое, говорить было бы не о чем. В реальности же любая аксиоматика представляет смесь ингредиентов. Разделить субстанции нелегко, и даже профессионалы то и дело попадают впросак.

Самое сложное заключается в том, что аксиоматика сама по себе даже не обладает определенной пропорцией наличия семантики. Смысл привносит человек. Количество зависит от характера, настроения, погоды, с какой ноги встал и т. п. И все это настолько глубоко интегрировано в суть вещей, что говорить об отделении языковой основы от предметной — можно лишь, пренебрегая диалектикой.

Чтобы почувствовать проблему, достаточно углубиться в любую чисто синтаксическую «на вид» аксиоматику. Скажем, абстрактное определение *группы*[7], в котором ни о какой содержательной интерпретации элементов группы — речь не идет, и потому кажется, что семантика отсутствует. Если «стоять на месте», — оно так и есть. Если же пытаться говорить о группах и делать заключения, то надо предполагать какой-то способ задания группы — таблицу умножения или определяющие тождества. Задавать таблицу умножения, конечно, не надо — иначе это будет уже модель, чисто смысловая конструкция[8]. Надо лишь предполагать возможность задания

[7] Для поиска определения см. предметный указатель.

[8] Интерпретации в виде поворотов или сдвигов в теоретико-групповом срезе к делу не относятся.

и способ. Но тогда не удается избежать примеси семантики, причем иногда субъективной.

Общие рассуждения хороши, безусловно, при наличии в воображении опорных точек. Степень восприятия данного разговора зависит от степени знакомства с программированием и хотя бы поверхностного знакомства с теорией групп. В *проблеме тождества слов*, например, обычный человек считает самоочевидной возможность вставки или исключения рядом стоящих сомножителей $a \cdot a^{-1}$. Программист понимает, что

$$Xa \cdot a^{-1}Y \Leftrightarrow XY$$

должно быть *программно* (если угодно *аксиоматически*) оговорено.

8.3. Аксиоматика Цермело—Френкеля

Нельзя сказать, что парадоксы теории множеств, связанные с рассмотрением «множества всех множеств» [9], производят сильное впечатление. Но для аксиоматизации теории — это был серьезный козырь. Попытки исключить возможность появления парадоксов породили различные системы, среди которых наибольшую известность получила *аксиоматика Цермело—Френкеля*, называемая обычно системой ZF или ZFC, где буква C выделяется специально для *аксиомы выбора*, которая иногда исключается из списка.

Любая теория вынуждена начинать с неопределяемых понятий. В теории множеств — это понятия «множества» и отношения $\in$ «быть элементом». К языку добавляются логические связки и кванторы, с помощью которых строятся все возможные *предикаты* на базе двух элементарных отношений: $x \in y$ и $u = v$. Ничто другое не допускается, но для удобства используются некоторые сокращения:

$$x \neq y, \quad x \notin y, \quad x \subset y.$$

Включение $x \subset y$, например, обозначает

$$\forall z : z \in x \to z \in y.$$

[9] *Парадокс Рассела*: если D — множество всех множеств, не являющихся элементами самих себя, $D = \{x : x \notin x\}$, то: «$D \in D \Leftrightarrow D \notin D$».

Константы в языке (в *сигнатуре*) не присутствуют, но аксиоматически провозглашаются: существование хоть какого-то множества, $\exists\, x : x = x$, и существование *пустого множества*,

$$x = \varnothing \Leftrightarrow \neg\exists\, y : y \in x.$$

Аксиомы существования во многих источниках не присутствуют в списке аксиом, что (наряду с другими нюансами) лишний раз указывает на зыбкость почвы, с которой сталкиваются аксиоматические построения. Цель обойтись минимумом предположений, и тем более обеспечить полную независимость постулатов друг от друга, оказывается недостижима. Получается взаимосвязанная «дышащая» сеть, в которой аксиомы существования, например, обеспечиваются наличием других звеньев.

В основание теории множеств, разумеется, входят логические постулаты. Специфическая часть системы ZFC включает следующие аксиомы.

Z1 *Аксиома объемности.* $\forall\, x : (x \in y \leftrightarrow x \in z) \to y = z$, т. е. множества равны, если и только если состоят из одних и тех же элементов.

Далее предпочтение отдается словесной формулировке. Логическая запись, как более точная, предпочтительнее при других целевых установках.

Z2 *Аксиома пары.* Каковы бы ни были x и y, существует множество z, содержащее x и y (иногда добавляют: только x и y, — что может быть получено в рамках ZF-системы в качестве теоремы).

Z3 *Аксиома отделимости.* Каковы бы ни были x и y, для любого предиката $\varphi(u, v)$ существует множество

$$z = \{t \in x : \varphi(t, y)\},$$

содержащее все $t \in x$, обладающие свойством $\varphi(\cdot, y)$.

Z4 *Аксиома объединения.* Любому семейству множеств $\mathcal{X}$ отвечает множество, содержащее все элементы, входящие в $\mathcal{X}$.

Z5 *Аксиома степени.* Для любого x существует множество 2^x всех подмножеств x.

Z6 *Аксиома бесконечности.* Существует бесконечное множество. Точнее говоря, речь идет о множестве специального вида:

$$\exists\, x : \big[\forall\, z : (z = \varnothing \to z \in x) \wedge \forall\, y \in x : \forall\, z : (z = \sigma(y) \to z \in x)\big],$$

где σ — аналог *функции следования*: $y = \sigma(x)$, если $y = x \cup \{x\}$, т. е.

$$\forall\, z : [z \in y \leftrightarrow (z \in x \vee z = x)].$$

Z7 *Аксиома выбора.* См. раздел 7.3.

Z8 *Аксиома фундирования* постулирует, что не существует бесконечных убывающих цепей, $x_1 \ni x_2 \ni \ldots$.

ZF9 *Аксиома подстановки* [10]. Для любого множества x и функции f, определенной на x, существует множество, состоящее из образов $z = f(y)$, $y \in x$.

8.3.1. Теорема. *Не существует множества всех множеств.*

◀ Если бы такое множество S существовало, то из *аксиомы отделимости* (Z3) вытекало бы существование *множества Рассела*

$$D = \{x \in S : x \notin x\},$$

что приводит к противоречию. ▶

Обозревать нечто без всякой мотивировки довольно трудно. Здесь, однако, легко найти, чем занять, если не мозги, то руки. Определение с помощью дозволенных средств теоретико-множественных операций $\cap$, $\cup$, Δ, $\setminus$ и их свойств — на первой половине дистанции вызывает раздражение, но после наступления второго дыхания может появиться либо спортивный азарт, либо спасительное отвращение.

В любом случае полезно осознавать, что в лице ZFC-системы происходит соприкосновение с грандиозной реальностью, занимающей в виртуальном мире намного больше места, чем египетские пирамиды на Земле. На создание внешне непритязательных аксиоматических систем уходит обычно колоссальное количество ментальной энергии.

Комментарии. ZFC-аксиоматика какими-то частями, как показывает опыт, плохо укладывается в голове, что происходит главным образом из-за фундаментальной человеческой тяги к области некомпетентности [11].

Есть и менее уважительные причины технического характера. Больше всего недоразумений возникает в связи с *аксиомой фундирования* [12] Z8, которая, между прочим, почти без потерь может быть

[10] Эта аксиома как раз добавлена *Френкелем*.

[11] Это явление лежит в основе одного из *законов Паркинсона*, который проявляется во всех сферах человеческой деятельности. В данном случае речь идет о тяге высшего порядка, влекущей за барьер познания, установленный для всей цивилизации.

[12] Введена *Бернайсом* и *Гёделем* в 1941 году, заменила аксиому регулярности *фон Неймана* (1925).

исключена из списка. Конечно, она блокирует *парадокс Рассела*, но с этим справляются и другие аксиомы. Главная роль Z8 в основном философская, обеспечивающая взгляд на мир множеств как на *универсум фон Неймана*, иерархически вырастающий из «ничего».

Важно, пожалуй, обратить внимание на простую деталь, которая часто оказывается причиной недоразумения. В Z8 речь идет о цепях, убывающих не по включению множеств. (!) Запись $x \in y$ не означает $x \subset y$. В $x \in y$ подразумевается, что x — элемент множества y. У натурального ряда $\mathbb{N}$, например, никакое подмножество не является элементом $\mathbb{N}$. Поэтому все цепи в $\mathbb{N}$ обрываются на втором шаге, $k \in \mathbb{N}$ — и все. Но возможны множества иного сорта, скажем,

$$\{1, 2, \{2, 4, \{3, 8\}\}, \{137\}, \{3\}, 3\ldots\}.$$

Здесь возможные цепи длиннее, но не могут быть бесконечными, если Z8 принимается.

За всю историю развития математики в прикладных областях (функциональный анализ, например) никогда не встречались множества с бесконечно убывающими «элементными» цепями. Поэтому аксиома фундирования в большей степени предназначена для философов, чем для математиков.

В первую очередь, конечно, надо было бы сказать об *аксиоме выбора*, но это слишком долгий разговор. Вскользь заметим: Z7 формулируется логически естественно, и выглядит не обещающим неожиданностей утверждением. Однако впечатление обманчиво. С помощью Z7 строится *неизмеримое по Лебегу множество Витали*, а шар разбивается на конечное число частей, которые после перестановки образуют два шара такого же размера (*теорема Банаха—Тарского* [2], именуемая *парадоксом* по эмоциональным соображениям).

8.4. Неевклидова геометрия

Слава и зна́чимость — явления разного порядка. Неевклидова геометрия знаменита, главным образом, кипевшими вокруг нее страстями. «Зна́чимость» тоже довольно высока, но до общеобразовательного курса все же недотягивает. В результате выпадает из педагогического поля зрения — целиком, вместе с некоторыми атрибутами, которые бы имели для математического образования первостепенную важность. Возврату в фокус внимания мешает традиция рассказывать о предмете с обременительными подробностями. Формулы, связывающие углы треугольника на римановой

поверхности, «никому» не нужны. Но этот балласт мешает оценить и впитать понятийную основу фундаментального характера.

История неевклидовых геометрий [13] началась в древней Греции с попыток освобождения обычной геометрии от пятого постулата о параллельных:

Е5 *Через точку, лежащую вне прямой, проходит единственная прямая, не пересекающая исходную, —*

и закончилась через две тысячи лет построением новой *геометрии Лобачевского* с заменой (Е5) аксиомой:

Л5 *Через точку, лежащую вне прямой, проходит по крайней мере две прямые, не пересекающие исходную.*

Долгое время поначалу думалось, что от постулата (Е5) можно отказаться, доказав его как теорему.

Проблема завораживала простотой, но не давалась. Много судеб сфокусировалось на ней. Накал страстей достиг апогея в восемнадцатом веке. Решение стало назревать. То там, то здесь начали появляться догадки и прозрения. Может быть, даже не прозрения, а поиск стал приближаться к месту, где «горячо» [14].

Итальянский монах, *Саккери*, доказывая (Е5) от противного, точнее, предполагая (Л5), двигался путем *Лобачевского*. Результаты опубликованы в 1733 году, но без последствий.

Более основательная попытка аналогичного толка была предпринята *Ламбертом*. Действуя от противного, как и *Саккери*, *Ламберт* получил значительную часть результатов геометрии Лобачевского, но что делать с этим — не знал. Желаемых противоречий не обнаружилось, и он даже высказал невнятное предположение, что такая геометрия может иметь место на некой мнимой сфере (1766).

Затем появилось еще несколько математиков, которые вплотную подошли к созданию «другой» геометрии. Стало совсем «горячо», и тут как раз возник *Лобачевский* со своей стопроцентной убежденностью в возможности построения иной геометрии. Какую при этом космическую задачу он решил? Построил саму геометрию? Да, построил, но это не космический масштаб. Да и нет там особо трудных теорем, и не в теоремах дело.

[13] Далее приводится адаптированный фрагмент из [2].

[14] Так часто бывает при решении крупных проблем. Словно цивилизация решает задачу, как единый биологический организм, о чем свидетельствуют информационно и географически отдаленные, но одновременные всплески.

Глубочайшая проблема была в другом. Человечество воспринимало геометрию как мировую данность. Сколько бы ни говорилось об абстрактном описании точек, линий и плоскостей, — их толкование явно и неявно было физическим. Все, что не соответствовало визуальному опыту, отвергалось. Даже высмеивалось.

«Возня» *Лобачевского* в лучшем случае смотрелась как чудачество. Представьте, некто декларирует «1 = 2» и начинает выводить следствия из разряда «всякое число равно нулю». Разве не то же самое делал Лобачевский? Провозгласил «нелепую» аксиому и стал доказывать издевательские теоремы типа «сумма углов треугольника меньше π».

Что при этом раздражало общественность, так это отсутствие противоречий. Шутника с аксиомой «1 = 2» было бы легко ткнуть носом в несоответствие азам арифметики. Здесь же несоответствия ждали, но оно не появлялось. Дело ведь заключалось не в расхождении получаемых результатов с геометрическим опытом, чего было в достатке, а в противоречии с другими аксиомами. Постулат (Л5) изначально не соответствовал опыту. Поэтому следствия из него были того же сорта, но в этом не было криминала. Другое дело, если бы среди следствий обнаружилось что-нибудь вроде утверждения: «через две точки можно провести две прямые». Тогда бы новая геометрия рухнула, а постулат (Е5) превратился бы наполовину в теорему [15]. Именно такие противоречия искали *Саккери* и *Ламберт*, но не нашли.

Лобачевский, наоборот, противоречий не искал и был уверен, что их нет. Некоторая слабость его позиции заключалась в том, что свою геометрию он считал воображаемой. Потом, конечно, у него появились соображения о геометрии реального мира, но это все же на серьезном уровне оказалось уделом других исполнителей.

Из сказанного ясно, что история на *Лобачевском* закончиться не могла. Прорыв образовался, но процессу требовалось завершение. Не говоря о том, что «сказка» могла в любой момент обернуться блефом, поскольку оставалось две ахиллесовых пяты.

Во-первых, нужна была модель, оправдывающая логические построения. Для аксиоматической системы *Пеано* моделью служат числа с заданными на них арифметическими операциями. Для геометрии *Евклида* — визуальная картина мира. Хотелось подобного, поскольку без реализующей модели логические фокусы остаются привидениями.

Во-вторых, дамокловым мечом нависала проблема непротиворечивости, которая, вообще говоря, неразрешима, но здесь ситуация была особая. Непротиворечивость геометрии *Евклида* тоже неясна, но там порукой определенного благополучия служит наличие реальной модели, интуиция и многовековой опыт. Здесь же — никакой опоры. Там интуиция — «за», здесь — «против».

Напряжение возрастало. Ситуация нуждалась в разрешении. Опять всплыла идея о мнимой сфере, но четко выразить ее не уда-

[15] «Наполовину» — потому что надо было бы отсечь и другое возможное предположение: «любые две прямые пересекаются».

валось. И только в 1868 году (через сорок с лишним лет после первой работы *Лобачевского*) *Бельтрами*, наконец, показал, что новая геометрия выполняется на поверхностях постоянной отрицательной кривизны, и в той же степени непротиворечива, что и анализ.

Решение вопроса геометров не вполне удовлетворило, для чего были определенные основания. Речь все же шла о локальной реализации геометрии *Лобачевского* на псевдосфере (покусочно).

Но вскоре объявился *Клейн* с гениально простой моделью, и ситуация стала совершенно прозрачной. *Клейн* предложил в качестве плоскости — внутренность круга, в качестве прямых — хорды, естественно, без концевых точек. Через точку C проходит целый пучок хорд, не пересекающих AB (рис. 1).

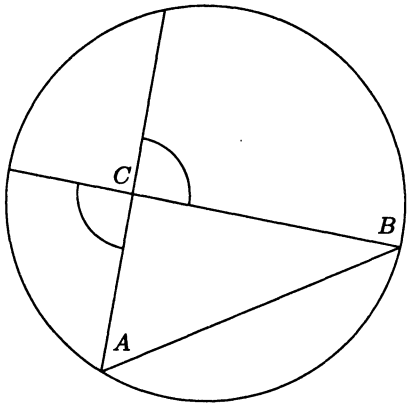


Рис. 1. Модель Клейна

Вот такая модель *геометрии Лобачевского*. Без преувеличения, высший пилотаж! Плюс к тому, поскольку модель строится как подсистема обычной геометрии, то она в той же степени непротиворечива.

Другая сторона медали. Внимание до сих пор было сфокусировано на течении идей. Что и как? Каковы препятствия? Туда ли поток вынес, куда направлялся? Почему долго? Откуда драматургия?

При таком ракурсе исполнители вторичны. Поэтому многие оказались не упомянуты, а там были выдающиеся участники процесса. Младший *Больяи*, получивший те же результаты, что и *Лобачевский*, но волей судьбы оставшийся вторым. Великий среди великих *Гаусс*, построивший ту же геометрию у себя в черновиках «задолго до». Гениальный *Риман*, прочитавший еще в 1854 году выдающуюся лекцию о новом геометрическом подходе, в рамках которого *геометрии Евклида* и *Лобачевского* — простые частные случаи.

Лекцию, правда, никто не понял, иначе бы не пришлось ждать еще 14 лет результатов *Бельтрами*. Интересно, что лекция Римана была опубликована после

смерти автора (в том же 1868 году, что и результаты *Бельтрами*, кстати) — и тут ее поняли сразу все, кому положено.

Но это другая тема, из сферы несогласованности содержания и формы. Исполнитель космического замысла, будучи един в двух ипостасях, еще ест, спит и тянет одеяло на себя, что при доброжелательной позиции вызывает улыбку симпатии, ибо такова природа. Наблюдать эту грандиозную картину — удовольствие и наука, но это совершенно другое занятие, и хорошо бы называть его не историей математики, а как-то иначе.

Еще хорошо было бы уйти от вопроса: «кто первым сказал А», — который всегда портит атмосферу. Один из законов типа Мэрфи—Паркинсона саркастически утверждает: *Ничто не было названо именем первооткрывателя.*

Но в этом нет ничего плохого. Тем более, если таков закон. Идею дарвиновского отбора, например, можно встретить еще у древних. Формула *Эйнштейна* $E = mc^2$ открыта *Хэвисайдом*, закон *Бойля—Мариотта* — *Гуком*, преобразования *Лоренца* — трудно вспомнить кем, но во всяком случае — не *Лоренцем*.

И не в плагиате дело. Ремарка *Ньютона*: «я стоял на плечах гигантов» — всегда применима при озарениях. Нет ни одного случая, когда бы идея родилась в голове отдельного индивида без подготовки, толчка, прообраза. И как тогда быть? Покинуть плечи гигантов или расшаркиваться всю последующую жизнь? Времяпровождение в реверансах не всем нравится. К тому же, не надо забывать, какая чаша перевешивает. *Гауссу* и *Ньютону* можно простить все. Всем все можно простить. Тем более, и прощать нечего, если разобраться. На чей счет отнести данное извне? Язык, стереотипы, подсознательные заимствования, перекрестное опыление, — не считая Ритмов Вселенной и нашептывающих голосов. Не смешно ли регистрировать законы Космоса на свою мимолетную фамилию?

Три-четыре сотни лет назад атмосфера в этом плане была намного лучше. Открытия шли валом, и к ним не было такого ревнивого отношения, как сейчас. Упомянутый *Гук*, например, их совершил несколько сотен, а что ему досталось в награду? Что названо его именем? Один только закон упругости: «сила пропорциональна сжатию», — и все. Но бить в набат по этому поводу не резон. Ситуация изнутри была специфической. Английская академия наук обязала *Гука* регулярно демонстрировать новые законы природы, что граничит с анекдотом. Так или иначе, но *Гук* под давлением контракта был вынужден поддерживать очень высокие обороты. Из общих соображений разумно предположить, что кое до чего он додумывался сам, кое-что разведывал, кое-где надувал щеки, а кое-где и вешал лапшу на уши, ибо бытие частично определяет сознание. Поэтому решать здесь вопросы, где что и что чье, — дело неблагодарное и бесперспективное.

Кроме того — самый важный аспект (!) — у каждого открытия есть нечто вроде критической массы. Пока она не достигнута — говорить не о чем. Кто-то думает, что должно быть так-то и так-то, или даже уверен, но на пустом месте. Это что угодно, но не открытие. *Гук*, между прочим, по-видимому, действительно первый сообразил, что гравитационное притяжение должно быть обратно пропорционально квадрату расстояния. И сказал *Ньютону*. И это впоследствии породило крупнейший приоритетный спор.

Что касается *Лобачевского*, то он, безусловно, первый преодолел эту самую критическую массу неевклидовой геометрии.

Возвращаясь к «течению идей», приходится обратить внимание на некоторые детали. Кое-где мы воспользовались тем обстоятельством, что ложь — лучший инструмент объяснения. Но это тактически. Стратегически выгоднее, конечно, говорить правду. Потому что быстро понятая вещь назавтра превращается в неразрешимую головоломку.

Подобное опасение возникает в связи с *моделью Клейна*. При попытке расставить точки над i могут возникнуть проблемы. Дело в том, что если позаботиться о справедливости не только пятого постулата (Л5), но и остальных аксиом, то движения, расстояния и углы приходится определять особо — на основе проективных преобразований. Вместо обычного расстояния, например, берется так называемое ангармоническое отношение четверок точек. Что это такое — неважно. Просто те самые детали, в которых прячется дьявол. Ничего сложного, но простота смазывается, и возникает простор для непонимания. Поэтому на семинаре у *Вейерштрасса* (1870) молодому *Клейну* дали от ворот поворот. И только через год *Клейн* «дожал» ситуацию, хотя и после этого у него остались противники.

На такого рода примерах интересно понять, почему даже простые вещи нередко воспринимаются в штыки. Попытка разобраться всегда походит на детектив. Всплывают подробности, радикально меняющие картину. Так и здесь. Во-первых, оказывается, *модель Клейна* была изобретена не *Клейном*, а *Кэли*, но для других целей — как реализация неких идей в области проективной геометрии. *Клейну* же пришло в голову, что на этой модели реализуется *геометрия Лобачевского*. Во-вторых, первоначальная целевая установка модели продолжала играть чуть ли не мистическую роль. Вместо того чтобы ограничиться фактом реализации неевклидовой геометрии, *Клейн* уходил в дебри взаимоотношения геометрий (Евклида, Лобачевского и проективной), где возникала путаница, и плодились противники, включая самого *Кэли*.

Картина событий, вообще говоря, неполна без *модели Пуанкаре*, но мы ограничимся лишь упоминанием. «Плоскостью» в этой модели служит, например, открытая полуплоскость, «прямыми» — полуокружности, как на рис. 2, и вертикальные полупрямые (как полуокружности бесконечного радиуса).

Справедливость (Л5) легко проверяется, что же касается других аксиом — возникают препятствия, которые изящно преодолеваются, но несколько услож-

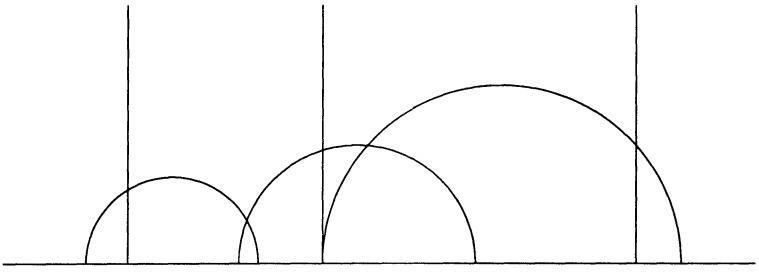


Рис. 2. Модель Пуанкаре

няют модель. Для придания естественности некоторым определениям *Пуанкаре* изобрел даже «температурный трюк» — см. [2, гл. 17].

Наконец последнее. Эффект драматургии всегда зависит от последовательности изложения. При перестановке нескольких фрагментов текста детектив превращается в протокол. Незначительная перестановка событий в описанном историческом процессе могла бы ликвидировать накал страстей и значительно опустить рейтинг неевклидовой геометрии. Причина и автор детективной организации событий в данном случае неизвестны.

Для справки упомянем остальные аксиомы Евклида, в современном изложении и с некоторыми натяжками и дополнениями, сделанными в последние 200 лет. Фактически это группы аксиом.

E1
- *Через две различные точки проходит одна прямая* [16].
- *На любой прямой есть две различные точки.*
- *Существуют три точки, не лежащие на одной прямой.*

E2
- *Из трех различных точек на прямой одна лежит между двумя другими.*
- *Между точками A и B на прямой есть бесконечно много других точек.*
- *Точка на прямой разделяет остальные точки на два класса так, что сама лежит между любыми точками из разных классов.*
- *Прямая делит плоскость на две области.*

E3 ***аксиомы движения***
- *Движение переводит отрезок в отрезок, угол в угол.*
- *Движения образуют группу.*

[16] Точнее: одна и только одна, но такие уточнения здесь опускаются.

- *Некоторые скучно формулируемые характеристики, связанные с существованием специальных движений для трех точек, находящихся в общем положении.*

E4 ***аксиомы непрерывности***

- *В варианте Дедекинда опираются на дедекиндовы сечения.*

E5 • *Через точку, лежащую вне прямой, проходит единственная прямая, не пересекающая исходную.*

Если стать в положение компьютера, об этой аксиоматике можно сказать много интересного.

8.5. Гипотеза континуума

Гипотеза континуума (ГК) [17] высказана *Кантором*, и состоит в предположении, что всякое бесконечное подмножество $[0, 1]$ либо счетно, либо равномощно $[0, 1]$. На языке «*алефов*» это формулируется как $2^{\aleph_0} = \aleph_1$, но при этом требуется опора на *аксиому выбора* (АВ).

Гёдель (1939) установил, что если система ZF непротиворечива, то она остается непротиворечивой и после присоединения ГК и АВ в качестве аксиом.

Коэн (1963) закрыл проблему, разобравшись заодно и с аксиомой выбора. Вот формулировка его результатов [11].

8.5.1. Теорема. *Если теория ZF непротиворечива, то гипотеза континуума не является теоремой теории ZFC.*

8.5.2. Теорема. *Если теория ZF непротиворечива, то аксиома выбора не является теоремой теории ZF.*

В итоге: к ZF можно с равным успехом добавить как ГК, так и ее отрицание. Причем ГК в некотором роде претендует на роль утверждения, которое ни при каком расширении ZF (детали в [11]) не может стать теоремой. Получается некий аналог высказывания (2.2).

[17] В знаменитом списке гильбертовых проблем стоит под номером один.

Глава 9

Теория моделей

Спектр моделирования весьма широк, от конкретизации до абстрагирования. В том же диапазоне находится и вся математика.

9.1. Логический аспект

Теория моделей как математическая дисциплина, которая примыкает к логике, направлена в основном на оправдание логических схем и аксиоматик. Центральная идея заключается в проектировании абстракции на что-нибудь реальное, с последующим выводом о непротиворечивости существующего. Безусловно, аксиоматики характеризуются и другими факторами [1], однако *непротиворечивость* играет наиболее существенную роль.

Напомним некоторые понятия и факты, относящиеся к данной теме. *Интерпретация языка* — есть преобразование φ множества C *констант языка* в некоторое множество M, сопоставляющее функциональным (и предикатным) символам f над C — функции f_φ над M, которые принимают значения 0 или 1.

При заданной *интерпретации* подстановка в $f_\varphi(\ldots)$ конкретных значений переменных дает «истину» или «ложь» — 1 или 0. Любые *замкнутые формулы* (не содержащие свободных переменных) являются высказываниями и также принимают значения 1 или 0.

***Моделью** множества A замкнутых формул называется интерпретация, в которой истинны все формулы из A.*

Множество A замкнутых формул может быть, в частности, совокупностью аксиом, из которых выводятся другие замкнутые формулы, $A \vdash f$, и такой процесс расширяет A до *теории* T. В силу полноты исчисления предикатов семантическое ($\models$) и синтаксическое ($\vdash$) расширение дает в итоге одинаковый результат.

---

[1] Степенью полноты, например. Система с единственной аксиомой $a + b = b + a$ слишком многое вмещает. Аксиоматика считается *полной*, если все модели порождаемой теории изоморфны друг другу.

Множество A замкнутых формул считается ***непротиворечивым****, если из него нельзя вывести два противоположных утверждения f и $\neg f$.*

Теорема 5.8.2. *Множество замкнутых формул, имеющее модель, непротиворечиво.*

Теорема 5.8.3. *Если аксиоматизируемая теория полна и непротиворечива, то она разрешима.*

Теорема 2.3.1. *Если теория T непротиворечива и содержит в себе арифметику, то непротиворечивость T недоказуема в T.*

Нокаутирующий удар по рассматриваемой проблематике наносит

Теорема 2.4.3. *Существуют системы аксиом, «порочность» которых принципиально нельзя обнаружить.*

Здесь речь идет о «неправильности» аксиоматики, которая видна *Всевидящему Оку*, но принципиально не может быть проверена, — и в этом смысле о ней можно не беспокоиться. Этакая странная картина: противоречия есть, но изнутри не могут быть выявлены (см. раздел 2.6).

Совершенно иная ситуация возникает в *арифметике Пеано*. Теорема 2.3.1 оставляет форточку для выхода из положения, но это путь в бесконечность (раздел 9.2).

Заметим, что в противоречивой теории, в которой выводится как некоторая формула f, так и $\neg f$, — *выводится любая формула*, поскольку $\neg U \to (U \to V)$, т. е. из ложного утверждения выводится что угодно.

Именно поэтому любая модель обязана наследовать противоречивость теории. И если хоть какая-то модель свободна от такого рода неприятностей, — теория непротиворечива.

В ситуации, когда теория охватывает бесконечное множество X формул, конкретные утверждения «замыкаются» на конечные подмножества. Например, если X противоречиво, то противоречиво и некоторое его конечное подмножество — *по той простой причине, что любой вывод конечен*, т. е. цепочка, ведущая к противоречию, содержит конечное число формул. Та же причина с учетом теоремы 5.8.2 приводит к следующему утверждению.

9.1.1. Теорема. *Если любое конечное подмножество $S \subset X$ замкнутых формул имеет модель, то и X имеет модель.*

Арифметика натурального ряда — интерпретация или модель?

9.2. Что стоит за результатами Генцена

Теорема 2.3.1 — есть теорема, и строгое обоснование непротиворечивости обязано выйти за пределы рассматриваемой области и опереться на новые предположения либо — на интуицию. Поэтому проблема непротиворечивости по большому счету принципиально не решается. Конечно, ее можно передвигать с места на место, сводя правильность одних механизмов заключения к правильности — других. Иногда это дает осязаемый результат. Например, *модель Клейна* сводит проблему непротиворечивости *геометрии Лобачевского* к непротиворечивости *евклидовой геометрии*, имеющей, в силу интуитивной убедительности и многовековой истории, солидную репутацию. Понятно, что статус неустоявшейся дисциплины в этом случае сразу возносится на максимально возможную высоту.

Попытки иного рода — сведение геометрии к теории чисел, например, — выглядят менее убедительно, но и они имеют определенный смысл, ибо сливают воедино опыт безошибочного развития независимых направлений.

На какой-то стадии подобного коловращения наступает момент, когда возникает идея двигать проблему «за пределы», вместо ее перепасовывания между имеющимися областями. В результате задача передается в метатеорию доказательств [5], т. е. «выносится за скобки», ибо какой резон останавливаться на втором метауровне? Поднимаясь по метаступенькам, можно вводить новые метааксиомы, каждый раз праздновать успех и двигаться дальше, сознавая, что процесс не имеет конца.

Особого упоминания в данном контексте заслуживают результаты *Генцена*[2)], доказавшего, как принято говорить, непротиворечивость арифметики. Это, конечно, чересчур. Более адекватные варианты звучат так: непротиворечивость арифметики сведена к непротиворечивости анализа либо — установлена с дополнительным использованием трансфинитной индукции. С определенными натяжками это соответствует действительности. С другой стороны, если сравнивать надежность фундамента арифметики и анализа,

[2)] Основные результаты Генцена опубликованы в сборнике [17].

то еще вопрос «чья возьмет». Арифметика представляется более самодостаточной, а интуиция, жонглируя целыми числами, реже ошибается.

Безусловно, непротиворечивость арифметики Пеано интуитивно кажется вполне естественной. Все аксиомы и правила вывода выглядят «правильными», а последовательность правильных шагов не может привести к ошибочным результатам, как хотелось бы думать.

Если 10 налогоплательщиков имеют по 100 гусей каждый, то отбор гусей у четверых и раздача остальным по кружке пива — большинством одобряется. Продолжение в том же духе изымает в итоге всю домашнюю птицу, но на каждой итерации коллектив голосует «за». Пример иллюстрирует типичную ситуацию, когда «шаги хороши, результат — плох».

Несмотря на такие параллели, вера в непогрешимость математической индукции у широких слоев населения достаточно крепка. Даже парадоксы теории множеств не вызывают особого беспокойства, потому что кажется, будто причина там не вполне серьезная, ибо даже точно не локализуется, словно равномерно размазана. Хотя именно поэтому компрометируется система рассуждений целиком.

9.3. Парадокс Сколема

Группа результатов о возможности перехода к моделям другой мощности (*теорема Лёвенгейма—Сколема* и ее вариации)[3] порождает следующую иллюзию, называемую *парадоксом Сколема*. Все утверждения теории множеств, выполнимые в континуальных моделях, — по теореме 5.8.6 выполнимы и в счетных моделях. Как быть тогда с теоремами *Дедекинда* и *Кантора*, связанными с существованием *континуума*?

При определенном складе психики мираж подобного розыгрыша производит столь сильное впечатление, что привлекаются объяснения чуть ли не мистического толка. *Континуум*, дескать,

[3] Теоремы 5.8.5, 5.8.6.

на самом деле *счетен*, и существует его *взаимно однозначное соответствие* с натуральным рядом. Но это «соответствие» не находится внутри модели теории множеств, а принадлежит *метатеории*, — что и разрешает парадокс.

Трюк придуман *Сколемом*, и разукрашенные варианты упрочились в литературе в виде стандартного объяснения. В результате мир, где *континуум можно пересчитать, хотя бы в метатеории*, — стал выглядеть менее скучно. При этом нельзя сказать, что объяснение не годится. Если договориться о подобающей терминологии, все именно так и выглядит [4)].

Однако реальное положение дел тоже заслуживает внимания, ибо тогда яснее становится, что стоит за предположениями и теоремами.

Откуда берется *континуум*? Из конечного рассуждения. В несколько шагов доказывается невозможность пересчитать числа, после чего в один шаг (от противного) делается заключение о несчетности. «Посадочная площадка» в виде континуума приготовлена заранее, и подмена происходит уже без каких-либо усилий на основе *закона исключения третьего* [5)], — почему, собственно, последний и вызывает столько споров.

Так или иначе, *континуум имеет счетное происхождение* в результате *конечного тасования* счетного множества рациональных чисел. Континуальность, как таковая, это уже из области художественного вымысла. Поэтому в теории, опирающейся на счетную аксиоматику и конечные выводы, — реальному континууму нет места. Разве что договориться об условном названии некоторых результатов, что, собственно, и произошло.

Если же говорить о «метатеории», то соответствие с натуральным рядом, упомянутое выше, может быть не с вещественными числами, а со счетными описаниями континуума.

Отмеченное выше разногласие возникает, конечно, не только из-за «*Кантора* и *Дедекинда*». Любое утверждение анализа, где речь идет о вещественных

[4)] Можно договориться также, что продающий газеты автомат способен диагностировать честность граждан, не давая газеты тем, кто не опускает монету.

[5)] В теории алгоритмов на основании того же закона и того же диагонального рассуждения из несчетности делается другой вывод, о невычислимости.

$\varepsilon \to 0$ либо трансцендентных функциях, опирается на «состоявшуюся» бесконечность. Переход к счетным моделям может означать в этих случаях замену, например, $\varepsilon \to 0$ на $\varepsilon = 1/n \to 0$ при $n \to \infty$, а *теорема Лёвенгейма—Сколема* будет гарантировать, что потери смысла не происходит, хотя краски — блекнут.

9.4. Модели булевых структур

Булева структура в разделе 5.3 описывалась сразу с помощью модели теоретико-множественной интерпретации, что позволяло за рябью формул видеть скелет привычной конструкции. Но это делало незаметной роль модели. Поучительно тот же сюжет разыграть иначе, начиная с голой системы аксиом и не предполагая никакой содержательной подоплеки.

Стерильно буквенная аксиоматика в этом случае производит мрачное впечатление [6]. Главный вопрос в таком сценарии: «не противоречат ли формулы друг другу», — на который только содержательная модель может дать положительный ответ. Интерпретация сразу показывает, что «все в порядке», и тогда проливается дополнительный свет на результаты типа теоремы 5.8.2 — «теория непротиворечива, если имеет модель».

Противоречива ли формула

$$\boxed{\exists x : P(x) \to \forall x : P(x)} \; ?$$

Непротиворечива [7]. Потому что существует модель, в которой x может принимать единственное значение, и в этой модели — формула верна.

Конечно, интерпретация булевой структуры как системы подмножеств некоторого «основного» множества E — имеет универсальный характер. Однако все подмножества E рассматривать необязательно [8]. В то же время любые системы подмножеств тоже не годятся, поскольку операции (сложения, умножения и дополнения) не должны выводить из системы.

---

[6] Конечно, если хорошо вжиться в роль, забыв о существовании модели.

[7] Но не общезначима.

[8] Крайний вариант системы двух подмножеств $\{\varnothing, E\}$, изоморфный логической интерпретации «истина — ложь», рассматривался в главе 5.

Если говорить о конечных интерпретациях, то аксиоматике могут удовлетворять только системы подмножеств в количестве 2^k. (?) Поэтому для трехзначной логики, например, булева основа не подходит.

Универсализм теоретико-множественных интерпретаций иногда заслоняет идеологические конструкции иной природы, которые обнаруживают в тех же структурах совершенно другие аспекты. Например, введение на отрезке $[0, 1]$ операций:

$$a + b = \max\{a, b\}, \quad a \cdot b = \min\{a, b\}, \quad \bar{a} = 1 - a,$$

порождает булеву структуру [9]. Модель подключает к анализу факты, добытые совсем в другой области.

Непохожая модель, но опять-таки с булевой структурой, возникает при введении операций

$$a + b = \text{НОК}\,\{a, b\}, \quad a \cdot b = \text{НОД}\,\{a, b\}, \quad \bar{a} = \frac{N}{a}.$$

на множестве делителей некоторого числа N, которое представляет собой произведение простых чисел в первой степени.

Модели начинают конкурировать и обогащать друг друга, расширяя заодно представления о гибкости и вместимости абстрактной схемы. Детали и уточнения по поводу рассмотренных моделей см. в [28].

9.5. Как модель разрушает схему

Конечно, разрушение и созидание — две стороны одного явления. Зависит — как смотреть.

Пример *HSI-проблемы Тарского* (раздел 4.2) дает красноречивый образец на обозначенную в заголовке тему, а также подводит к другой мысли: «разрушить схему может только модель». Разумеется, если схема грубо противоречива сама по себе, она рухнет под собственным грузом. Но ситуации «общего положения» иногда очень сложны.

[9] С точностью до некоторых оговорок [28].

Напомним, *HSI-проблема Тарского* заключалась в предположении, что все арифметические тождества с участием *сложения*, *умножения и возведения в степень* могут быть доказаны в рамках аксиоматической схемы, использующей только обычные свойства перечисленных операций.

Положительное решение — не давалось, а для отрицательного — требовалось нечто неординарное. Оставаясь в рамках обычной арифметики, ответ «нет» получить было невозможно. Как наличие пистолета в принципе можно доказать, а отсутствие — нельзя, так и здесь. Какие-то тождества не доказываются с помощью разрешенных средств, но это вовсе не гарантирует отсутствия подходящих доказательств. На поиск «разрушающей» модели за пределами арифметики ушли сотни человеко-лет, и конструкция в конце концов была найдена (см. раздел 4.2).

Идея моделирования в определенном смысле универсальна и работоспособна далеко за пределами чисто алгебраических схем типа «$a + b = b + a$». Под соответствующим углом зрения полезно взглянуть на многие задачи, имеющие вроде бы иную природу.

Требуется накрыть фишками домино фигуру, полученную из клетчатого квадрата 10 *на* 10 *удалением двух клеток на одной из диагоналей. Каждая фишка накрывает две клетки.*

◄ Допустим, исходный квадрат был раскрашен как шахматная доска. Тогда удаленные клетки, будучи расположенными на общей диагонали, имеют одинаковый цвет. Фишка же домино накрывает две клетки разного цвета. Поэтому накрыта может быть только фигура, имеющая одинаковое количество черных и белых клеток. ►

Возможность раскраски — та самая свобода маневра в задаче, которую не всегда легко заметить, но с той или иной пользой для дела — можно распорядиться.

Циник скажет, что «моделирование» здесь притянуто за уши. Раскраска, дескать, не модель, а удачное соображение. Но «удачное соображение» — это «ничто», которое никак не освещает ни одну другую задачу. Наша беда часто в том и заключается, что, добиваясь успеха, мы не задумываемся о причинах. Поиск ответа на вопрос «почему» — способен выводить на ту или иную позицию, вызывающую ассоциации, на выработку «угла зрения», с которого видна общность разнородных явлений. Даже плохой ответ в этом направлении кое-что дает.

Конечно, можно считать, что речь идет о типичной ситуации поиска контрпримеров. Но при такой расстановке акцентов теряется руководящий принцип в нестандартных положениях. Предъявление корня $P(x)$ для гипотезы $\forall\, x : P(x) \neq 0$ — тоже контрпример, но он низводит идею до пресного варианта. Однако даже в тех случаях, когда изобретательность и неожиданность выходят на первый план, кажется, будто имеется в виду поиск в заданном секторе.

Это не так в приведенном выше простом примере (раскраска клеток — вещь явно не предусмотренная заранее), и это не так во многих знаменитых контрпримерах, так или иначе повлиявших на развитие научных дисциплин. Скажем, на *канторову лестницу* [10] можно смотреть как на любопытный эпизод, фрагмент, но это модель целого явления, играющего принципиальную роль в теории меры, — и которое не так легко было обнаружить.

Нечто подобное можно сказать о фигурах, не имеющих площади; о недифференцируемых функциях; о неполных функциональных пространствах и т. п. Все это модели, выявляющие слабые звенья различных теоретических схем.

9.6. Абстрактные и конкретные модели

Взаимоотношения аксиом и моделей чаще воспринимаются в направлении «абстрактное $\Rightarrow$ конкретное». Дескать, аксиома

$$a \times b = b \times a$$

слишком «пуста», модель обязана быть более конкретной, менее абстрактной. Пусть, мол, a и b будут — хотя бы числами.

На самом деле, проблема в другом. Аксиомы часто не определяют операции, фиксируя лишь их свойства. В стиле: пусть $\times$ будет чем угодно, но — коммутативным. Поэтому на модель ложится задача подобрать «вариант», который вовсе не обязан быть чем-то «реальным».

Хороший пример — *идеальные числа Куммера*, исторически возникшие в русле исследований по *теореме Ферма*, в доказательствах которой было много «проко-

[10] Непрерывная монотонная функция $f(x)$, производная которой почти всюду равна нулю, тем не менее $f(x)$ на $[0, 1]$ успевает вырасти от 0 до 1, — см. [3, т. 5].

лов» в связи с необоснованным применением основной теоремы арифметики к объектам иной природы.

В частности, *Ламэ* и, независимо, *Куммер* в середине девятнадцатого века предложили «доказательства», опирающиеся на манипуляции с числами вида

$$a_0 + a_1\zeta + \ldots + a_{n-2}\zeta^{n-2}, \tag{9.1}$$

где коэффициенты a_k — целые, а

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Авторы поначалу не заметили, что числа (9.1) не разлагались *единственным образом*, подобно числам натурального ряда, на простые множители (неразложимые далее).

Выстрел, казалось, получился холостым, но Куммер сделал гениальный ход, дополнив множество (9.1) фиктивными числами. Единственность разложения на простые множители была восстановлена, доказательство заработало! Правда, не на полную мощность — фикция привнесла свои трудности, — но идея эксплуатации вымысла получила новый импульс.

Не вдаваясь в подробности, суть дела можно пояснить примером *короткой арифметики Гильберта* на множестве G чисел вида $4k + 1$,

$$G = \{1, 5, 9, 13, 17, \ldots\},$$

с единственной операцией обычного умножения, не выводящего из G.

Число 693 в G раскладывается на простые множители двумя способами:

$$693 = 21 \cdot 33 = 9 \cdot 77.$$

Сомножители 9, 21, 33, 77 просты в G. Единственность разложения (числа 693) восстанавливается введением в G фиктивных чисел, удовлетворяющих равенствам

$$\alpha\beta = 9, \quad \gamma\delta = 77, \quad \alpha\gamma = 21, \quad \beta\delta = 33. \tag{9.2}$$

Числа фиктивны, конечно, для G. Обычным решением системы (9.2) является

$$\alpha = \beta = 3, \quad \gamma = 7, \quad \delta = 11. \tag{9.3}$$

Возможность натурального решения (9.3), конечно, снижает эффект чуда, однако «натуральность» имеет смысл лишь для внешнего наблюдателя. Внутри G числа 3, 7, 11 ничем не лучше букв α, γ, δ. В конце концов, фикция $i^2 = -1$ служит образцовым примером раскрепощенного моделирования. Жаль только, что привычка перевернула представления. Обычная единица ничуть не реальнее мнимой.

Возвращаясь к исходному вопросу, подчеркнем еще раз, что мера абстракции в модели не обязана быть ниже, чем в аксиоматике. Сконструировать модель группы, например, означает одно — определить групповую операцию, которая бы удовлетворяла аксиомам группы. Для этого достаточно задать «таблицу умножения»: $g_i \times g_j = g_k$. Что такое g_i не играет роли. Без содержательной опоры создание «таблицы» — нелегкая работа, но это другой вопрос.

9.7. В чем состоит общая идея

Предмет разговора значительно размыт, ибо к моделированию сводится едва ли не вся математика. Везде, где одна система объектов отражается в другую — изоморфно или с соблюдением лишь некоторого сходства, с искажениями дозволенного характера, с умеренным приобретением новых свойств и потерей старых, — везде в таких случаях можно говорить о моделировании. Употребление термина, конечно, необязательно, но оно подталкивает мысль в продуктивных направлениях. Потому что нет трудных задач, есть плохие точки зрения.

Хороший пример — игра «Ним». *В каждой кучке по n_k спичек. Двое берут по очереди любое количество ($\geqslant 1$) спичек, но каждый раз только из одной кучки. Кому в итоге нечего брать, — тот и проиграл.*

Выглядит просто, однако выигрывающий алгоритм найти — трудно, пока не приходит идея записать все n_k в двоичной системе. Тогда вычисляется поразрядная сумма σ всех n_k по модулю 2: если сумма единиц в разряде четная, пишется 0; если нечетная — 1. Чтобы выиграть, надо противнику все время оставлять σ из одних нулей [11].

Вот такая модель, внутри которой ситуация совершенно прозрачна. Усмотреть «двоичную природу» задачи, вообще говоря, трудно, и подобное «попадание в десятку» случается редко. Если задача из задачника, умышленно замаскированная идея вскрывается, как правило, легче. Хотя — зависит, кто прятал.

Еще один пример. На рисунке 3 три хорды пересекаются в одной точке. Не бог весть какая теорема, но в данном случае интересна модель, делающая результат очевидным. На окружности надо поставить полусферы, пересечения которых в проекции на исходную плоскость будут хордами. Результат становится очевиден.

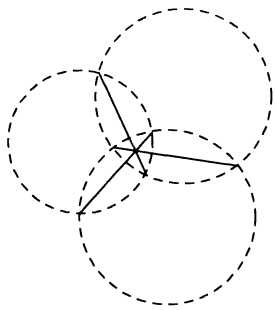


Рис. 3

Такие задачи, где «лишнее» не убирается, а навешивается, — доставляют определенное удовольствие своей нестандартностью. Плоская модель переводится в объемную. Не обязательно в геометрическом

[11] В чем состоит выигрывающий алгоритм, если каждый раз спички можно брать из двух кучек?

смысле. В том же ключе можно интерпретировать задачу о накрытии фигуры фишками домино (раздел 9.5), где «выход в пространство» обеспечивает *раскраска* фигуры. В том же ключе естественно интерпретируются и многие задачи негеометрического характера.

Доказывать, например, что сумма квадратов

$$1^2 + 2^2 + \ldots + n^2$$

является квадратом некоторого $m \in \mathbb{N}$ не очень удобно. Да и непонятно как. Матиндукция «в лоб» не действует — чем-то задача нехороша. Слишком слабое утверждение. Навешивание деталей все ставит на свои места. На «усилении»

$$1^2 + 2^2 + \ldots + n^2 = (1 + 2 + \ldots + n)^2$$

индукция легко работает.

Интересно, что с этих же самых позиций можно расценивать алгоритмическую кухню. Машины Тьюринга, нормальные алгоритмы Маркова, канонические системы Поста, диофантовы уравнения — все это модели, выросшие из общего ядра «вычислимости» и представляющие собой выходы в другие пространства по отношению друг к другу.

9.8. Конечные базисы

В алгебраической системе A (с одной или несколькими операциями над элементами) естественно возникает вопрос о конечной совокупности тождеств S, из которых следуют все остальные тождества A. В этом случае S называют *конечным базисом*, каковой является в некотором роде системой аксиом для A при специфически ограниченном угле зрения.

• В качестве примера еще раз упомянем *HSI-проблему Тарского*, столкнувшуюся с отсутствием конечного базиса для арифметических тождеств с участием *сложения, умножения и возведения в степень*.

Проблема конечности базисов тождеств — довольно популярное направление исследований, на котором здесь нет смысла подробно останавливаться [12], но там есть один любопытный аспект

[12] См. обзор: *Бахтурин Ю. А., Ольшанский А. Ю.* II. Тождества // Современные проблемы математики. Фундаментальные направления. **18**. М.: ВИНИТИ, 1988. С. 117–240.

с точки зрения неразрешимости и доказуемости. Ограничимся двумя примерами полугрупп.

Напомним, *полугруппой* называют множество G с определенным на парах его элементов *ассоциативным* «умножением». Полугруппы могут задаваться «таблицами умножения», а также с помощью *определяющих соотношений* (*тождеств*).

Наиболее эффектно выглядят тождества в *конечных* полугруппах, не имеющие *конечного базиса*. Минимальная полугруппа такого сорта состоит из шести матриц

$$\begin{bmatrix}0&0\\0&0\end{bmatrix},\quad \begin{bmatrix}1&0\\0&0\end{bmatrix},\quad \begin{bmatrix}0&1\\0&0\end{bmatrix},\quad \begin{bmatrix}0&0\\1&0\end{bmatrix},\quad \begin{bmatrix}0&0\\0&1\end{bmatrix},\quad \begin{bmatrix}1&0\\0&1\end{bmatrix},$$

с матричным умножением в качестве полугрупповой операции. В полугруппе всего 6 элементов, $G = \{g_1, \ldots, g_6\}$, любое произведение $g_i g_k$ не выводит из G, но тождеств бесконечно много, причем несводимых ни к какой конечной совокупности [13].

Другой наглядный пример. Перестановки обычно принято записывать в виде

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}.$$

По аналогии под

$$g = \begin{pmatrix}1&2&3\\i&j&k\end{pmatrix}$$

будем подразумевать отображение g «точки» $\{1, 2, 3\}$ в «точку» $\{i, j, k\}$, где каждое i, j, k может принимать три значения: 1, 2 или 3. Понятно, что отображений рассматриваемого вида всего $27 = 3^3$. Взяв композицию отображений в качестве полугрупповой операции, получаем конечную полугруппу

$$G = \{g_1, \ldots, g_{27}\},$$

тождества в которой, как оказывается [14], не имеют конечного базиса.

Мы оставляем в стороне обоснования, поскольку хотим обратить внимание лишь на один аспект. В том и другом случае за счет искусственного ограничения средств возникает совокупность тождеств, сидя *внутри* которой невозможно дать эффективную аксиоматизацию системы. Иными словами, никакая конечная

[13] *Перкинс П.* Базисы для эквациональных теорий полугрупп // Киберн. сб. 1974. № 11. 5–23.

[14] *Волков М. В.* О конечной базируемости многообразий полугрупп // Матем. заметки. 1989. **45**. № 3. 12–23.

[*внутренняя* (!)] аксиоматика не позволяет сделать все тождества доказуемыми. Однако выход за пределы системы дает конечный инструмент для доказательства любых тождеств. В последнем случае, например, для проверки тождества $x^2 = x^8$ достаточно вместо x подставить последовательно $g_1, \ldots, g_{27}$, — и убедиться в соблюдении равенства.

Мысль о возможности чего-то подобного для арифметики бесперспективна. Там ограничения имеют абсолютный характер [15], и никакие выходы «за пределы» не способны кардинально изменить ситуацию.

[15] Эквивалентом соответствующей «абсолютности» является *тезис Чёрча*.

Глава 10

Степени неразрешимости

Изучение перечислимых множеств направляется двумя силами. Осмысленными установками и тенденцией к расширению. Неуправляемый рост обеспечивает работой математиков, но иногда ведет к открытиям, на которые трудно было рассчитывать.

Нижеследующий текст преследует несколько странную, на первый взгляд, цель — показать, что рассматриваемая область не для «общего образования», и на нее не стоит тратить время в ущерб решению более важных задач типа продолжения рода.

10.1. Сводимость

Отношения порядка и эквивалентности на изучаемых совокупностях позволяют выявлять структуру и, тем самым, лучше «видеть». Что касается вычислимости, было бы желательно понимать, все ли неразрешимые множества «одинаково неразрешимы» либо есть какая-то иерархия. Понятие сводимости одних задач к другим — порождает некое упорядочивание задач по сложности.

Читателей, у которых хватает проблем за пределами рассматриваемой тематики, необходимо предупредить, что культурное и философское ядро алгоритмического взгляда составляют другие ингредиенты. Неразрешимые задачи, теоремы Гёделя — вот стержневые факты, обеспечивающие прорыв в другое пространство, из которого мир по-другому видится. А наведение порядка — удел профессионалов. Поэтому технические подробности далее в основном игнорируются. Подробная информация о сводимостях и степенях неразрешимости имеется в [23, 27], см. также [4, 13].

Множество $X \subset \mathbb{N}$ называют m-*сводимым* к $Y \subset \mathbb{N}$, что обозначается как $\boxed{X \leqslant_m Y}$, если существует такая *всюду определенная* вычислимая функция $f(x)$, что

$$x \in X \quad \Leftrightarrow \quad f(x) \in Y. \tag{10.1}$$

В случае $X \leqslant_m Y$, $Y \leqslant_m X$ множества X и Y называют ***m*-эквивалентными** и пишут $X \equiv_m Y$.

Отношение $\leqslant_m$ (как и $\equiv_m$) рефлексивно, $X \leqslant_m X$, и транзитивно,

$$X \leqslant_m Y, \quad Y \leqslant_m Z \Rightarrow X \leqslant_m Z.$$

Кроме того,

$$X \leqslant_m Y \quad \Rightarrow \quad \mathbb{N}\backslash X \leqslant_m \mathbb{N}\backslash Y.$$

Легко устанавливается следующий факт.

10.1.1. Теорема. *Если X **m**-сводится к разрешимому или перечислимому множеству Y, то X, соответственно, разрешимо или перечислимо.*

Если же $X \leqslant_m Y$, но X неразрешимо или неперечислимо, то и Y, соответственно, неразрешимо или неперечислимо.

10.1.2. Определение. *Перечислимое множество Y называется **m**-полным, если к нему **m**-сводится любое другое перечислимое множество.*

Другими словами, множество Y ***m*-полно**, если перечислимо, и любое другое перечислимое множество X представимо в виде прообраза $X = f^{-1}(Y)$, где f всюду определенная вычислимая (т. е. общерекурсивная) функция.

В силу транзитивности отношения $\leqslant_m$ все ***m*-полные множества** ***m*-сводятся** друг к другу. Кроме того, *все **m**-полные множества неразрешимы*, поскольку к ним обязаны ***m*-сводиться** перечислимые неразрешимые множества, существование которых гарантирует, например, теорема 1.6.4.

Все непустые отличные от $\mathbb{N}$ разрешимые множества ***m*-эквивалентны** друг другу. (**?**)

Отношение ***m*-эквивалентности** разбивает числовые множества на непересекающиеся классы ***m*-эквивалентных множеств**, а отношение ***m*-сводимости** частично упорядочивает эти классы. Среди перечислимых множеств (если не считать $\varnothing$ и $\mathbb{N}$) наименьшим в смысле $\leqslant_m$ оказывается класс разрешимых множеств, а наибольшим — класс ***m*-полных множеств**.

10.2. Продуктивность и креативность

Если перечислимое множество неразрешимо, то его дополнение неперечислимо (теорема 1.6.3). Поэтому, пытаясь как-то классифицировать неразрешимые объекты, естественно сосредоточиться на отличиях неперечислимых множеств. Первое, что приходит в голову, — выделить класс множеств, отличия которых от любого перечислимого множества можно конструктивно обосновать, т. е. эффективно указать элемент x, входящий в одно множество и не входящий — в другое.

Подобным свойством обладает, например, дополнение *диагонального множества*

$$\overline{D} = \{x : x \notin S_x\},$$

где $S_1, \ldots, S_n, \ldots$ — *гёделевская нумерация* перечислимых множеств.

В общем виде соответствующее свойство формулируется так.

10.2.1. Определение. *Множество X называется продуктивным, если существует общерекурсивная функция $f(x)$ такая, что* [1]

$$S_x \subset X \quad \Rightarrow \quad f(x) \in X \setminus S_n. \tag{10.2}$$

Более естественно выглядело бы, конечно,

$$S_x \neq X \quad \Rightarrow \quad f(x) \in X \triangle S_n \tag{10.3}$$

вместо (10.2), что позволяло бы с бóльшим основанием говорить об *эффективной неперечислимости* [4]. Но требования (10.2) и (10.3) на самом деле эквивалентны. (**?**)

10.2.2. Определение. *Перечислимое множество, дополнение которого продуктивно, называется креативным.*

На мотивации определений лучше не останавливаться, поскольку здесь трудно сказать что-либо убедительное. Просто так было названо, потом закрепилось.

Принципиальную характеристику продуктивных множеств дает следующий результат.

10.2.3. Теорема. *Любое продуктивное множество X содержит бесконечное перечислимое подмножество.*

---

[1] Для $\overline{D}$ функция $f(x) \equiv x$.

◄ Пусть n_0 — какой-либо гёделевский номер пустого множества $\varnothing$. Поскольку $S_{n_0} \subset X$, то $f(n_0) \in X$ в силу (10.2). Далее, пусть n_1 гёделевский номер перечислимого множества $\{f(n_0)\}$, состоящего из одного элемента. Ищем номер n_2 перечислимого множества $\{f(n_0), f(n_1)\}$, и так далее. ►

Строго говоря, это есть идея, а не само доказательство, поскольку в рамках идеологии конструктивизма недостаточно сказать: «берем какой-либо номер n_k». Однако алгоритм конкретного выбора обеспечивается немного скучными уточнениями.

Из теоремы 10.2.3 и определения 10.2.1 вытекает, что любое продуктивное множество X содержит цепочку вложенных друг в друга перечислимых множеств,

$$X_1 \subset \ldots \subset X_n \subset \ldots \subset X,$$

в некотором роде приближающих X.

10.3. Иммунные множества

Закономерный вопрос: существуют ли неразрешимые множества, не являющиеся *продуктивными* (равносильно, *креативными*)?

10.3.1. Определение. *Бесконечное множество, не содержащее бесконечных перечислимых подмножеств, называется иммунным, а перечислимое множество с иммунным дополнением — простым.*

Определить, конечно, легко. Труднее убедиться в существовании. Тут опять-таки преуспел Пост, сконструировавший *простое множество*.

◄ Конструкция основана на естественной идее. Простое множество X должно иметь *бесконечное дополнение* и *пересекаться с любым бесконечным перечислимым множеством* S_n, где $S_1, \ldots, S_n, \ldots$ нумерация перечислимых множеств. Если бездумно взять по одному номеру из каждого S_n, то невозможно гарантировать бесконечность дополнения $\overline{X}$.

Выигрывающий маневр заключается в следующем. Рассмотрим множество пар $W = \{(x, n)\}$, где одновременно (для каждой пары) $x \in S_n$ и $x > 2n$. Отбрасывание ранее встречавшихся пар при перечислении W дает множество пар $\widehat{W}$, вторые члены которого (проекция) порождают перечислимое множество $X \subset \mathbb{N}$, пересекающееся с любым бесконечным перечислимым множеством. ►

Иммунные множества обычно характеризуют как «тесные», поскольку они не вмещают ни одного бесконечного перечислимого

множества. В то же время [23]: *существует континуум множеств, иммунных вместе со своими дополнениями*[2]. Но обоснование этого факта, разумеется, неконструктивно.

Иммунное множество представляет собой, безусловно, аномалию. Про него нельзя даже конструктивно сказать, конечно оно или бесконечно. Ибо в последнем случае надо бы уметь предъявлять сколько угодно членов, но это уже вариант продуктивного множества.

10.4. Вычисления с оракулом

Вычисления с оракулом — скользкая область, поскольку в некотором роде предполагает существование «того света» и волшебной палочки. С другой стороны, если попытку упорядочить множества, не поддающиеся конструктивному анализу, считать правомочной, почему бы не выпустить джинна из бутылки.

Допустим, имеется «черный ящик», называемый *оракулом*, выдающий значения функции $O(x)$. Под вычислением с оракулом $O(x)$ подразумевается любой алгоритм, имеющий возможность по мере вычислений время от времени посылать на вход оракула любое x и получать ответ $y = O(x)$. В иной интерпретации оракул дает ответ о принадлежности x некоторому множеству Ω, но этот вариант, очевидно, взаимосвязан с предыдущим.

Чтобы судить о «криминальности» замаха, достаточно сказать, что один из простейших и широко используемых оракулов — решает проблему останова машины Тьюринга[3]. На вход посылается программа и входное слово, на выходе — точный прогноз об остановке машины или зацикливании. Конечно, на фоне «какой-нибудь» аксиомы выбора такое предположение не слишком зашкаливает, но тут особая ситуация. Предположение делается в той же епархии, в которой была обоснована принципиальная неразрешимость *проблемы останова*. Причем дело не в соблюдении приличий, а в некоторой идеологической несовместимости подходов. Однако, как

[2] То есть X и $\overline{X}$ оба тесные, но $X \cup \overline{X} = \mathbb{N}$.

[3] Алгоритмы, использующие оракул, решающий проблему останова, называются $\mathbf{0}'$-*вычислениями*.

говорится, собака лает, караван идет. Плохо ли, хорошо ли, но понятие оракула позволяет различать (видеть) оттенки в невидимой области, что хотя и не отмечено в книге рекордов Гиннесса, имеет свои плюсы.

Релятивизация. Возможность обращения к оракулу $O(x)$ *релятивизует* теорию алгоритмов. Алгоритмы приобретают новые свойства, но это никак не влияет на фундаментальные результаты о вычислимых функциях, теперь уже «*O-вычислимых*». Среди функций остаются принципиально недоопределяемые; возникают «*O-неразрешимые*» множества, «*O-перечислимые*»; существуют «*O-универсальные функции*» и т. п.

При этом не меняются не только результаты, но и доказательства. Собственно, результаты не меняются как раз потому, что остаются работоспособны все старые схемы рассуждений. В определение рекурсивных функций привносим еще одну всюду определенную функцию $O(x)$. Никаким принципиальным выводам это не мешает. В этом полезно убедиться, примерив нововведение к разным ситуациям. То же самое — с машинами Тьюринга. Но это тема для индивидуального размышления[4)].

Релятивизация теории вычислимых функций — очень простая, но важная идея. «Важная» с точки зрения понимания, что такое алгоритм. Перемена обстоятельств, не влияющая на природу явления, кое-что дает для проникновения в суть изучаемых механизмов. И не будь оракулов — их бы стоило выдумать, чтобы осмыслить предмет в направлении релятивизации.

10.5. Тьюринговы степени

Разрешающая способность m-сводимости все-таки недостаточна, чтобы охватить любые неразрешимые множества. Более совершенную лакмусовую бумажку, хотя и фантастического происхождения, дает сводимость по Тьюрингу, позволяющая сравнивать по сложности решения даже те задачи, которые не поддаются алгоритмическому определению.

[4)] «Коллективное» обсуждение некоторые темы только запутывает.

Множество X называют *сводимым по Тьюрингу* (T-*сводимым*) к Y, что обозначается как $\boxed{X \leqslant_T Y}$, если X разрешимо при наличии оракула для Y.

При этом характер использования оракула не обязательно предполагает простейший вариант $x \in X \Leftrightarrow f(x) \in Y$, как в случае $\boldsymbol{m}$-сводимости. Допускаются алгоритмически более сложные схемы.

Отношение $\leqslant_T$ рефлексивно и транзитивно, рáвно как и $\equiv_T$,

$$X \equiv_T Y, \quad \text{если} \quad X \leqslant_T Y,\ Y \leqslant_T X,$$

что позволяет ввести классы эквивалентности по $\equiv_T$, называемые *тьюринговыми степенями*, или T-*степенями*, или, наконец, *степенями неразрешимости*. Иными словами, T-степень $\mathrm{dg}X$ — это класс эквивалентности, которому принадлежит множество[5] X.

Неперечислимые множества теперь «легализуются» и могут даже T-сводиться к перечислимым. Например, диагональное множество и его дополнение T-сводятся друг к другу, попадая в один класс эквивалентности. В один класс попадают все $\boldsymbol{m}$-полные множества и их дополнения.

Тем не менее самого сложного множества Z в смысле тьюринговой сводимости не существует, поскольку в релятивизации теории алгоритмов с помощью оракула Z были бы свои «неразрешимости».

Строгой упорядоченности T-сводимость не обеспечивает. Существование T-несравнимых множеств устанавливается достаточно просто (*Клини*, *Пост*) на примере несколько экзотических множеств. Долгое время оставался нерешенным вопрос о существовании несравнимых по Тьюрингу перечислимых множеств (*проблема Поста*). Она была решена независимо *Мучником* и *Фридбергом*. Решение оказалось достаточно сложным и вызвало определенный резонанс в математических кругах, но какого-то принципиального значения для теории алгоритмов это *пока* не имеет, если не считать изобретение по ходу дела *метода приоритетов*, который теперь достаточно широко применяется в качестве инструмента.

[5] В аналогичные классы можно объединять функции [27].

10.6. Иерархия степеней

Любое перечислимое множество X есть проекция разрешимого множества $Y \subset \mathbb{N} \times \mathbb{N}$, и наоборот,

$$x \in X \quad \Leftrightarrow \quad \exists y : (x, y) \in Y. \tag{10.4}$$

◀ Алгоритм, перечисляющий X, получается перечислением пар с удалением по ходу дела вторых членов.

Обратно, перечислимое X есть проекция разрешимого множества пар (x, y), где $x \in X$ появляется в течение y шагов работы алгоритма, перечисляющего X. ▶

Замена в (10.4) $\exists$ на $\forall$ приводит к условию

$$x \in X \quad \Leftrightarrow \quad \forall y : (x, y) \in Y, \tag{10.5}$$

которое имеет другую интерпретацию, описывая множества X с перечислимыми дополнениями (если под Y по-прежнему подразумевается разрешимое множество пар).

Механизмы (10.4), (10.5) используются для индуктивного определения *тьюринговых классов* Σ_n, Π_n. Множество X из (10.4) принадлежит классу Σ_{k+1}, если $Y \in \Pi_k$, а X из (10.5) принадлежит классу Π_{k+1}, если $Y \in \Sigma_k$.

В качестве Σ_0, Π_0 выбираются классы разрешимых множеств. Тогда Σ_1 — перечислимые множества, Π_1 — их дополнения. И так далее — в теории. Практика заканчивается после первой итерации.

Глава 11

Сводка определений и результатов

11.1. Алгоритмы и вычислимость

✓ *Алгоритм — это программа на любом универсальном языке программирования (например, на фортране).*

✓ *Может ли алгоритм доказывать теоремы?* Может, причем *любые доказуемые*. Известные и еще неизвестные. Идея заключается в поиске цепочек, ведущих от исходных аксиом к формулировкам теорем. Все это кодируется, и перебором любая конечная цепочка рано или поздно будет найдена, *если существует*.

✓ **Определение 1.3.1.** *Целочисленную функцию $f(n)$ целочисленного аргумента называют вычислимой, если существует алгоритм, вычисляющий значения $f(n)$, но необязательно приводящий к результату. Множество вычислимых функций обозначается через $\mathbb{F}$.*

✓ Вычислимые функции (программы вычислений) могут быть эффективно пронумерованы:

$$f_1(n), \ldots, f_k(n), \ldots .$$

Сначала перечисляются все программы из одной буквы, потом из двух, потом из трех и так далее.

✓ **Теорема 1.5.1.** *Любая попытка ввести понятие вычислимой функции $f(n)$ так, чтобы она была определена при любом n, — неразумна.*

✓ Множество считается *перечислимым*, если существует эффективная процедура (алгоритм) порождения его элементов. Элементы перечислимого множества эффективно нумеруются — в порядке появления.

✓ Множество называется *разрешимым*, если существует эффективная процедура для выяснения принадлежности любого n этому множеству. Говорят также, что разрешимое множество *распознаваемо*.

✓ Эквивалентные определения:

Определение. *Множество X перечислимо, если оно есть область значений либо область определения вычислимой функции.*

Определение. *Множество* X *разрешимо, если его характеристическая функция,*

$$\theta_X(x) = \begin{cases} 1, & \text{если } x \in X; \\ 0, & \text{в противном случае,} \end{cases}$$

вычислима.

✓ **Теорема Поста 1.6.3.** *Для разрешимости* X *необходимо и достаточно, чтобы* X *и его дополнение* $\overline{X}$ *были перечислимы.*

✓ **Теорема 1.6.4.** *Существует перечислимое, но неразрешимое множество положительных целых чисел.*

✓ *Образ и прообраз перечислимого множества при вычислимом преобразовании — перечислимы.*

✓ *Для вычислимости* $f(x)$ *необходима и достаточна перечислимость графика, т. е. множества пар* $\{x, f(x)\}$.

✓ Аналогом разрешимого множества является понятие *эффективно вычислимой функции* $f(n)$, которая, по определению, вычислима и определена при любом n. В теории рекурсивных функций — это так называемые *общерекурсивные функции.*

Теорема 1.7.1. *Множество эффективно вычислимых функций неперечислимо (не может быть эффективно пронумеровано).*

✓ **Определение.** *Функция называется* ***примитивно рекурсивной****, если она может быть получена с помощью операций:*

$$o(x) = 0 \qquad \text{(обнуление)},$$

$$\sigma(x) = x + 1 \qquad \text{(следование)},$$

$$\theta_m^n(x_1, \ldots, x_n) = x_m \qquad \text{(проектирование)},$$

а также *суперпозиции,*

$$\omega(x_1, \ldots, x_n) = \psi[\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_m(x_1, \ldots, x_n)],$$

и *примитивной рекурсии,*

$$\begin{cases} f(x, 0) = g(x), \\ f(x, y + 1) = h[x, y, f(x, y)], \end{cases}$$

где $x = \{x_1, \ldots, x_n\}$.

✓ **Определение.** *Функция называется* ***частично рекурсивной****, если она может быть получена с помощью операций, определяющих примитивно рекурсивные функции, и* ***оператора минимизации***

$$\mu y\{\varphi(x; y) = 0\},$$

дающего наименьшее $y \in \mathbb{N}$, *которое удовлетворяет уравнению* $\varphi(x; y) = 0$, *либо неопределенного, если такое* y *не существует.*

✓ **Определение 1.11.1.** *Множество* A *положительных векторов*

$$a = \{a_1, \ldots, a_k\}$$

называется диофантовым, если при любом $a \in A$ *и только при* $a \in A$ *полиномиальное уравнение* $p(a, x_1, \ldots, x_m) = 0$ *разрешимо в целых положительных* $x_1, \ldots, x_m$.

✓ ***Диофантовость множества равносильна перечислимости.***

✓ **Лемма 1.11.2.** *Множество* $A \subset \mathbb{N}$ *диофантово в том и только том случае, когда оно является множеством положительных значений некоторого полинома* $P(x_1, \ldots, x_k)$.

✓ Отрицательное решение *десятой проблемы Гильберта* дает простой перевод на другой язык факта существования перечислимого, но неразрешимого множества. Последнее означает существование такого полинома $P(x_1, \ldots, x_k)$, что разрешимость уравнения

$$P(x_1, \ldots, x_k) - y = 0$$

по $x_1, \ldots, x_k$ при любом положительном y — алгоритмически непроверяема.

✓ Вычислимые функции $y = f(x)$ — это функции, график которых

$$G = \{x_1, \ldots, x_n,\ y = f(x_1, \ldots, x_n)\}$$

диофантов.

11.2. Неполнота арифметики

✓ **Теорема 2.1.1.** *Какова бы ни была совокупность аксиом, существует полином* $Q(x_1, \ldots, x_k)$, *отсутствие у которого целых положительных корней недоказуемо.*

✓ **Теорема 2.1.2.** *Существует полином* $P(x) = P(x_1, \ldots, x_k)$ *такой, что высказывание*:

«*уравнение* $P(x) - y = 0$ *неразрешимо по* x *при некоторых* y»

истинно, но недоказуемо ни в какой непротиворечивой системе аксиом, включающей **примитивную** *арифметику.*

✓ **Теорема 2.3.1 о непротиворечивости.** *Если теория* T *непротиворечива и содержит в себе арифметику, то непротиворечивость* T *недоказуема в* T.

Разумеется, теорема 2.3.1 не исключает возможности решения проблемы за счет привлечения дополнительных средств (аксиом), и такого сорта утверждения о непротиворечивости арифметики получены, например, *Генценом*. Но гарантировать непротиворечивость *расширенной аксиоматики* опять-таки нельзя в силу теоремы 2.3.1, и необходим следующий акт расширения. Путь ведет в «никуда», и в этом смысле *проблема непротиворечивости* не имеет абсолютного решения.

✓ **Теорема 2.4.1.** *Множество $\mathcal{P}$ неразрешимых полиномов $P(x)$ — неперечислимо (тем более, неразрешимо).*

✓ **Теорема 2.4.2.** *Арифметика неаксиоматизируема, даже при включении в систему бесконечного, но конструктивно (перечислимо) задаваемого множества аксиом.*

✓ **Теорема 2.4.3.** *Существуют системы аксиом, «порочность» которых принципиально нельзя обнаружить.*

11.3. Универсальные функции и нумерации

✓ Нумерация вычислимых функций

$$f_1(x), \ldots, f_n(x), \ldots$$

позволяет считать двуместную функцию

$$U(n, x) = f_n(x)$$

универсальной.

Поднятие индекса означает, что функция $U(n, x)$ *вычислима* в рамках той же самой идеологии. Другими словами, что нумерация осуществима программой на фортране (рекурсивной функцией, машиной Тьюринга), т. е. теми же средствами, которые вычисляют сами функции $f_n(x)$.

✓ **Определение.** *Нумерация и функция $U(n, x)$ называются* ***гёделевскими****, если существует всюду определенная вычислимая функция $s(n)$ такая, что для любой двуместной функции $f(n, x)$ справедливо*

$$f(n, x) = U(s(n), x).$$

✓ *Упорядочение программ вычисления по их длине дает гёделевскую нумерацию.*

✓ *Диагональная функция $u(n) = U(n, n)$ заведомо не определена при всех n и принципиально недоопределяема.* Другими словами, существует n, при котором значение $f_n(n)$ не определено, т. е. n-я программа не применима сама к себе (к своему номеру).

✓ **Теорема 3.1.3.** *Среди вычислимых — существуют функции, область определения которых не может быть расширена до $\mathbb{N}$.*

✓ **Теорема 3.2.1.** *Область определения универсальной функции $U(n, x)$, а также множество пар $\{n, U(n, x)\}$, — являются гёделевскими универсальными множествами.*

✓ **Теорема Клини о неподвижной точке 3.4.1.** *Какова бы ни была вычислимая всюду определенная функция $q(n)$, найдется n, при котором*

$$U(n, x) = U(q(n), x)$$

тождественно по x, где $U(n, x)$ — гёделевская универсальная функция.

✓ **Теорема Райса 3.5.1.** *Любое нетривиальное свойство вычислимых функций алгоритмически неразрешимо.*

11.4. Доказуемость

✓ Природа конфликта доказуемости с истинностью заключается *в конструктивном определении теорем и неконструктивном определении истины.* Истинные утверждения допускают обороты «для всех x» «не существует x», а поскольку возможных значений x бесконечно много — не ясно, как это проверить. Доказательства же рассматриваются как цепочки, соединяющие «предположения» с «выводами», — звенья которых регулируются аксиоматикой. Концы цепочек — это доказуемые *теоремы*. Если возможностей языка хватает для формулировки результатов, у которых «посылки» не соединяются с «заключениями», — возникает ниша недоказуемых фактов.

✓ **HSI-проблема Тарского.** Из *арифметики Пеано* извлекаются тождества, записанные на языке «$+$, $\times$, $\uparrow$», и ставится задача выделить конечный набор (базис) тождеств, из которых бы все остальные следовали. Такого базиса в данном случае нет, что можно интерпретировать как *неаксиоматизируемость арифметики в срезе* «$+$, $\times$, $\uparrow$».

✓ **Нормальные алгоритмы Маркова.** Любой алгоритм при записи опирается на некие правила, которые на синтаксическом уровне сводятся к некоторой *системе подстановок*. Точнее говоря, исходное слово в избранном алфавите — скажем, $\mathbb{A} = \{a, b, c\}$, — шаг за шагом преобразуется с помощью регламентированных замен кусков текста, порождая цепочки преобразований вида

$$cbc \to bbcc \to bbbac \to bbbaa.$$

В *нормальном алгоритме* процедура уточняется следующим образом. На каждом шаге подстановки перебираются в заданном порядке, и применяется первая возможная (слова просматриваются слева направо). При отсутствии разрешенной подстановки алгоритм останавливается.

✓ Машина Тьюринга представляет собой частный случай нормального алгоритма. В то же время *нормальные алгоритмы реализуются на подходящих машинах Тьюринга.*

✓ **Канонические системы Поста** идеологически близки к нормальным алгоритмам Маркова, но это иной по духу инструмент. В записи подстановок помимо символов собственного алфавита $\mathbb{A} = \{a, b, \ldots\}$ могут фигурировать переменные (обозначаемые большими буквами), вместо которых можно подставлять слова, записанные в $\mathbb{A}$. Такие подстановки называются *продукциями Поста*. Например, «$S \Rightarrow Saa$» обозначает возможность приписать aa справа к любому слову.

✓ ***Определение.*** *Каноническая система Поста есть система из трех составляющих*:

- *собственный алфавит* $\mathbb{A}$ *плюс алфавит переменных* $\mathbb{X}$,
- *набор аксиом* (*слов в алфавите* $\mathbb{A}$),
- *совокупность продукций.*

✓ ***Определение.*** *Последовательность слов в канонической системе есть* ***доказательство****, если каждое слово этой последовательности есть либо аксиома, либо выводимо из предыдущих слов применением одной из продукций. Последнее слово любого доказательства называется* ***теоремой****.*

✓ В общем случае система Поста не предполагает алгоритмическую реализацию, поскольку при последовательном применении не предусмотрено правило выбора продукции на каждом шаге. Но если вернуться к *нормальным алгоритмам Маркова*, добавив к исходному — алфавит свободных переменных и оговорив список начальных слов (аксиом), — получится система Поста с наложением дополнительного правила выбора продукции.

✓ **Теорема 4.4.3.** *Каково бы ни было перечислимое множество T слов в алфавите $\mathbb{A}$, существует каноническая система, множество теорем которой совпадает с T.*

✓ Пост установил, что за счет *канонического расширения* любая система может быть сведена к системе с *единственной аксиомой* и *нормальными продукциями* вида $\alpha X \Rightarrow X\beta$, где α, β — слова в расширенном алфавите.

✓ При заданном наборе продукций $\{\Pi_k\}$ естественно возникает вопрос о возможности преобразовать то или иное слово α в слово β. Для некоторых наборов $\{\Pi_k\}$ такая задача разрешима для любой пары слов (α, β). Но не в общем случае.

Близкая по характеру проблема возникает для так называемых *ассоциативных исчислений*, или *систем Туэ*, — определяемых *системами подстановок*, но с возможностью замен в обоих направлениях, что не так уж принципиально, поскольку $\alpha \Leftrightarrow \beta$ равносильно совокупности двух подстановок $\alpha \Rightarrow \beta$ и $\beta \Rightarrow \alpha$. Однако для преобразований одних слов в другие возникает новая ситуация.

Слова α и β называют *эквивалентными*, или *равными*, если одно преобразуется в другое с помощью подстановок ассоциативного исчисления.

Теорема 4.5.1. *Существуют ассоциативные исчисления, в которых проблема эквивалентности слов — неразрешима.*

11.5. Математическая логика

✓ Если говорить о решении конкретных математических задач, то логика больше мешает, чем помогает, — ибо задумывалась как *метаматематическая* дисциплина, призванная наблюдать математику извне. В этом ее главная задача. Не способствовать доказательству теорем, а «орлиным взглядом» оценить сам процесс обоснования. Разобраться в принципиальных возможностях и ограничениях.

✓ Исходным материалом *двузначной логики* являются переменные x, y, z, ..., принимающие одно из двух значений: $\{1, 0\}$ либо $\{$*истина* (И), *ложь* (Л)$\}$. Цифровой вариант $\{1, 0\}$ выглядит симпатичнее, хотя «кому как».

На том же уровне «первичности» — *логические связки*:

$$\bar{}\,(\textit{отрицание «не»}),\quad \vee\ (\textit{или}),\quad \wedge\ (\textit{и}),\quad \to\ (\textit{следует}),$$

которые являются функциями, принимающими, как и аргументы, одно из двух значений, 1 или 0.

• Для *отрицания* наряду с «чертой сверху» используется также знак $\neg$: $\bar{x} = \neg x$ означает «не x», т. е. $\bar{x} = 0$, если $x = 1$, и наоборот.

• Связку $\vee$ называют *дизъюнкцией*; $x \vee y$ («x *или* y») — это функция двух переменных, равная 1, если хотя бы одна переменная равна 1, и равная 0 в противном случае.

• Функция $x \wedge y$ («x *и* y»), равная 1, если $x = y = 1$, и равная 0 в противном случае, называется *конъюнкцией*; эквивалентные обозначения: $x\&y$ либо $x \cdot y$, и даже xy.

• *Импликация* $x \to y$ («*из* x *следует* y», «*если* x, *то* y») как функция двух переменных всюду принимает значение 1 за исключением случая $x = 1$, $y = 0$, где $x \to y$ равна 0. Другими словами, из «истины» не может следовать «ложь», все остальное — возможно.

✓ Конъюнкция и дизъюнкция часто путаются в голове. Многие лучше воспринимают вместо $\wedge$, $\vee$, соответственно, знаки «$\cdot$» (либо «$\times$») и «$+$». На игровом поле $\{1, 0\}$ конъюнкция — в чистом виде арифметическое умножение $x \cdot y$. Плюс для дизъюнкции не соответствует обычному сложению, но в целом, как показывает опыт, к обозначениям «$\cdot$», «$+$» привыкают быстрее.

✓ Как в арифметике с помощью умножения и сложения выписываются сложные формулы, так и в логике комбинации связок позволяют задавать n-местные *логические функции* $\varphi(x_1, \ldots, x_n)$.

Любая n-местная логическая функция $\varphi(x_1, \ldots, x_n)$ записывается (с помощью *конъюнкций, дизъюнкций и отрицаний*) в *дизъюнктивной нормальной форме*, т. е. в виде суммы произведений (дизъюнкции конъюнкций) переменных или их отрицаний. Например,

$$x \cdot y \cdot z + x \cdot \bar{y} \cdot z + \bar{x} \cdot y \cdot \bar{z} = x \cdot z + \bar{x} \cdot y \cdot \bar{z}.$$

✓ В *булевой алгебре* рассматривается структура $\mathscr{E}$ с операциями $\{+, \times, \bar{}, \supset\}$, которые не выводят из $\mathscr{E}$ и обладают свойствами, очевидными при теоретико-множественной интерпретации «$\cup \Leftrightarrow +$», «$\cap \Leftrightarrow \times$».

✓ Рассуждения предполагаются состоящими из элементарных фрагментов u_j, называемых *высказываниями*, которые представляют в совокупности некое множество $U = \{u_j\}$ и могут быть либо истинными, либо ложными. Высказывания объединяются с помощью логических связок в *формулы*: $f(u_1, \ldots, u_n)$. Символы f называют *функциональными*. Формулам, каковыми, в том числе, считаются *константы языка*, приписываются имена (*термы*). Таким образом, объекты изучения в логике напоминают стандартную ситуацию. Упрощенно говоря, есть аргументы и функции.

✓ Логический анализ обычно направлен на изучение той или иной предметной области — теория множеств, арифметика, теория групп. Высказывания при этом констатируют свойства и взаимоотношения изучаемых объектов, и называются предикатами. Говоря более общим языком, *предикат* $P(x_1, \ldots, x_n)$ — это многоместное (в том числе, одноместное) отношение, которое превращается в истинное или ложное высказывание при подстановке конкретных значений переменных $\{x_1, \ldots, x_n\}$. Предикатами часто называют сами знаки отношений: $+$, $-$, $\geqslant$, $\times$.

При общетеоретическом рассмотрении предикаты записываются в виде $P_j(x_1, \ldots, x_n)$ с помощью *предикатных символов* P_j, но фактически за этим подразумеваются отношения типа $x > y$, которые удобнее воспринимать в их привычном виде, а не в форме $>(x, y)$. Висящая без опоры запись $P(u_1, \ldots, u_n)$ подразумевает обычно истинность $P(u_1, \ldots, u_n)$, т. е. $P(u_1, \ldots, u_n) = 1$. Понятно, что в этом случае предикат $P(x_1, \ldots, x_n)$ представляет собой характеристическую функцию множества истинных высказываний о совокупностях $\{x_1, \ldots, x_n\}$.

✓ При переходе от исчисления высказываний к исчислению предикатов возникает дрейф терминологии, что создает определенные неудобства. Предикаты $P(t_1, \ldots, t_n)$, где t_j — *термы*, называются теперь *атомарными формулами*, а *формулы* в новой редакции определяются как *атомарные формулы*, а также их комбинации с помощью *логических связок*, которые могут находиться под действием *кванторов*.

При этом *термы* понимаются несколько шире, чем было сказано выше. Переменная — терм, и если $t_1, \ldots, t_n$ термы, а f n-местная функция, то $f(t_1, \ldots, t_n)$ — также терм.

✓ **Кванторы.** Характерной особенностью исчисления предикатов является использование кванторов: *квантора общности* $\forall x$ — «для всех x», и *квантора существования* $\exists x$ — «существует x». Область изменения x подразумевается оговоренной либо указывается,

$$\forall x \in X, \quad \exists x \in X.$$

Под $\forall x P(x)$ имеется в виду $\forall x P(x) = 1$, аналогично $\exists x P(x)$ трактуется как $\exists x P(x) = 1$.

Переход от $P(x)$ к $\forall x P(x)$ либо $\exists x P(x)$ связывает переменную x, принципиально меняя ее роль. Переменные, находящиеся под действием какого-либо квантора, называют *связанными* (*немыми*), остальные — *свободными*. *Формулы*, не содержащие свободных переменных, называются *замкнутыми*.

Навешивание квантора, $\forall x_1 P(x_1, \ldots, x_n)$, превращает n-местный предикат $P(x_1, \ldots, x_n)$ в — $(n-1)$-местный [1].

✓ **Языки.** Логика уделяет повышенное внимание средствам описания изучаемых явлений. Специфику языка определяют: *константы языка*, а также функциональные и предикатные символы, — объединяемые в так называемую *сигнатуру*. Причем *константами языка* называют не обязательно конкретные числа (что не исключается), а вообще *собственные символы* — элементы множества, на котором «разворачивается сюжет» (переменные имеют право принимать значения констант языка).

✓ Логические исследования развиваются двумя параллельными курсами, *семантическим* и *синтаксическим*.

В семантическом русле за символами стоят реальные операции («или», «не», «для всех», «+») и объекты (числа, множества). Синтаксическое рассмотрение предмета оставляет только символы. Знаки $\forall$, $\exists$, $\vee$, $\subset$, $\times$ — превращаются в буквы, за которыми нет никакого смыслового содержания. Поэтому преобразования и выводы, базировавшиеся ранее на понимании свойств операций, теперь должны регулироваться новыми механизмами, каковыми являются различные *правила вывода* и *аксиомы*.

Операция вывода [2] обозначается знаком $\vdash$. Выражения

$$p_1, \ldots, p_n \vdash q \qquad (\textit{из } p_1, \ldots, p_n \textit{ следует } q)$$

называются *секвенциями* [3], а *правила вывода* записываются в форме

$$\frac{S_1, \ldots, S_m}{S},$$

что означает: «*из секвенций* $S_1, \ldots, S_m$ *следует* S». Секвенция, находящаяся под чертой, называется *заключением*, а секвенции над чертой называются *посылками*.

✓ **Аксиоматика и семантическое следование.** В предметных областях обычно фиксируется некоторая совокупность *замкнутых формул*, называемых *аксиомами*. Выводить следствия из аксиом можно по правилам синтаксического следования — такие правила специально оговариваются, — и тогда используется знак $\vdash$. Например, $A_1, A_2 \vdash X$ означает, что X «синтаксически» следует из A_1, A_2, где A_1, A_2 могут быть аксиомами или ранее доказанными формулами.

---

[1] Аналогично $\sum_x f(x, y)$ превращает двуместную функцию $f(x, y)$ — в одноместную.

[2] Сосуществование импликации и операции вывода часто служит источником путаницы.

[3] Запись $\vdash p$ означает «p доказуемо», а $p_1, \ldots, p_n \vdash$ — «система $p_1, \ldots, p_n$ противоречива».

Семантическое следование $A_1, A_2 \models X$ означает, что X «логически» вытекает из A_1, A_2.

Соответствия

$$A_1, A_2 \vdash X \quad \Leftrightarrow \quad A_1, A_2 \models X$$

являются обычно предметом специального исследования и свидетельствуют о том, насколько хорошо определена грамматика.

✓ На основе семантического и синтаксического следования определяются два типа *теорий*. Множество замкнутых формул, которые семантически следуют из принятой системы аксиом, называют *семантической теорией*, а если следуют синтаксически — *дедуктивной теорией*. При согласовании смыслового и грамматического следования обе теории совпадают друг с другом, что обычно оформляется «теоремами о полноте исчислений».

При формализации математических теорий на базе логики высказываний семантика игнорируется. *Теоремы* трактуются как формулы, которые могут быть выведены по определенным правилам, составляющим *аксиоматику теории*. Примером может служить правило *модус поненс* (*modus ponens*): «если x и $x \to y$, то y», — входящее обычно в любую аксиоматику.

✓ **Языки первого уровня.** *Исчисление предикатов*, в отличие от исчисления высказываний, допускает использование в *языке первого уровня* кванторов $\forall$ и $\exists$.

Как и в исчислении высказываний, здесь возникает тот же вопрос, насколько хороши дозволенные средства. Все ли истинное доказывается, и все ли доказуемое истинно? Ответ — снова «да», но это уже более сложная теорема *о полноте исчисления предикатов*.

✓ **Теорема 5.7.1.** *Если формула* $\neg f$ *недоказуема в исчислении предикатов, то* f *выполнима в* $\mathbb{N}$.

✓ **Теорема Чёрча 5.7.2.** *Исчисление предикатов неразрешимо.*

✓ **Интерпретации и модели.** *Интерпретация языка* — есть преобразование φ множества C *констант языка* в некоторое множество M, сопоставляющее функциональным символам[4] f над C — функции f_φ над M, принимающие значения 0 или 1. При этом под $f \Rightarrow f_\varphi$ подразумевается

$$\varphi[f(t_1, \ldots, t_n)] = f_\varphi(t_{1\varphi}, \ldots, t_{n\varphi})$$

с сохранением соответствия между композициями функций и соблюдением обычных «правил истинности» для логических связок.

✓ При заданной *интерпретации* подстановка в $f_\varphi(\ldots)$ конкретных значений переменных дает «истину» или «ложь» — 1 или 0. Любые *замкнутые формулы*[5] являются, по сути, высказываниями и также принимают значения 1 или 0.

[4] Имеется в виду понятие функции в рамках исчисления предикатов.

[5] Не содержащие свободных переменных.

Функцию f называют *общезначимой*, если $f_\varphi(\ldots) \equiv 1$ при любой интерпретации φ, и — *выполнимой*, если существует интерпретация, в которой $f_\varphi(\ldots) = 1$ при некоторых значениях переменных.

Определение. *Моделью множества A замкнутых формул называется интерпретация, в которой истинны все формулы из A.*

✓ Множество A замкнутых формул может быть, в частности, совокупностью аксиом, из которых выводятся другие замкнутые формулы, $A \vdash f$, и такой процесс расширяет A до *теории T*. Причем в силу полноты исчисления предикатов семантическое ($\models$) и синтаксическое ($\vdash$) расширение дает в итоге одинаковый результат. Если говорить точнее, то *теория T* — это наименьшее множество формул, содержащее систему аксиом и замкнутое относительно правил вывода. *Теория T* называется *полной*, если любая замкнутая формула f либо сама, либо ее отрицание $\neg f$ — принадлежит T.

Множество A замкнутых формул считается *непротиворечивым*, если из него нельзя вывести два противоположных утверждения f и $\neg f$.

Теорема 5.8.2. *Множество A замкнутых формул, имеющее модель, непротиворечиво.*

✓ **Теорема 5.8.3.** *Если аксиоматизируемая теория полна и непротиворечива, то она разрешима.*

✓ **Теорема компактности 5.8.4.** *Если $X \models f$, то существует конечное подмножество $S \subset X$ замкнутых формул такое, что $S \models f$.*

✓ **Теоремы Лёвенгейма—Сколема:**

5.8.5. *Если счетная теория имеет модель, то она имеет также счетную модель.*

5.8.6. *Любое выполнимое множество формул выполнимо в некоторой счетной структуре.*

✓ *Арифметический язык*

$$L_0 = \{+, \times, =, \exists\}$$

подразумевает возможность *сложения*, *умножения*, *равенства и декларации существования*, позволяет записать любой полином $p(a, x)$ и делать высказывания вида $\exists\, x : p(a, x) = 0$.

Теорема 5.9.1. *Множество является диофантовым в том и только том случае, когда оно описывается на языке L_0.*

✓ **Теорема 5.10.4.** *В языке*

$$L_G = \{+, \times, =, \wedge, \exists, \forall_{\leqslant}\}$$

выразимы любые частично рекурсивные функции.

✓ **Теорема 5.10.5.** *Языки L_G и L_0 эквивалентны.*

Эта теорема решает по сути *десятую проблему Гильберта*. Средства описания вычислимых функций и перечислимых множеств, оказывается, могут быть ужаты до чисто арифметического языка диофантовых уравнений

$$L_0 = \{+,\ \times,\ =,\ \exists\},$$

выделяющегося на общем фоне экономностью и фундаментальностью.

11.6. Диофантов язык и десятая проблема Гильберта

✓ **Теорема 6.1.1.** *Диофантовость множества равносильна его перечислимости.*

✓ **Теорема 6.1.2.** *Ограниченный квантор общности $\forall_{\leqslant}$ может быть выражен в языке L_0.*

✓ Перечислению перечислимых множеств $S_1, S_2, \ldots$ может быть поставлен в соответствие *универсальный полином* $U(n, s, x_1, \ldots, x_k)$, перечисляющий все S_n,

$$s \in S_n \quad \Leftrightarrow \quad \exists\,(x_1, \ldots, x_k) : U(n, s, x_1, \ldots, x_k) = 0,$$

причем $U(n, s, x)$ при желании строится конструктивно.

✓ В эквивалентном варианте существует универсальный полином $\widehat{U}(n, x_1, \ldots, x_{k+1})$, множество положительных значений которого при фиксированном n совпадает с S_n,

$$s \in S_n \Leftrightarrow \exists\,(x_1, \ldots, x_{k+1}) : s = \widehat{U}(n, x_1, \ldots, x_{k+1}) \wedge s > 0.$$

Конкретно:

$$\widehat{U}(n, x_1, \ldots, x_{k+1}) = x_{k+1}[1 - U^2(n, x_{k+1}, x_1, \ldots, x_k)].$$

✓ **Теорема 6.3.1.** *Каков бы ни был полином $P(n, z_1, \ldots, z_N)$ и какова бы ни была размерность N, существует полином*

$$\widehat{U}(n, x_1, \ldots, x_m)$$

фиксированной размерности m, множество положительных значений которого при любом n в точности совпадает с множеством положительных значений полинома $P(n, z_1, \ldots, z_N)$.

✓ Помимо степени n полинома важна и другая характеристика: число переменных $\{x_1, \ldots, x_m\}$, по которым декларируется существование решения. Для любого диофантова множества можно указать полином с $n \leqslant 4$ (но, возможно, большим m) либо $m \leqslant 9$ (но, может быть, большим n).

11.7. Конструктивная математика

✓ **Последовательность Шпеккера.** Пусть числа записываются в двоичной системе, все $\alpha_n \in \{0, 1\}$, и пусть всюду определенная вычислимая функция $f(k)$ перечисляет *без повторений* те номера n, которым отвечает $\alpha_n = 1$, т. е. те позиции в записи числа, где стоят единицы (а не нули).

Изначально считаем, что во всех позициях стоят нули. Через N шагов в каких-то N позициях будут расставлены единицы. Получится рациональное число

$$S_n = 0{,}00101101\ldots011.$$

Очевидно, последовательность $\{S_n\}$ строго монотонно возрастает, $S_{n+1} > S_n$, и ограничена, $S_n \leqslant 1$.

Но *если $f(k)$ перечисляет неразрешимое множество, — воспользоваться классической теоремой анализа о сходимости ограниченной монотонной последовательности не удается.* В этом случае $\{S_n\}$ называют *последовательностью Шпеккера*. Она не сходится, поскольку не является фундаментальной.

11.8. Аксиоматические теории

✓ *Аксиоматика Пеано* сводит арифметическую систему $\{\mathbb{N}, +, \times\}$ к алгебре с одной *операцией счета* σ, называемой также *функцией следования*, $\sigma : \mathbb{N} \to \mathbb{N}$, и удовлетворяющей трем *аксиомам Пеано*:

A1 $\sigma(m) = \sigma(n) \Rightarrow m = n$.

A2 $\forall n \in \mathbb{N} : \sigma(n) \neq 1$.

A3 Если $1 \in Q \subset \mathbb{N}$, где Q — произвольное подмножество $\mathbb{N}$, и «$n \in Q \Rightarrow \sigma(n) \in Q$», то $Q = \mathbb{N}$.

Последняя аксиома A3 выражает *принцип математической индукции*.

✓ *Аксиомы теории множеств — система* ZFC:

Z1. *Аксиома объемности.* $\forall x : (x \in y \leftrightarrow x \in z) \to y = z$, т. е. множества равны, если и только если состоят из одних и тех же элементов.

Z2. *Аксиома пары.* Каковы бы ни были x и y, существует множество z, содержащее x и y (иногда добавляют: только x и y, — что может быть получено в рамках ZF-системы в качестве теоремы).

Z3. *Аксиома отделимости.* Каковы бы ни были x и y, для любого предиката $\varphi(u, v)$ существует множество $z = \{t \in x : \varphi(t, y)\}$, содержащее все $t \in x$, обладающие свойством $\varphi(\cdot, y)$.

Z4. *Аксиома объединения.* Любому семейству множеств $\mathcal{X}$ отвечает множество, содержащее все элементы, входящие в $\mathcal{X}$.

Z5. *Аксиома степени.* Для любого x существует множество 2^x всех подмножеств x.

Z6. *Аксиома бесконечности.* Существует бесконечное множество.

Z7. *Аксиома выбора.* В любом семействе $\Phi = \{X_\alpha : \alpha \in A\}$ непустых множеств X_α в каждом $X_\alpha \in \Phi$ можно выбрать по одному элементу, т. е. существует функция выбора $f : A \to \Phi$.

Z8. *Аксиома фундирования* постулирует, что не существует бесконечных убывающих цепей, $x_1 \ni x_2 \ni \ldots$.

ZF9. *Аксиома подстановки.* Для любого множества x и функции f, определенной на x, существует множество, состоящее из образов $z = f(y)$, $y \in x$.

✓ **Теорема 8.5.1.** *Если теория ZF непротиворечива, то гипотеза континуума не является теоремой теории ZFC.*

✓ **Теорема 8.5.2.** *Если теория ZF непротиворечива, то аксиома выбора не является теоремой теории ZF.*

11.9. Теория моделей

✓ Теория моделей, как математическая дисциплина, которая примыкает к логике, направлена в основном на оправдание логических схем и аксиоматик. Центральная идея заключается в проектировании абстракции на что-нибудь реальное, с последующим выводом о непротиворечивости существующего.

✓ **Теорема 9.1.1.** *Если любое конечное подмножество $S \subset X$ замкнутых формул имеет модель, то и X имеет модель.*

✓ *Парадокс Сколема*: Все утверждения теории множеств, выполнимые в континуальных моделях, — по теореме 5.8.6 выполнимы и в счетных моделях. Как быть тогда с теоремами *Дедекинда* и *Кантора*, связанными с существованием *континуума*?

✓ В алгебраической системе A (с одной или несколькими операциями над элементами) естественно возникает вопрос о конечной совокупности тождеств S, из которых следуют все остальные тождества A. В этом случае S называют *конечным базисом*, каковой является в некотором роде системой аксиом для A при специфически ограниченном угле зрения.

Конечный базис может не существовать даже для тождеств в конечных группах.

11.10. Степени неразрешимости

✓ Множество $X \subset \mathbb{N}$ называют m-*сводимым* к $Y \subset \mathbb{N}$, что обозначается как $X \leqslant_m Y$, если существует такая *всюду определенная* вычислимая функция $f(x)$, что

$$x \in X \quad \Leftrightarrow \quad f(x) \in Y.$$

В случае $X \leqslant_m Y$, $Y \leqslant_m X$ множества X и Y называют m-*эквивалентными* и пишут $X \equiv_m Y$.

✓ **Теорема 10.1.1.** *Если X m-сводится к разрешимому или перечислимому множеству Y, то X, соответственно, разрешимо или перечислимо.*

✓ **Определение 10.1.2.** *Перечислимое множество Y называется m-полным, если к нему m-сводится любое другое перечислимое множество.*

Другими словами, множество Y m-полно, если перечислимо, и любое другое перечислимое множество X представимо в виде прообраза $X = f^{-1}(Y)$, где f всюду определенная вычислимая (т. е. общерекурсивная) функция.

✓ **Определение 10.2.1.** Множество X называется продуктивным, если существует общерекурсивная функция $f(x)$ такая, что

$$S_x \subset X \quad \Rightarrow \quad f(x) \in X \backslash S_n.$$

✓ **Определение 10.2.2.** *Перечислимое множество, дополнение которого продуктивно, называется креативным.*

✓ **Теорема 10.2.3.** *Любое продуктивное множество X содержит бесконечное перечислимое подмножество.*

✓ **Определение 10.3.1.** *Бесконечное множество, не содержащее бесконечных перечислимых подмножеств, называется иммунным, а перечислимое множество с иммунным дополнением — простым.*

✓ Множество X называют *сводимым по Тьюрингу* (T-*сводимым*) к Y, что обозначается как $X \leqslant_T Y$, если X разрешимо при наличии *оракула* для Y.

✓ Отношение $\leqslant_T$ рефлексивно и транзитивно, рáвно как и $\equiv_T$, что позволяет ввести классы эквивалентности по $\equiv_T$, называемые *тьюринговыми степенями*, или T-*степенями*, или, наконец, *степенями неразрешимости*. Иными словами, T-степень $\mathrm{dg}X$ — это класс эквивалентности, которому принадлежит множество X.

Сокращения и обозначения

◄ и ► — начало и конец рассуждения, темы, доказательства

(?) — предлагает проверить или доказать утверждение в качестве упражнения, либо довести рассуждение до «логической точки»

(!) — предлагает обратить внимание

$A \Rightarrow B$ — из A следует B

$x \in X$ — x принадлежит X

$X \cup Y$, $X \cap Y$, $X \setminus Y$ — объединение, пересечение и разность множеств X и Y

$X \triangle Y = (X \setminus Y) \cup (Y \setminus X)$ — симметрическая разность множеств X и Y

$X \subset Y$ — X подмножество Y, в том числе имеется в виду возможность $X \subseteq Y$, т.е. между $X \subset Y$ и $X \subseteq Y$ различия не делается

$\varnothing$ — пустое множество

$\mathbb{N}$ — множество натуральных чисел $\{1, 2, \ldots\}$

$\mathbb{Z}$ — множество целых чисел $\{\ldots, -1, 0, 1, \ldots\}$

$\mathbb{F}$ — множество вычислимых функций

$\mathbb{C}$ — множество конструктивных чисел

Z — арифметика Пеано

$\lfloor a \rfloor$ — целая часть числа a

$a \mid b$ — «a делит b», т.е. b делится нацело на a (вертикальная черта используется также для обозначения *штриха Шеффера*, что обычно ясно из контекста)

$x \equiv a \bmod p$ — «x при делении на p дает в остатке a»

$\uparrow$ — операция возведения в степень

НОД — наибольший общий делитель

НОК — наименьшее общее кратное

$\exists$ — квантор существования

$\forall$ — квантор общности

$\forall_{\leqslant}$ — ограниченный квантор общности, $\forall_{\leqslant n} x$ означает «для всех $x \leqslant n$»

$\vee$ — дизъюнкция

$\wedge$ — конъюнкция

$\neg$ — отрицание (равносильное обозначение: черта сверху $\bar{x}$ — «не x»)

язык $L_0 = \{+, \times, =, \exists\}$

язык $L_G = \{+, \times, =, \wedge, \exists, \forall_{\leqslant}\}$

$\rightarrow$ — импликация («следует»)

$\vdash$ — операция синтаксического (формального) вывода

$\models$ — операция смыслового (логического) вывода

$c(x, y)$ — канторовский номер пары (x, y)

$x = l(n)$, $y = r(n)$, — если $n = c(x, y)$

$\Gamma(i, n)$ — функция Гёделя

Литература

1. *Ахо А.*, *Хопкрофт Дж.*, *Ульман Дж.* Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.
2. *Босс В.* Интуиция и математика. М.: Айрис-Пресс, 2003.
3. *Босс В.* Лекции по математике. Т. 1. Анализ; Т. 2. Дифференциальные уравнения; Т. 3. Линейная алгебра; Т. 4. Вероятность, информация, статистика; Т. 5. Функциональный анализ. М.: URSS, 2004–2005.
4. *Верещагин Н. К.*, *Шень А.* Лекции по математической логике и теории алгоритмов. Вычислимые функции. М.: МЦНМО, 2002.
5. *Гильберт Д.*, *Бернайс П.* Основания математики. Теория доказательств. М.: Наука, 1982.
6. *Гладкий А. В.*, *Мельчук И. А.* Элементы математической лингвистики. М.: Наука, 1969.
7. *Гэри М.*, *Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
8. *Дэвис М.* См.: *Davis M.* Hilbert's Tenth Problem is Unsolvable // The Amer. Math. Monthly. 1973. № 3. С. 233–269.
9. *Ершов Ю. Л.* Теория нумераций. М.: Наука, 1977.
10. *Клини С. К.* Введение в метаматематику. М.: ИЛ, 1957.
11. *Коэн П. Дж.* Теория множеств и континуум-гипотеза. М.: Мир, 1969.
12. *Кузнецов О. П.*, *Адельсон-Вельский Г. М.* Дискретная математика для инженера. М.: Энергоатомиздат, 1988.
13. *Мальцев А. И.* Алгоритмы и рекурсивные функции. М.: Наука, 1986.
14. *Манин Ю. И.* Доказуемое и недоказуемое. М.: Сов. радио, 1979.
15. *Манин Ю. И.* Вычислимое и невычислимое. М.: Сов. радио, 1980.
16. *Мартин-Лёф П.* Очерки по конструктивной математике. М.: Мир, 1975.
17. Математическая теория логического вывода: Сб. переводов. М.: Наука, 1967.
18. *Матиясевич Ю. В.* Диофантовы множества // УМН. 1972. Т. 22. Вып. 5. С. 185–222.
19. *Матиясевич Ю. В.* Десятая проблема Гильберта. М.: Наука, 1993.
20. *Минский М.* Вычисления и автоматы. М.: Мир, 1971.
21. *Новиков П. С.* Элементы математической логики. М.: Наука, 1973.

22. Проблемы математической логики. Сложность алгоритмов и классы вычислимых функций. М.: Мир, 1970.
23. *Роджерс Х.* Теория рекурсивных функций и эффективная вычислимость. М.: Мир, 1972.
24. Сложность вычислений и алгоритмов. М.: Мир, 1974.
25. *Чень Ч., Ли Р.* Математическая логика и автоматическое доказательство теорем. М.: Наука, 1983.
26. *Шенфилд Дж.* Математическая логика. М.: Наука, 1975.
27. *Шенфилд Дж.* Степени неразрешимости. М.: Наука, 1977.
28. *Яглом И. М.* Булева структура и ее модели. М.: Сов. радио, 1980.

Предметный указатель

В проекте издания «Лекций по математике» В. Босса вышли тома:

1. Анализ. 2. Дифференциальные уравнения. 3. Линейная алгебра. 4. Вероятность, информация, статистика. 5. Функциональный анализ. 6. От Диофанта до Тьюринга.

Следующий том 7. Оптимизация.

В условиях информационного наводнения инструменты вчерашнего дня перестают работать.
Поэтому учить надо как-то иначе.
«Лекции» дают пример.
Плохой ли, хороший – покажет время.
Но в любом случае, это продукт нового поколения.
Те же «колеса», тот же «руль», та же математическая суть, – но по-другому.

В. Босс

Из отзывов читателей:

Чтобы усвоить предмет, надо освободить его от деталей, обнажить центральные конструкции, понять, как до теорем можно было додуматься. Это тяжелая работа, на которую не всегда хватает сил и времени. В «Лекциях» такая работа проделывается автором.

Популярность книг В. Босса среди преподавателей легко объяснима. Дается то, чего недостает. Общая картина, мотивация, взаимосвязи. И самое главное — легкость вхождения в любую тему.

Содержание продумано и хорошо увязано. Громоздкие доказательства ужаты до нескольких строчек. Виртуозное владение языком. Что касается замысла изложить всю математику в 20 томах, с трудом верится, что это по силам одному человеку.

Лекции В. Босса — замечательные математические книги. Как учебные пособия, они не всегда отвечают канонам преподавания, но студентам это почему-то нравится.

НАУЧНАЯ И УЧЕБНАЯ ЛИТЕРАТУРА

E-mail: URSS@URSS.ru
Каталог изданий в Интернете:
http://URSS.ru
Тел./факс: 7 (095) 135–42–16
URSS Тел./факс: 7 (095) 135–42–46

3798 ID 35004

Отзывы о настоящем издании, а также обнаруженные опечатки присылайте по адресу **URSS@URSS.ru**. Ваши замечания и предложения будут учтены и отражены на web-странице этой книги в нашем интернет-магазине **http://URSS.ru**